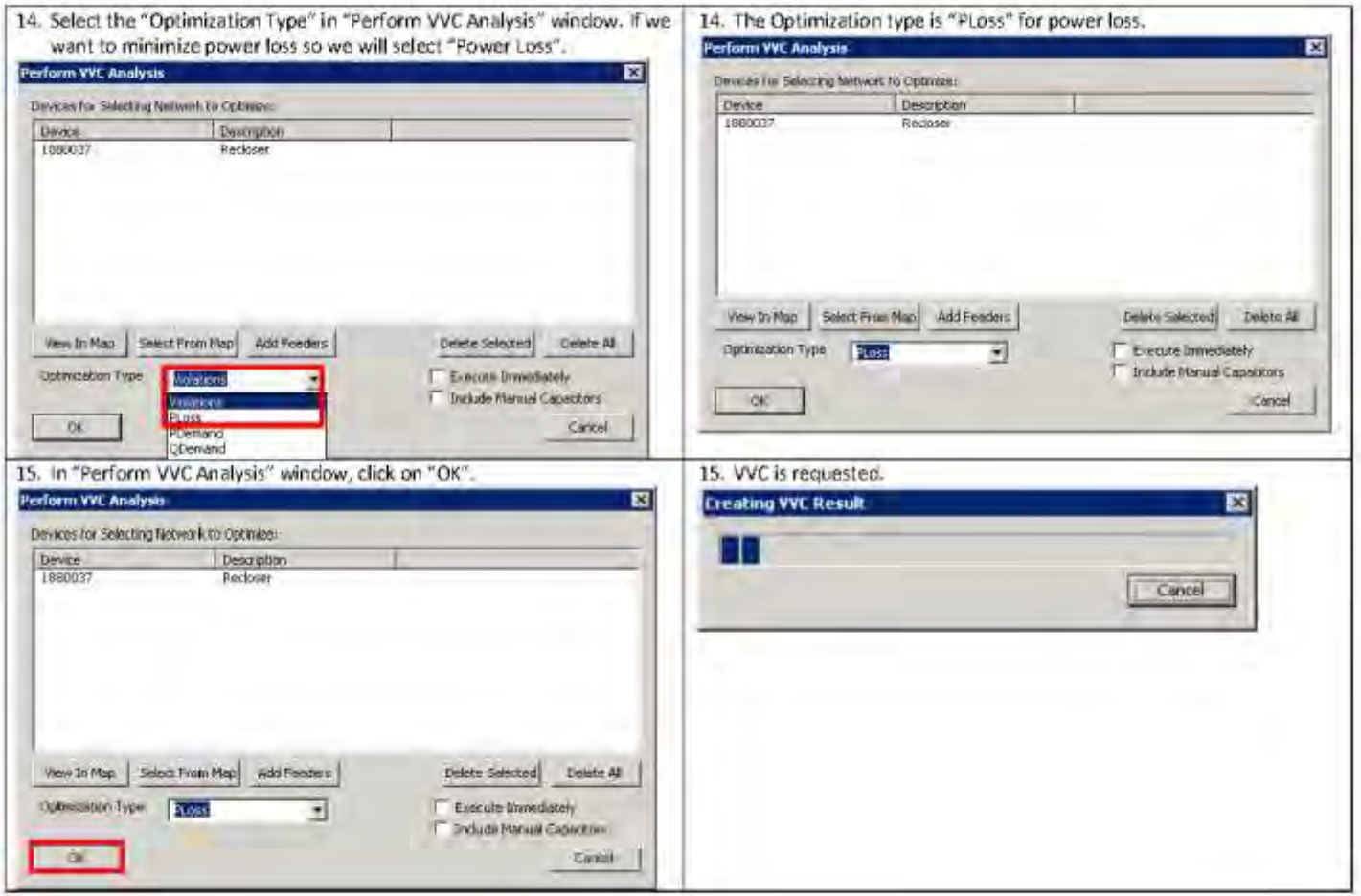
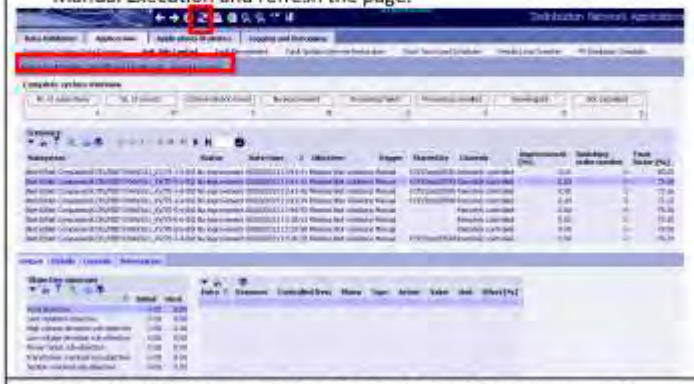

14. Select the "Optimization Type" in "Perform VVC Analysis" window. If we want to minimize power loss so we will select "Power Loss".
Perform VVC Analysis
Devices for Selecting Network to Optimize:
Device
Description
1880037
Recloser
View In Map
Select From Map
Add Feeders
Delete Selected
Delete All
Optimization Type
Violations
Violations
PLoss
PDemand
QDemand
Execute Immediately
Include Manual Capacitors
OK
Cancel
14. The Optimization type is "PLoss" for power loss.
Perform VVC Analysis
Devices for Selecting Network to Optimize:
Device
Description
1880037
Recloser
View In Map
Select From Map
Add Feeders
Delete Selected
Delete All
Optimization Type
PLoss
Execute Immediately
Include Manual Capacitors
OK
Cancel
15. In "Perform VVC Analysis" window, click on "OK".
Perform VVC Analysis
Devices for Selecting Network to Optimize:
Device
Description
1880037
Recloser
View In Map
Select From Map
Add Feeders
Delete Selected
Delete All
Optimization Type
PLoss
Execute Immediately
Include Manual Capacitors
OK
Cancel
15. VVC is requested.
Creating VVC Result
Cancel

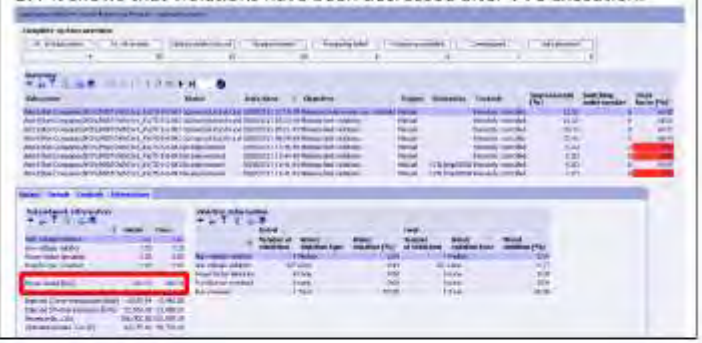
16. Go to the DNA Web UI window, opened with VVC Open Loop Results – Manual Execution and refresh the page.



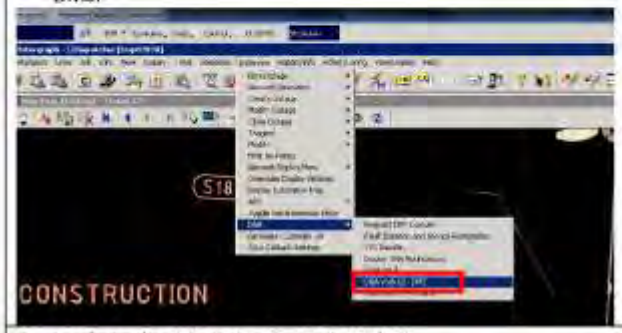
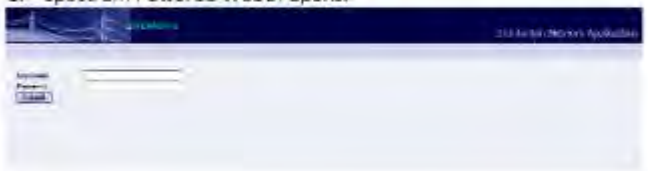
16. The VVC Open Loop Results – Manual Execution page shows the updated VVC result.

17. In the VVC Open Loop Results – Manual Execution page, go to the details tab. This shows the violations before and after VVC execution.

17. It shows that violations have been decreased after VVC execution.



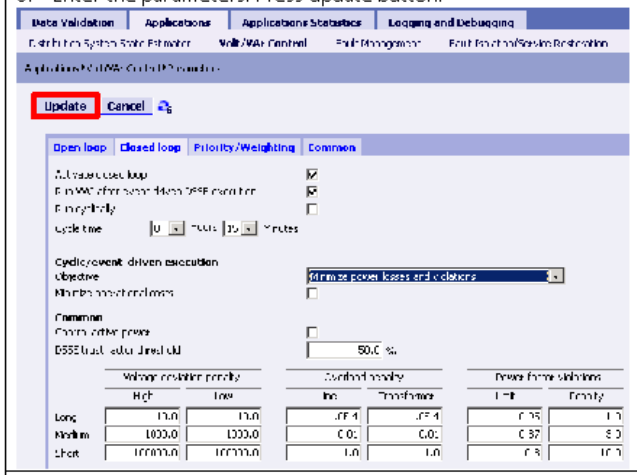
VVC in Close Loop Mode

Steps	Expected Results
1. Start WebUI from Idispatcher. Go to InService > DNA > DNA WebUI – DMS. 	1. Spectrum PowerCC WebUI opens. 
2. Log in to the Spectrum PowerCC WebUI. 	2. Successfully logged in. 
3. Select "Applications" tab. 	3. The WebUI displays the distribution network applications. 

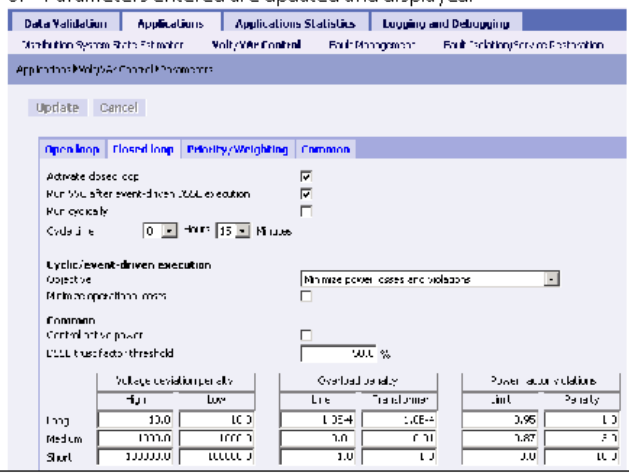

4. Under Volt/VAr Control tab, select Parameters.
Data Validation
Applications
Applications Statistics
Distribution System State Estimator
Volt/VAr Control
Fault Manag
Applications
Open loop
Closed loop
Parameters


4. A new window with parameters to be entered is displayed.

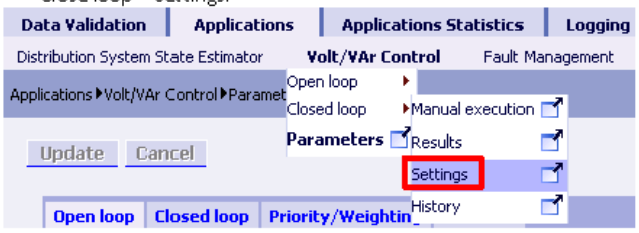
5. Enter the parameters. Press update button.



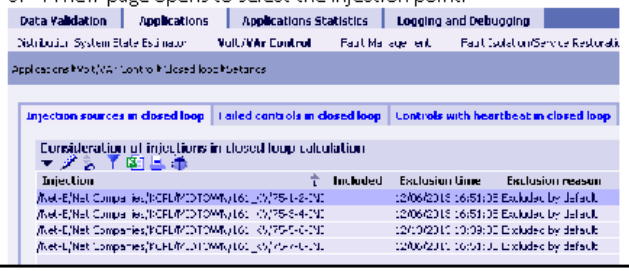
5. Parameters entered are updated and displayed.

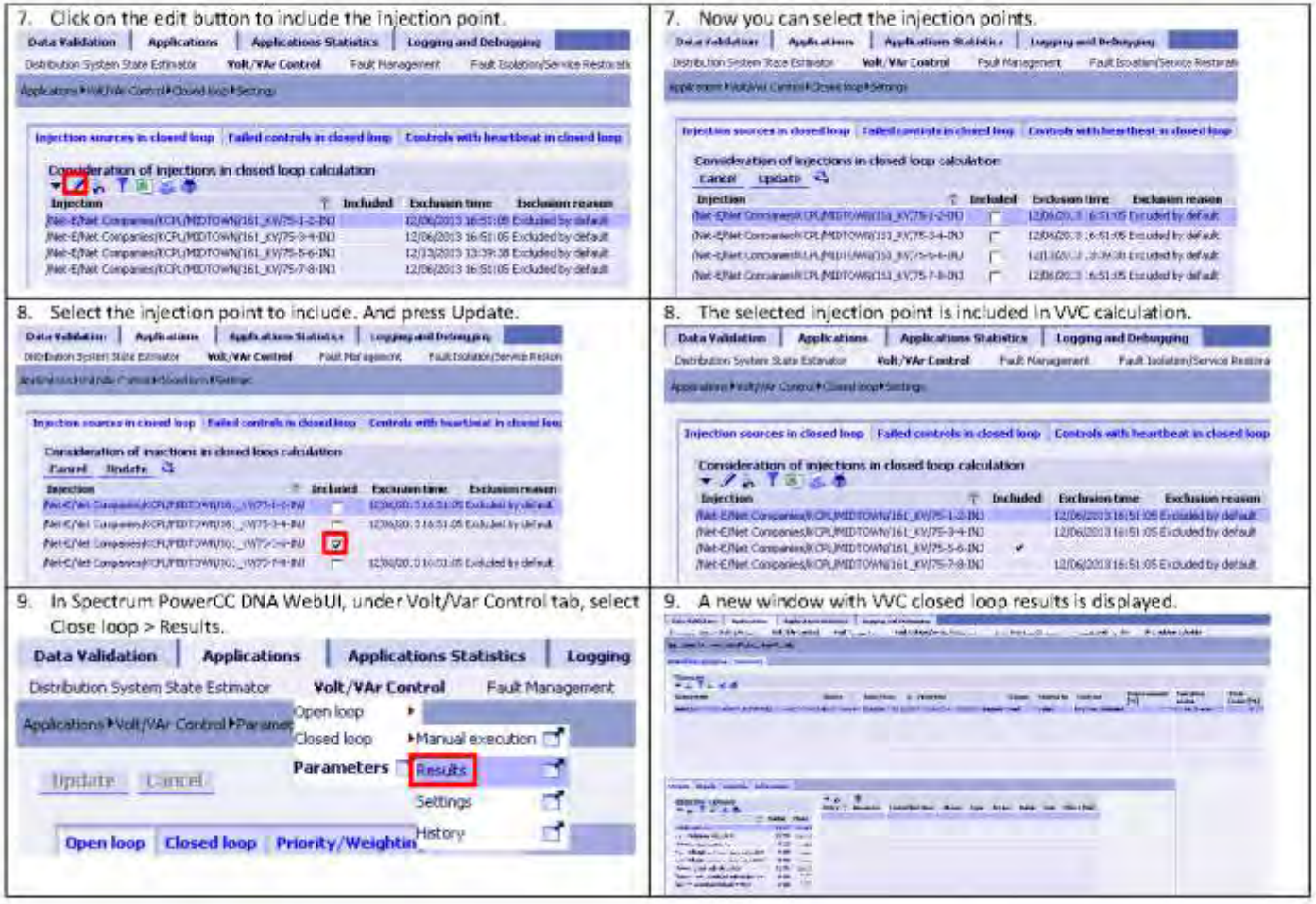


6. In Spectrum PowerCC DNA WebUI, under Volt/Var Control tab, select Close loop > Settings.

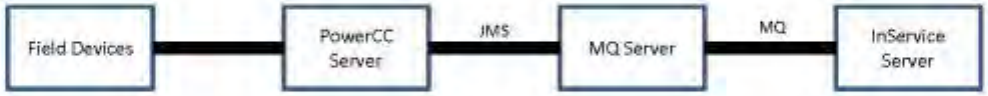


6. A new page opens to select the injection point.



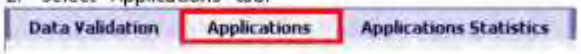

7. Click on the edit button to include the injection point.
Data Validation
Applications
Applications Statistics
Logging and Debugging
Distribution System State Estimator
Volt/VAr Control
Fault Management
Fault Isolation/Service Restorati
Applications ▸ Volt/Var Control ▸ Closed loop ▸ Settings
Injection sources in closed loop
Failed controls in closed loop
Controls with heartbeat in closed loop
Consideration of injections in closed loop calculation
Injection
Included
Exclusion time
Exclusion reason
7. Now you can select the injection points.
Cancel
Update
8. Select the injection point to include. And press Update.
8. The selected injection point is included in VVC calculation.
9. In Spectrum PowerCC DNA WebUI, under Volt/Var Control tab, select Close loop > Results.
Data Validation
Applications
Applications Statistics
Logging
Distribution System State Estimator
Volt/VAr Control
Fault Management
Applications ▸ Volt/VAr Control ▸ Parameter
Open loop
Closed loop
Manual execution
Parameters
Results
Settings
History
Update
Cancel
Open loop
Closed loop
Priority/Weightin
9. A new window with VVC closed loop results is displayed.

1st Responder Function – Feeder Load Transfer



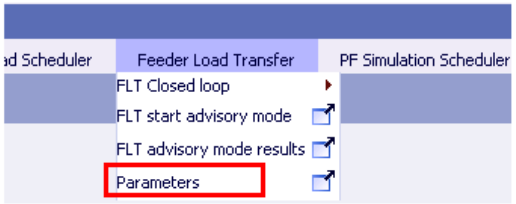
Feeder Load Transfer in Open Loop or Advisory Mode

Pre-Condition: Overload occurs in one of the feeders in the system.

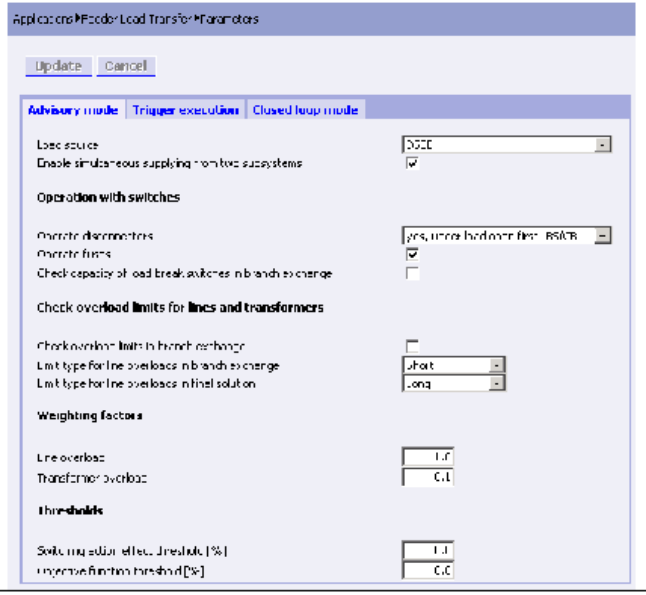
Steps	Expected Results
1. Log in to the Spectrum PowerCC WebUI. 	1. Successfully logged in. 
2. Select "Applications" tab. 	2. WebUI displays the distribution network applications. 

1

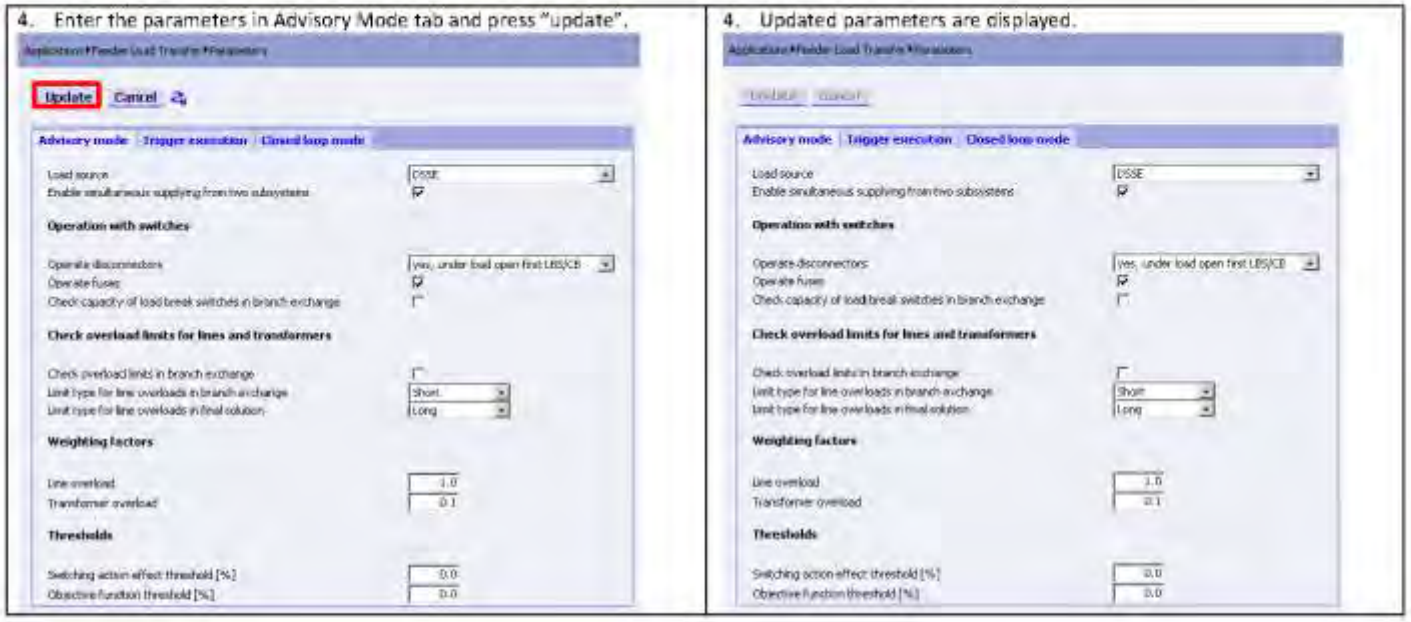
3. Under Feeder Load Transfer tab, select Parameters.



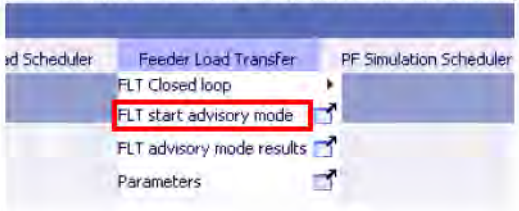
3. A new window with parameters to be entered is displayed.



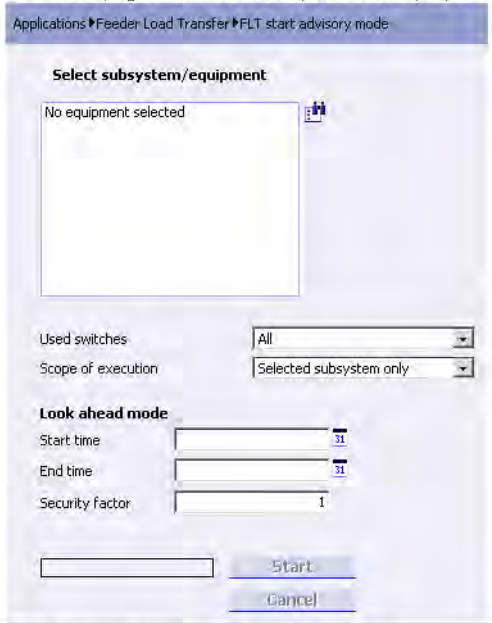
2


4. Enter the parameters in Advisory Mode tab and press "update".
Update
Cancel
Advisory mode
Trigger execution
Closed loop mode
Load source
DSSE
Enable simultaneous supplying from two subsystems
Operation with switches
Operate disconnectors
yes, under load open first LBS/CB
Operate fuses
Check capacity of load break switches in branch exchange
Check overload limits for lines and transformers
Check overload limits in branch exchange
Limit type for line overloads in branch exchange
Short
Limit type for line overloads in final solution
Long
Weighting factors
Line overload
1.0
Transformer overload
0.1
Thresholds
Switching action effect threshold [%]
0.0
Objective function threshold [%]
0.0
4. Updated parameters are displayed.
Advisory mode
Trigger execution
Closed loop mode
Load source
DSSE
Enable simultaneous supplying from two subsystems
Operation with switches
Operate disconnectors
yes, under load open first LBS/CB
Operate fuses
Check capacity of load break switches in branch exchange
Check overload limits for lines and transformers
Check overload limits in branch exchange
Limit type for line overloads in branch exchange
Short
Limit type for line overloads in final solution
Long
Weighting factors
Line overload
1.0
Transformer overload
0.1
Thresholds
Switching action effect threshold [%]
0.0
Objective function threshold [%]
0.0

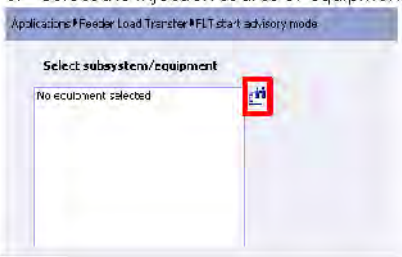
5. Under Feeder Load Transfer, Select FLT start advisory mode



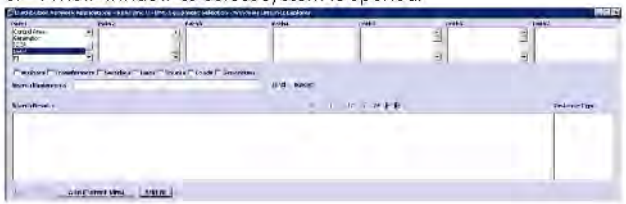
5. A new page FLT start advisory mode is displayed.



6. Select the injection source or equipment.



6. A new window to select system is opened.

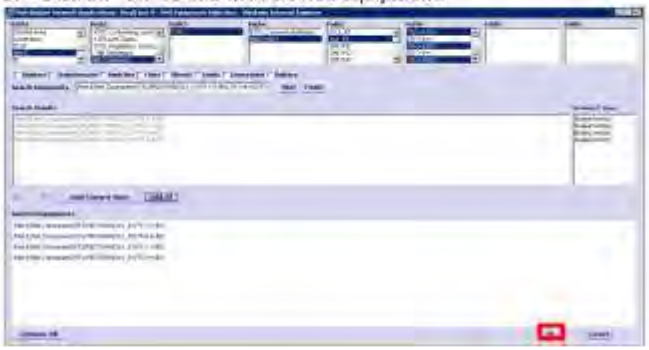


4

7. Select Net E > Net Companies > KCPL > Midtown > 161kV and select Injection points 75-1-2-INJ, 75-3-4-INJ, 75-5-6-INJ and 75-7-8-INJ. Then click "Find". 	7. The Search Results section is populated. 
8. Click "Add All". 	8. The Selected Equipments section is updated with the added equipment. 

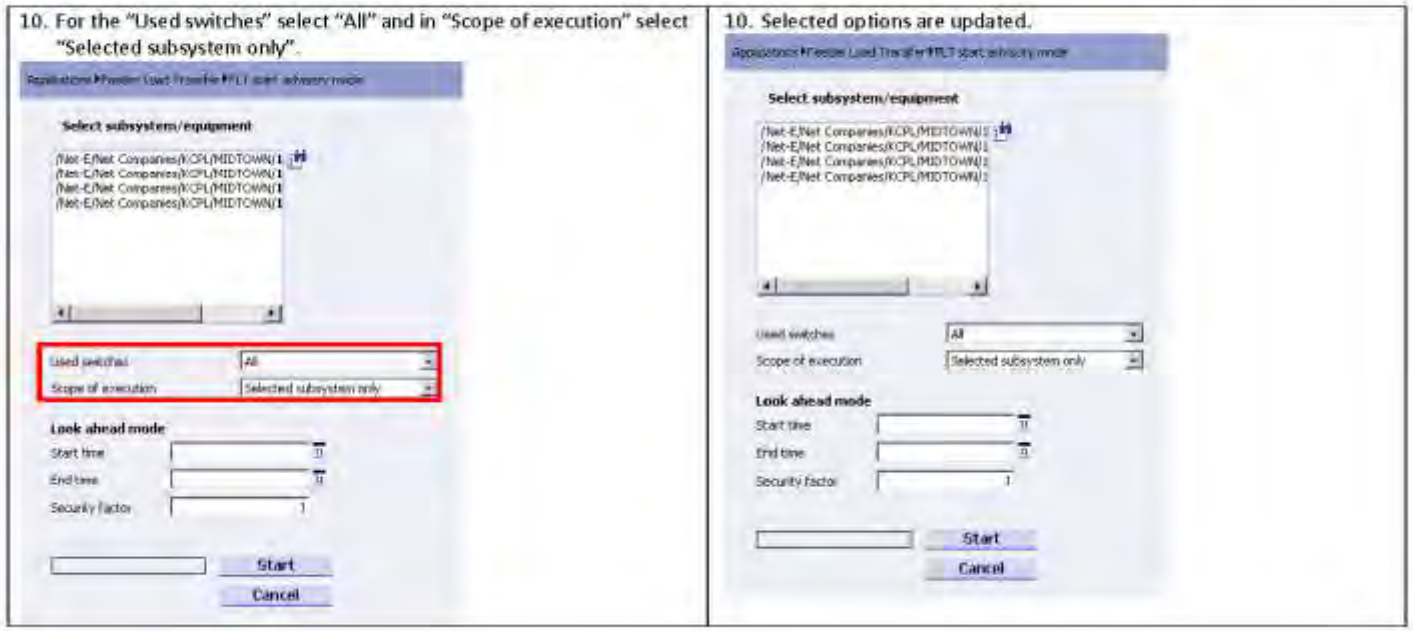
5

9. Click on "Ok" to add the selected equipment.

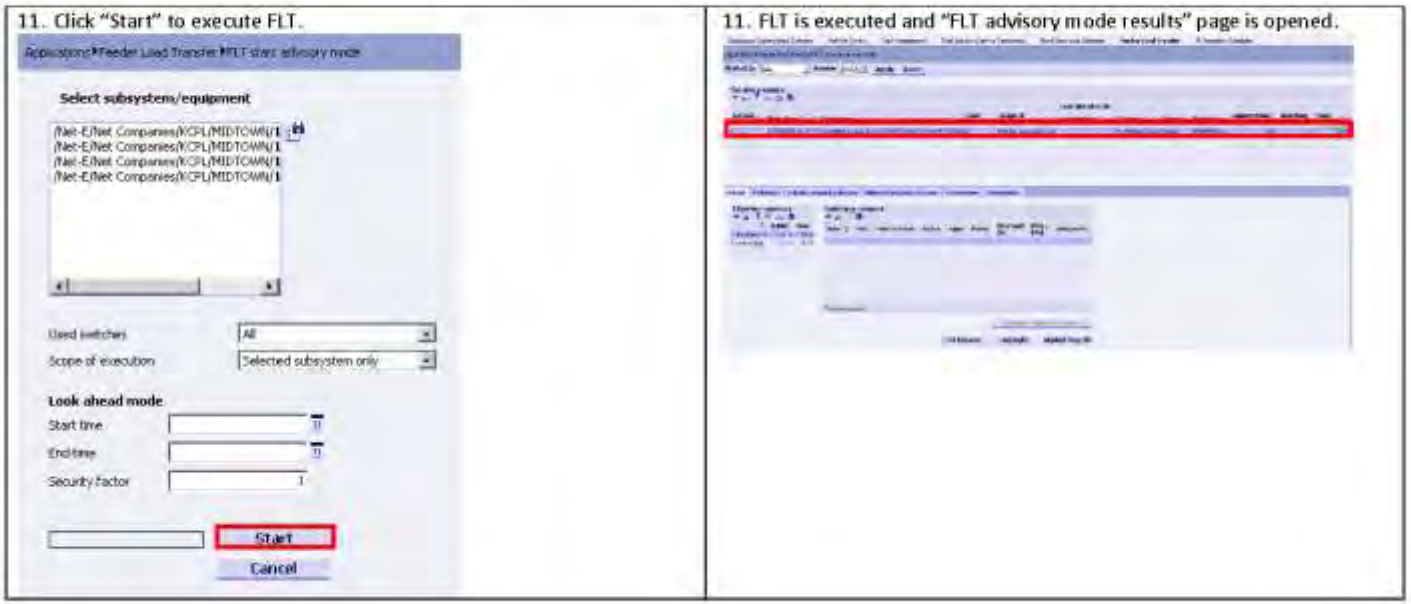


9. The selected injection points are added in the "Select subsystem/equipment" field.

6


10. For the "Used switches" select "All" and in "Scope of execution" select "Selected subsystem only".
Select subsystem/equipment
Look ahead mode
Start time
End time
Security factor
Start
Cancel
10. Selected options are updated.
Select subsystem/equipment
Look ahead mode
Start time
End time
Security factor
Start
Cancel

7


11. Click "Start" to execute FLT.
Select subsystem/equipment
Scope of execution
Selected subsystem only
Look ahead mode
Start time
End time
Security Factor
Start
Cancel
11. FLT is executed and "FLT advisory mode results" page is opened.
8

12. Go to the "Violations" tab to see the violations summary.

12. Any violations, if present are displayed.

13. Go to "Initially opened switches" tab.

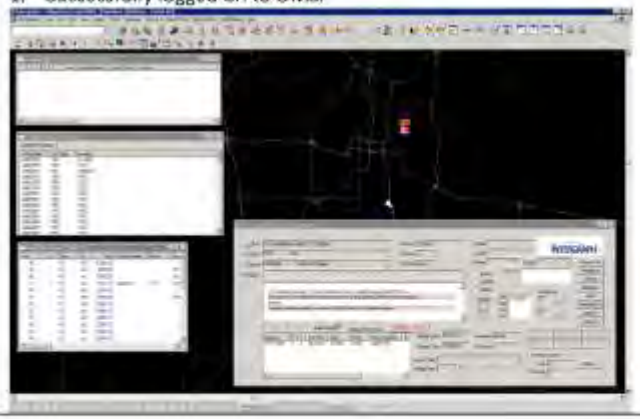
13. Switches used are displayed.

9

1st Responder Function – Fault Location, Isolation and Service Restoration

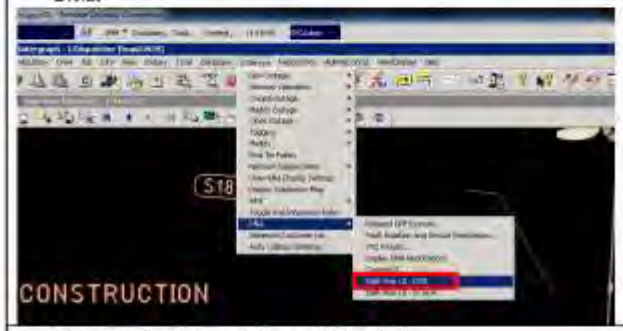
FISR Manual Execution in Open Loop Mode

Pre-Condition: A fault occurs in the system.

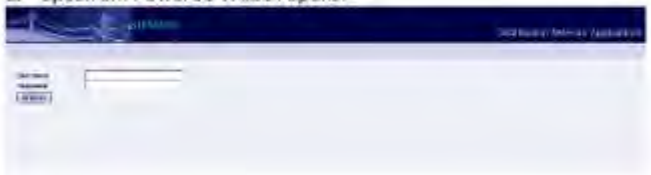
Steps	Expected Results
1. Log in to I/Dispatcher OMS system. 	1. Successfully logged on to OMS. 

1

2. Start WebUI from IDispatcher. Go to InService > DNA > DNA WebUI – DMS.



2. Spectrum PowerCC WebUI opens.



3. Log in to the Spectrum PowerCC WebUI.

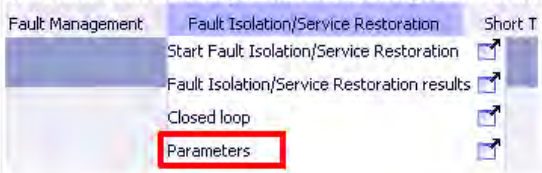
3. Successfully logged in.

4. Select "Applications" tab.

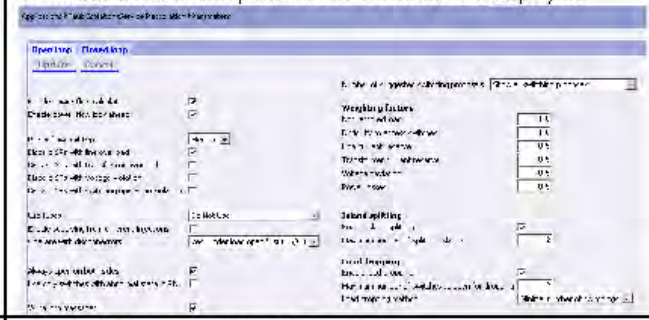
4. WebUI displays the distribution network applications.

2

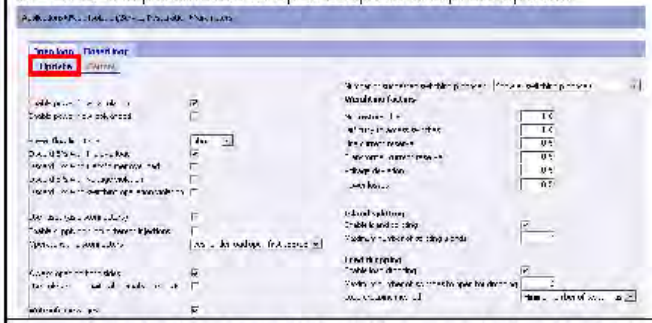
5. Under Fault Isolation/Service Restoration, select Parameters.



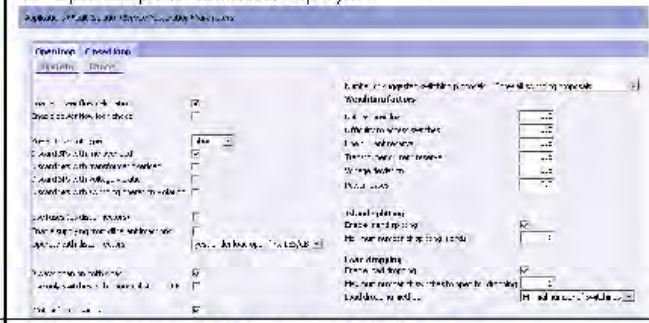
5. A new window with parameters to be entered is displayed.



6. Enter the parameters in Open Loop tab and press update.



6. Updated parameters are displayed.

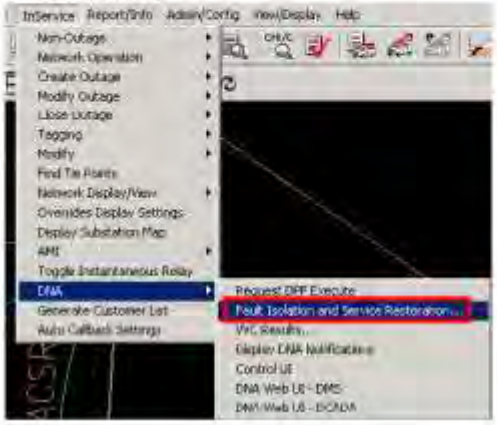


7. Go to Applications tab and in Fault Management tab, select Faults Overview.

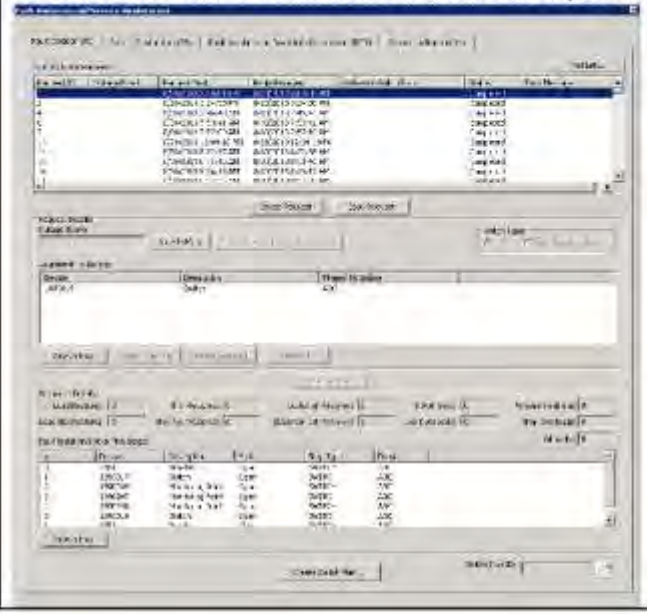
7. A page opens with the latest faults in the system.

3

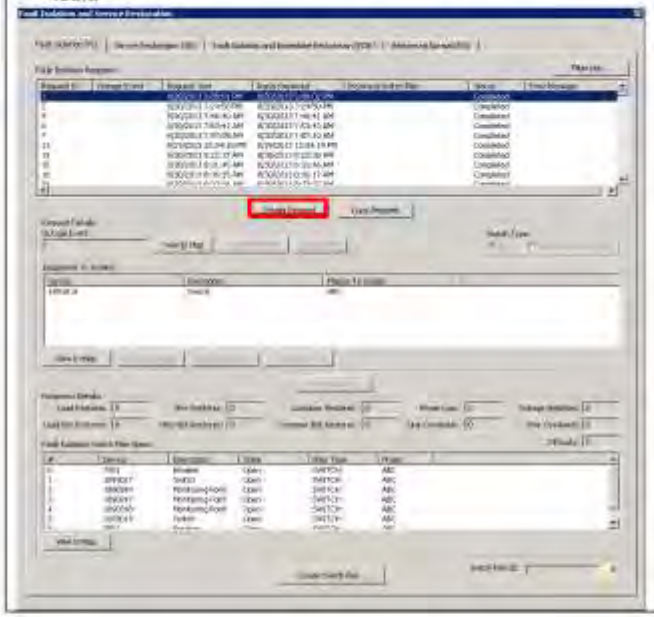
8. In I/Dispatcher, go to InService > DNA > Fault Isolation and Service Restoration.



8. A new window Fault Isolation and Service Restoration is opened.



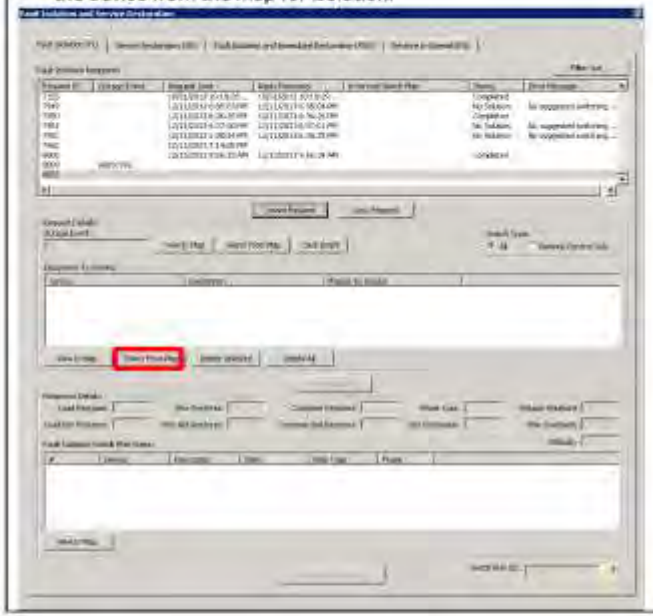
9. Select the Fault Isolation tab. Click Create Request to isolate the fault.



9. A new line is created in the Fault Isolation Requests section.

5

10. In the Equipment to Isolation section, click Select from Map to select the device from the map for isolation.

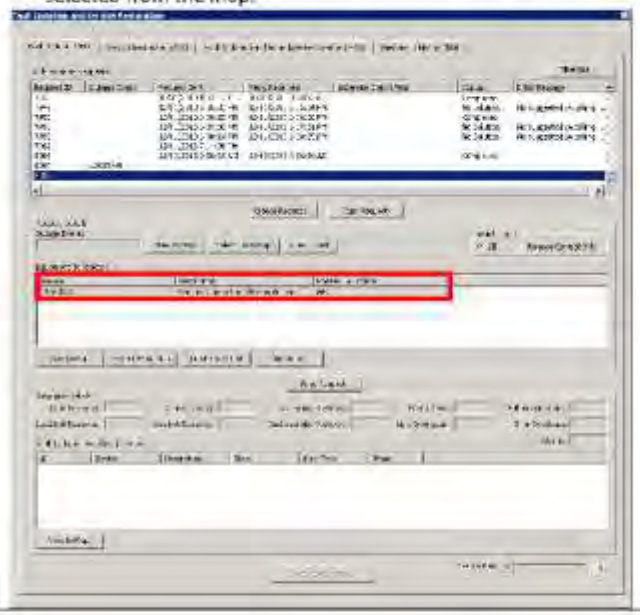


10. In i/Dispatcher map, select the equipment to isolate.

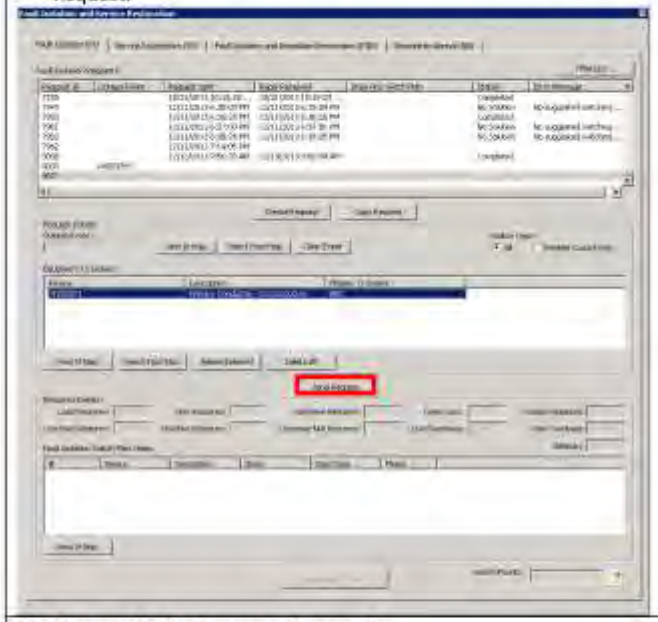
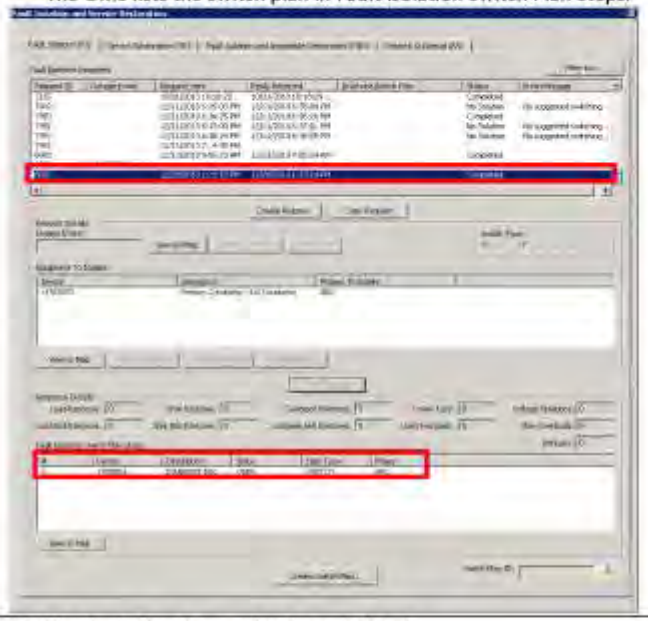
6

11. Double click the device/line from the map.

11. The Equipment to Isolate section is populated with the device selected from the map.



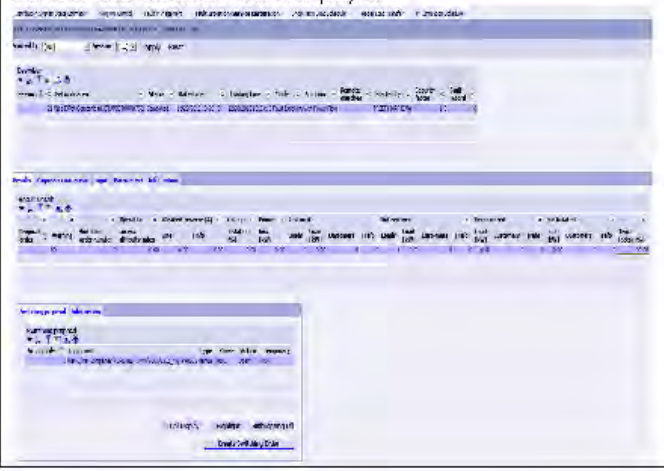
7

12. Select the device in Equipment to Isolate section and click Send Request. 	12. The Fault Isolation Requests section is updated with the information. The OMS lists the switch plan in Fault Isolation Switch Plan Steps. 
13. The switch plan is executed manually.	13. The device/equipment has been isolated.

8

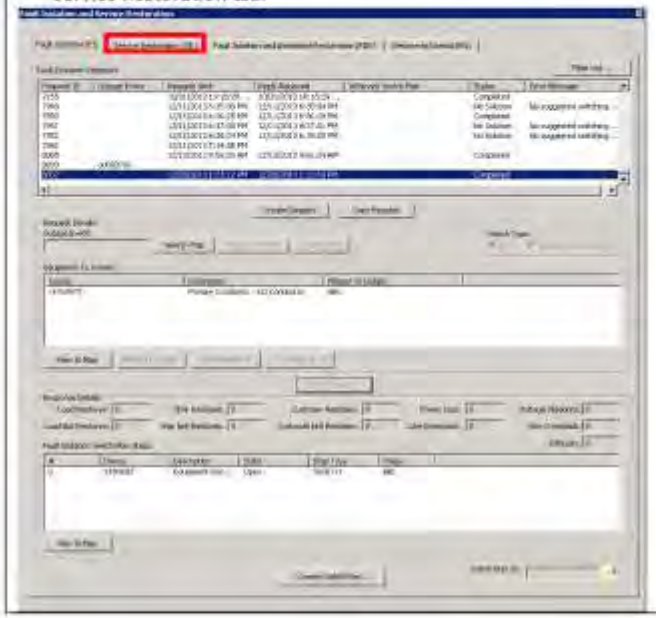
14. In the PowerCC DNA, go to Fault Isolation/Service Restoration > Fault Isolation/Service Restoration Results.

14. The Fault Isolation result is displayed.

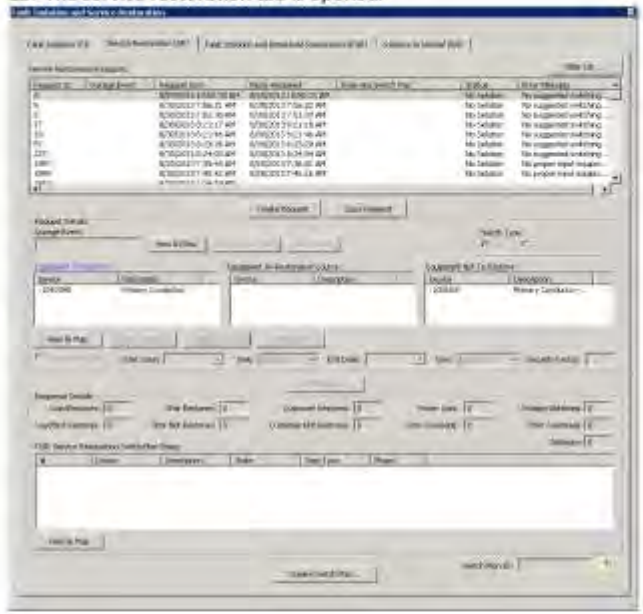


9

15. In the Fault Isolation and Service Restoration window, go to the Service Restoration tab.

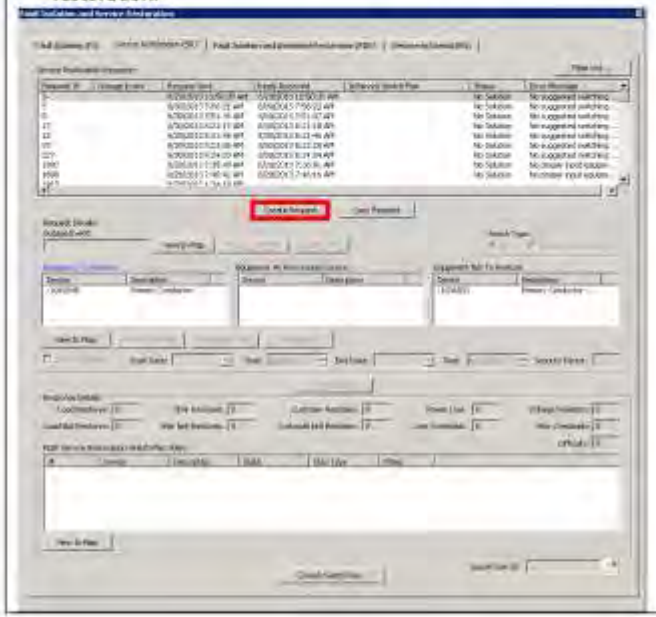


15. The service restoration tab is opened.

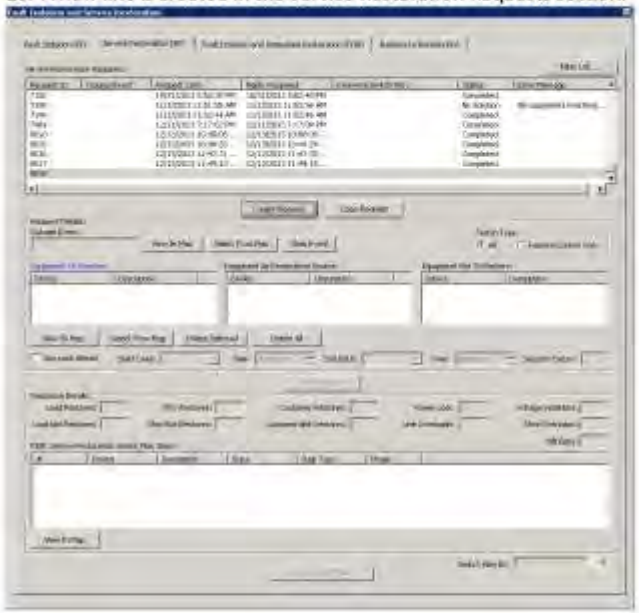


10

16. In the Service Restoration Requests, press Create Request for service restoration.

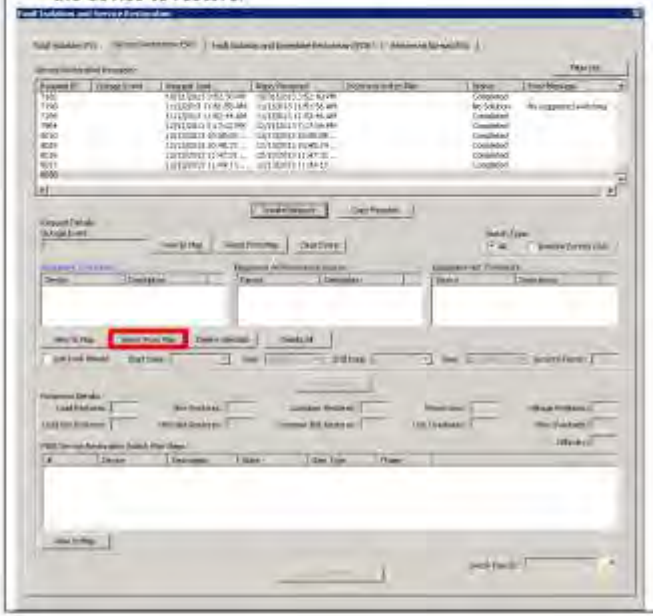


16. A new line is created in the Service Restoration Requests section.



11

17. In the Equipment to Restore section, click Select from Map to select the device to restore.

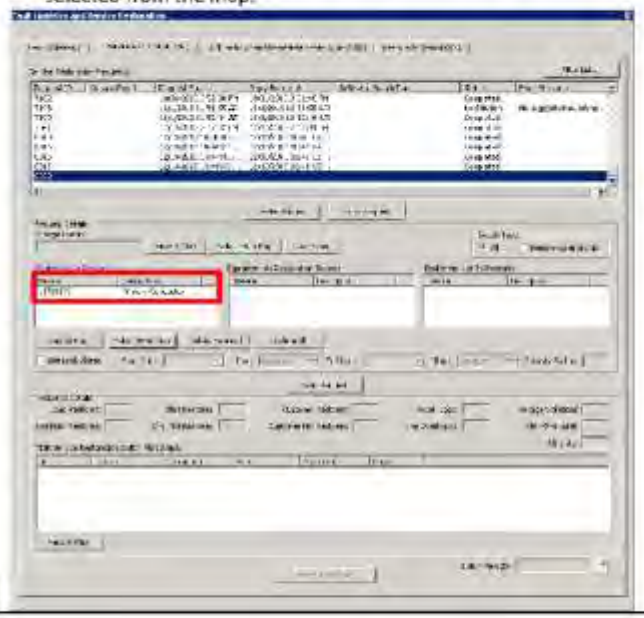


17. In I/Dispatcher map select the device to be restored.

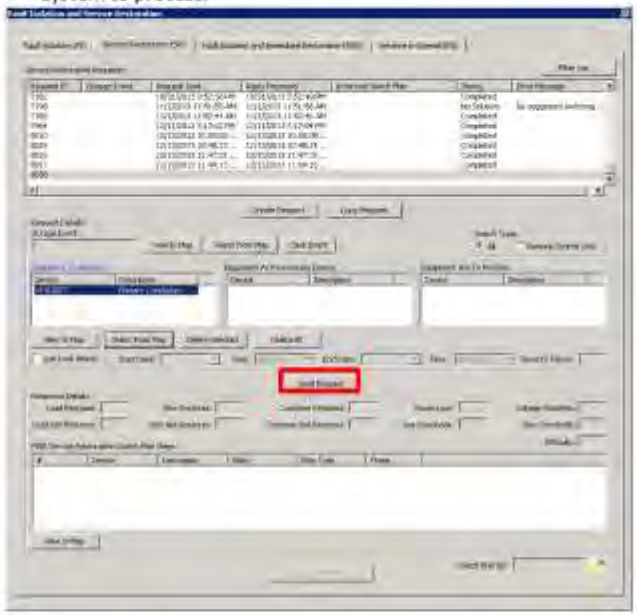
12

18. Double click the device/line from the map.

18. The equipment to restore section is populated with the device selected from the map.



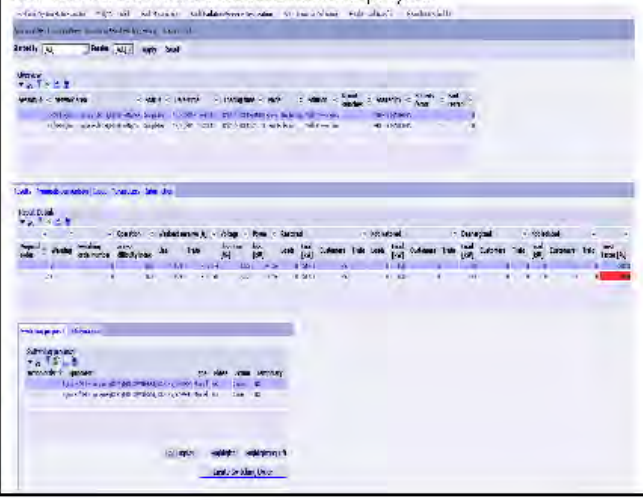
13

19. Select the device selected to restore and click Send Request for the system to process. 	19. The Service Restoration Requests is filled with the information and status "Completed". It lists the switch plan in Service Restoration Switch Plan Steps. 
20. The Service Restoration switch plan is executed manually.	20. Service is restored to the devices.

14

21. In the PowerCC DNA, go to Fault Isolation/Service Restoration > Fault Isolation/Service Restoration Results.

21. The Service Restoration result is displayed.



15

Outage and Restoration Events

Outage event

Precondition: MFR within SmartMeter detects a sustained voltage loss for more than 30 seconds and generates an outage event.

Meter ID: 1284810711062

Steps	Expected Results
1. SmartMeter loses power for more than 30 seconds.	1. Meter doesn't have power.
2. Log in to Gridstream Command Center to verify that meter has sent outage event to AHE. 	2. Successfully logged in to the Gridstream Command Center. 

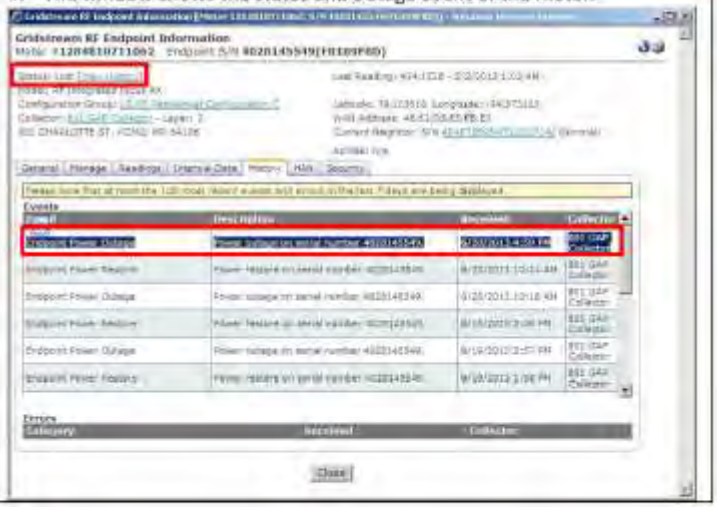
1

3. In the Search box, type in the meter ID 1284810711062.

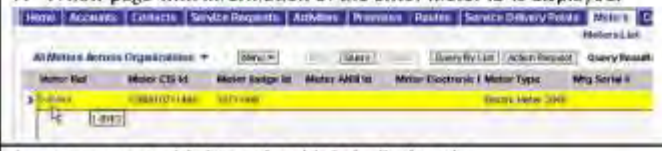
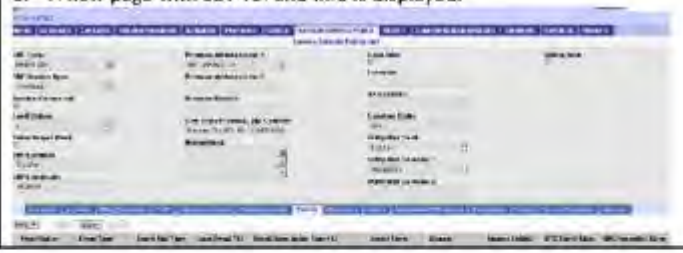
3. A new page opens with Gridstream RF Endpoint Information of the meter ID.

4. Click on the "History" tab to view the outages.

4. The window shows the status and outage event of the meter.



2

5. Log in to the MDM. 	5. Successful log in to the system. 
6. Select the "Meters" tab to search for Meter ID. 	6. A new page is opened to enter the Meter ID. 
7. Enter the meter ID 1284810711062 in Meter CIS Id column. 	7. A new page with information of the enter meter ID is displayed. 
8. Select the Service Delivery Points tab. 	8. A new page with SDP ref and info is displayed. 

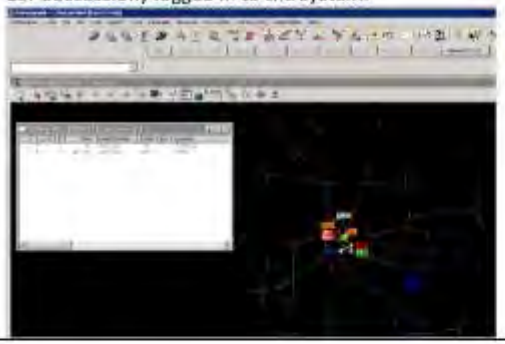
3

9. Select the events tab.

9. A new page with meter outage event in the entered meter ID is displayed.

10. Log in to IDispatcher OMS system.

10. Successfully logged in to the system.

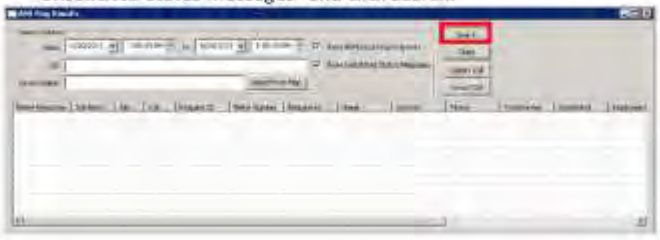


4

11. Select InService > AMI > AMI Ping Results to view any outages.

11. AMI Ping Results window pops open.

12. Select "Show all Manual Ping Request and Outages" and "Show Unsolicited Status Messages" and click search.



12. Outages between the selected date and time are displayed.

5

Restoration Event

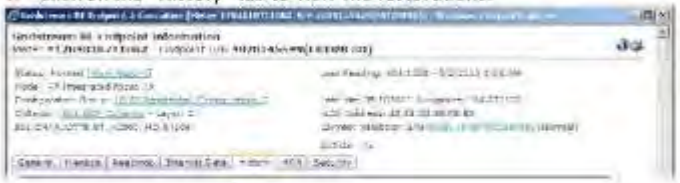
Precondition: MFR within SmartMeter detects a power restoration event following an outage and generates a restoration event.

Meter ID: 1284810711062

Steps	Expected Results
1. SmartMeter restores power.	1. Meter has power restored to it.
2. Log in to Gridstream Command Center to verify that meter has sent restoration event to AHE. 	2. Successfully logged in to the Gridstream Command Center. 
3. In the Search box, type in the meter ID 1284810711062. 	3. A new page opens with Gridstream RF Endpoint Information of the meter ID. 

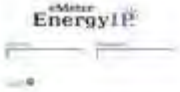
6

4. Click on the "History" tab to view the restorations.



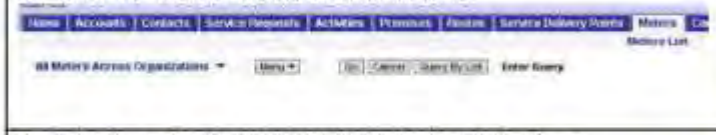
4. The window shows the status and restoration event of the meter.

5. Log in to the MDM.



5. Successful log in to the system.

6. Select the "Meters" tab to search for Meter ID.



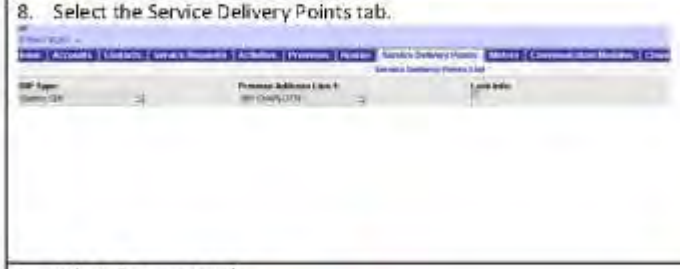
6. A new page is opened to enter the Meter ID.

7. Enter the meter ID 1284810711062 in Meter CIS Id column.

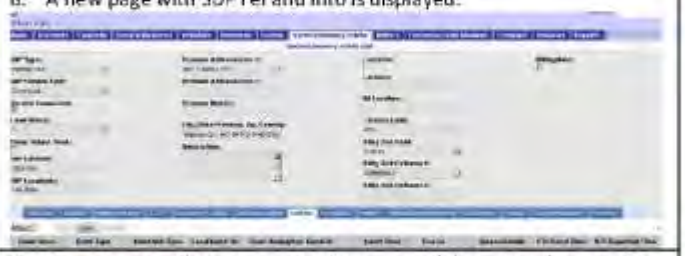
7. A new page with information of the enter meter ID is displayed.

7

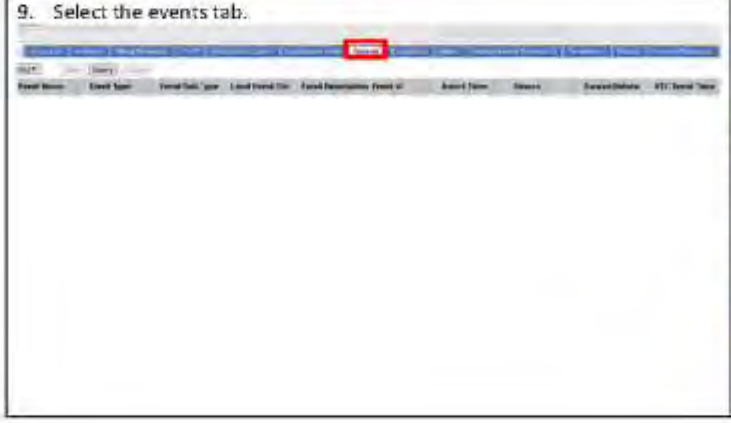
8. Select the Service Delivery Points tab.



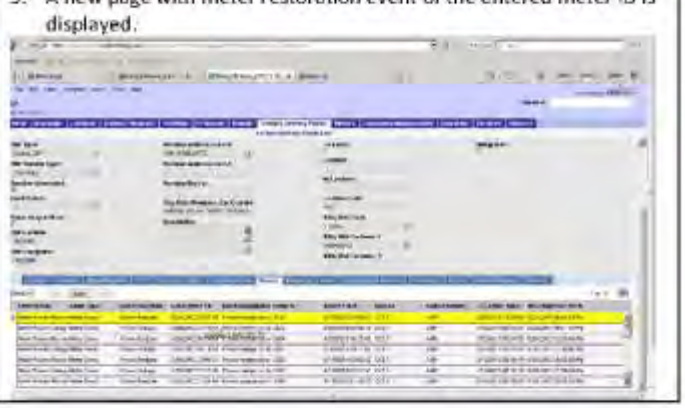
8. A new page with SDP ref and info is displayed.



9. Select the events tab.



9. A new page with meter restoration event of the entered meter ID is displayed.

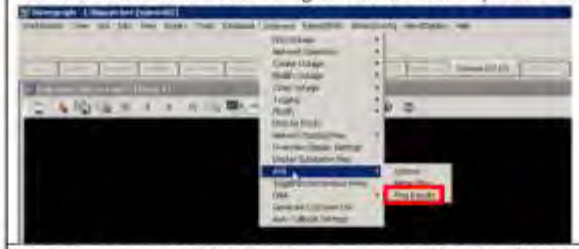


8

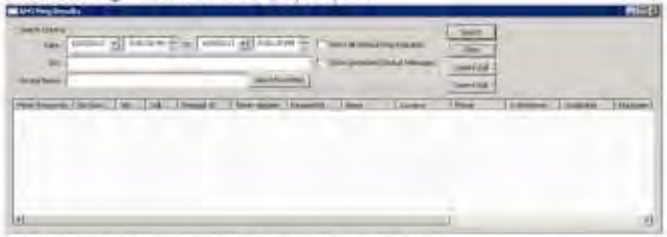
10. Log in to IDispatcher OMS System.

10. Successfully logged in to OMS system.

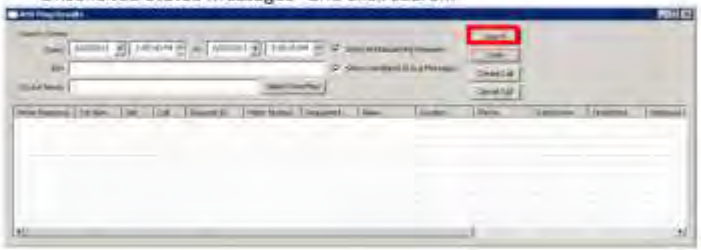
11. Select InService > AMI > Ping Results to view any restorations.



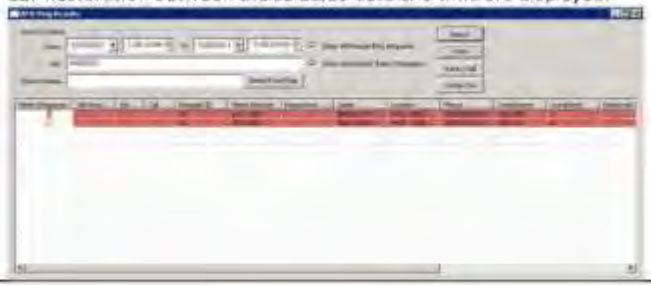
11. AMI Ping Results window pops open.



12. Select "Show all Manual Ping Request and Outages" and "Show Unsolicited Status Messages" and click search.

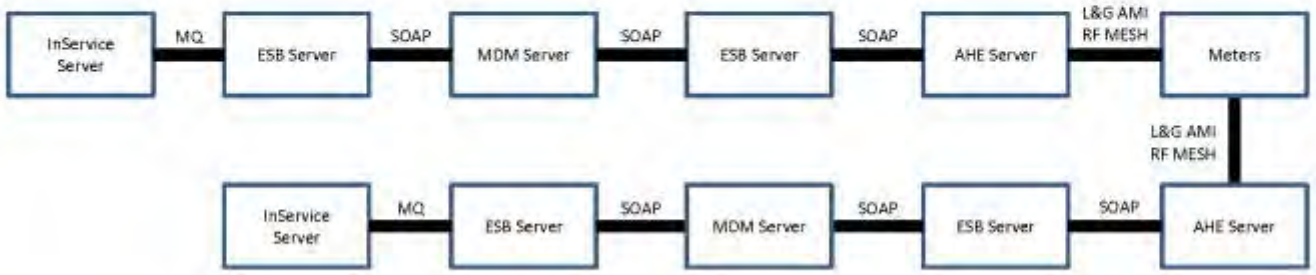


12. Restoration between the selected date and time are displayed.

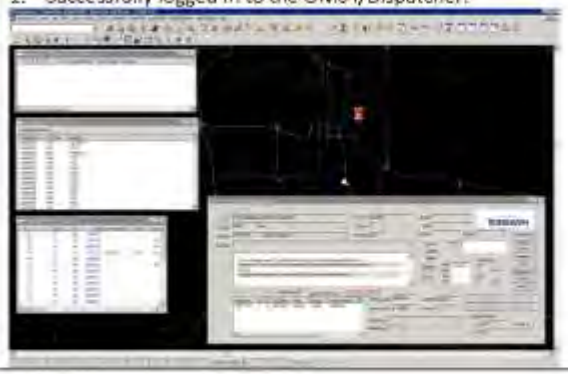


9

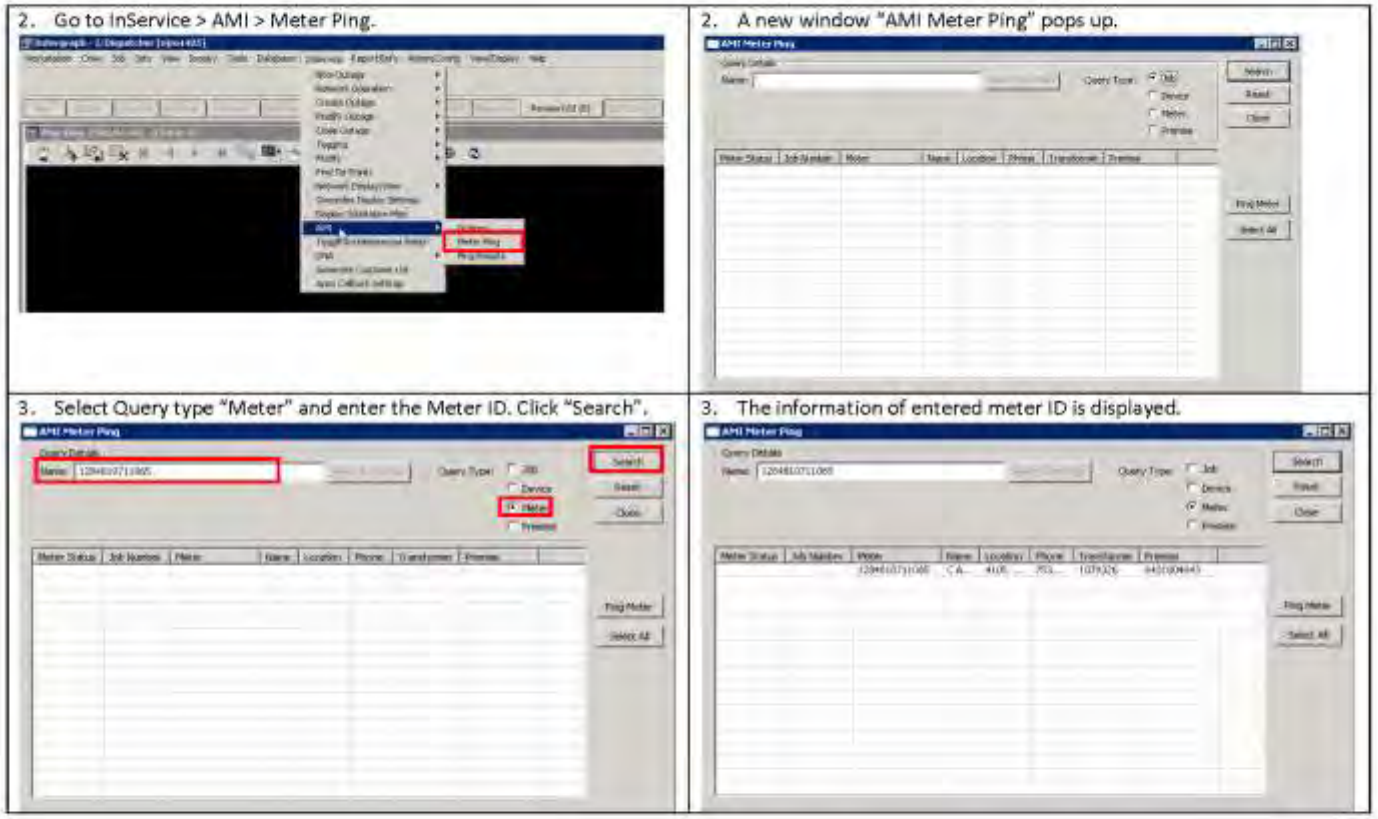
Power Status Verification



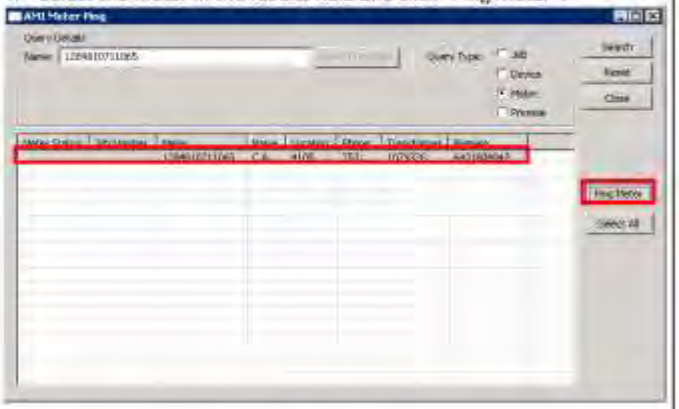
Power Status Verification

Steps	Expected Results
1. Log in to the OMS I/Dispatcher. 	1. Successfully logged in to the OMS I/Dispatcher. 

1


2. Go to InService > AMI > Meter Ping.
2. A new window "AMI Meter Ping" pops up.
3. Select Query type "Meter" and enter the Meter ID. Click "Search",
3. The information of entered meter ID is displayed.
2

4. Select the meter in the results field and click "Ping Meter".



4. The meter ping request is sent to meter via MDM/AHE.

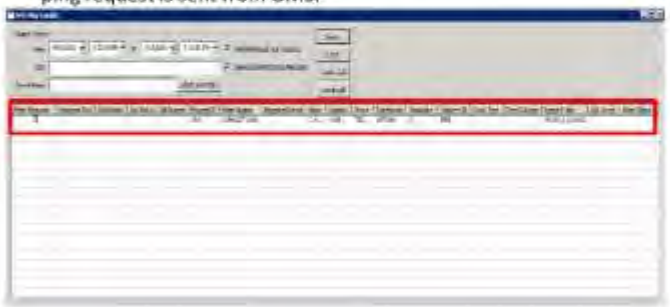
5. Go to InService > AMI > Ping Results.

5. AMI Ping Results window is opened.

3

6. Select the Date and Time and check "Show All Manual Ping Request" and "Show Unsolicited Status Messages" and click Search.

6. The Meter Ping Request is displayed in the AMI Ping Results window. The "Hour Glass" in Meter Response column represents that meter ping request is sent from OMS.



7. Log in to MDM to check Power Status Verification.

7. Successfully logged in to the MDM.

4

8. Select the "Meters" tab and enter meter number 1284810711065 in Meter CIS id column. Click "Go" to execute the query.

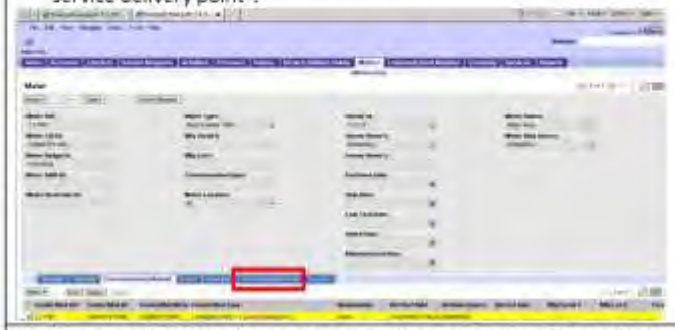
8. The page refreshes with information of the enter meter ID is displayed.

9. Click on the Meter Ref. This selects the meter.

9. The page displays the detailed information on that meter.

5

10. Select the "Service Delivery Points" tab. This is the "Meter level service delivery point".



10. The page displays the SDP ID of the entered meter number.

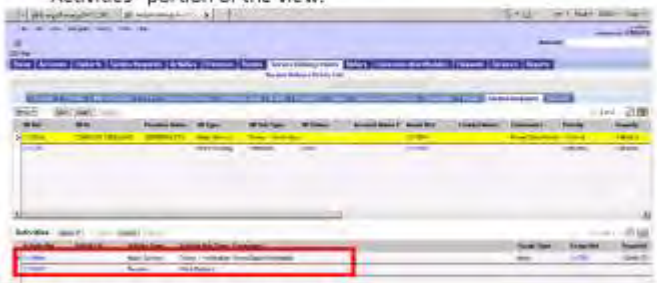
11. Select the SDP Ref of the meter to navigate to Service Delivery Points List.

11. The SDP info of the entered meter is displayed.

6

12. Select the "Service Requests" tab.

12. This displays the PSV request with the transaction level details in the "Activities" portion of the view.



13. Log in to AHE Command Center.

13. Successfully logged in to the AHE.

7

14. Search the meter number 1284810711065.

14. Meter search displays the information.

15. Select the "Manage" tab.

15. The Manage tab displays the meter ping request received from MDM.

8

16. AHE receives the meter ping request and sends the request to meter. Press "refresh" button.

16. The meter ping request is sent to meter.

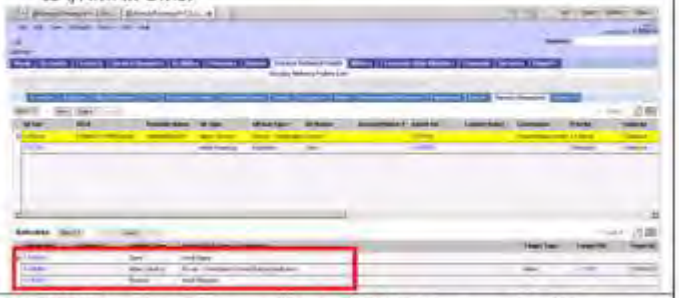
17. AHE receives the meter ping response from meter. Press "refresh" button.

17. AHE sends meter ping response from meter to MDM.

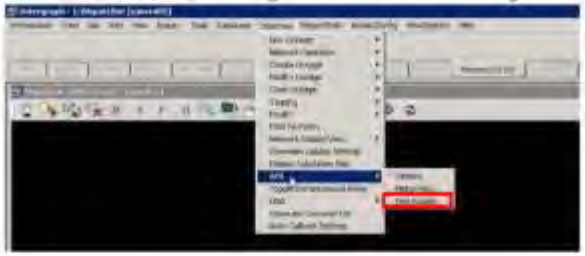
9

18. In the MDM, navigate to Service Delivery Points > Service Requests.

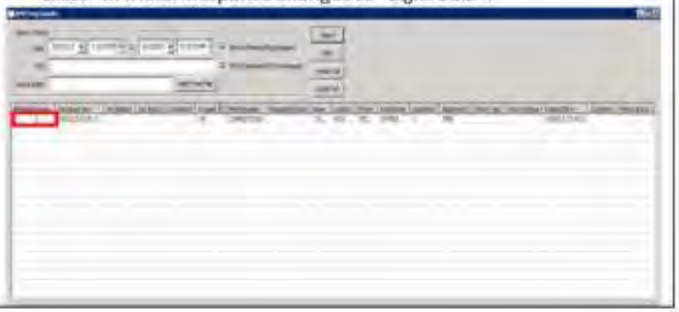
18. The PSV message received from AHE is processed by MDM and sent to I/AMI in OMS.



19. In the OMS I/Dispatcher, go to InService > AMI > Ping Results.



19. "AMI Ping Results" is populated with Ping Response, the "Hour Glass" in Meter Response changes to "Light Bulb".



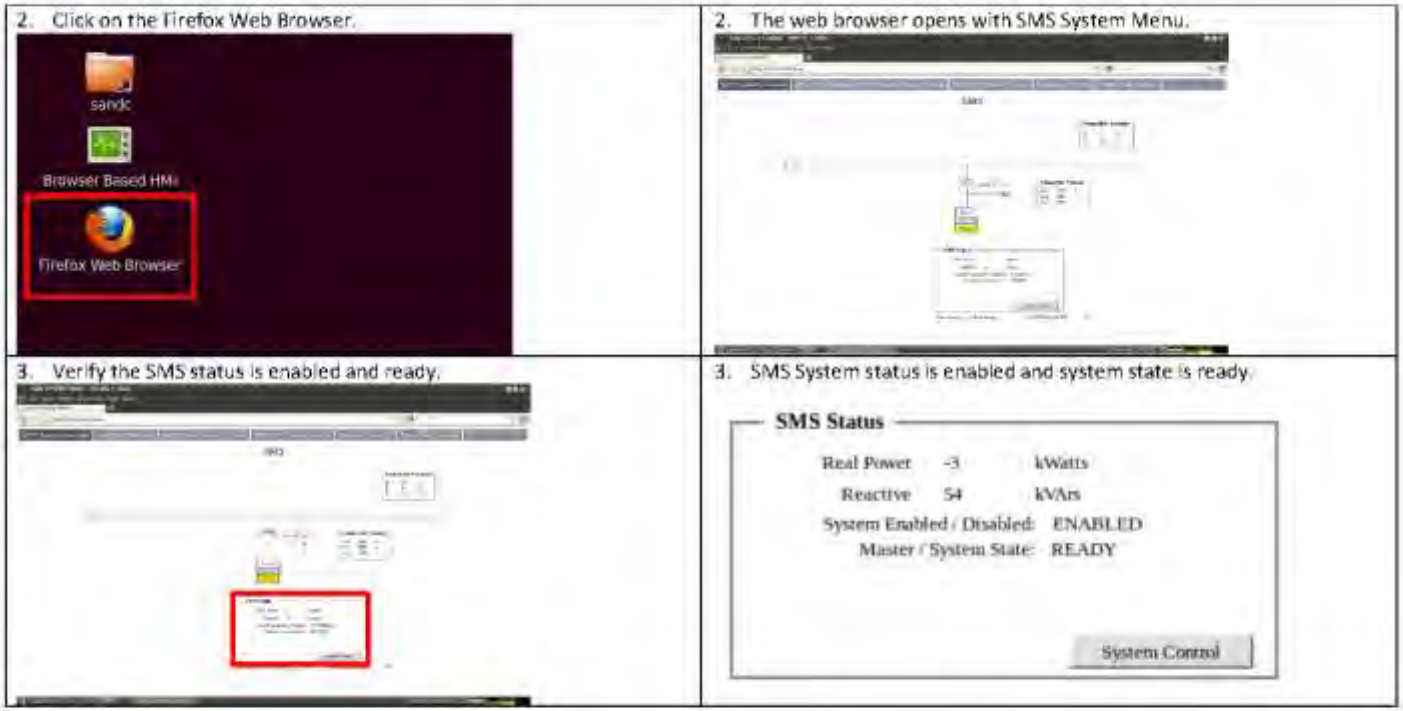
10

Battery Grid Operation – Local Control (Discharge)

Local Control – Battery Discharging in Power Mode

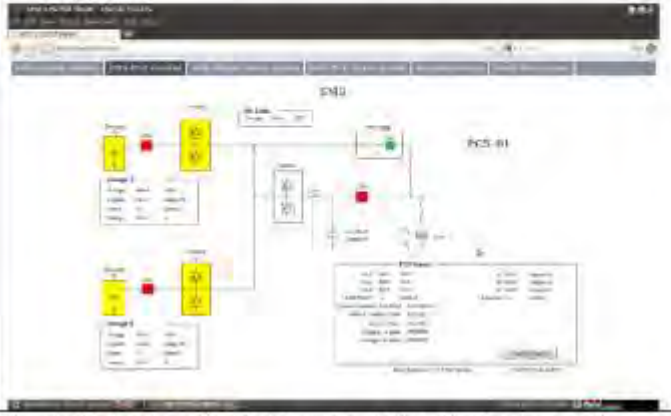
Precondition: Battery is fully charged.

Steps	Expected Results
1. Log in to the S&C SMS for battery. 	1. Successfully logged in to the system. 

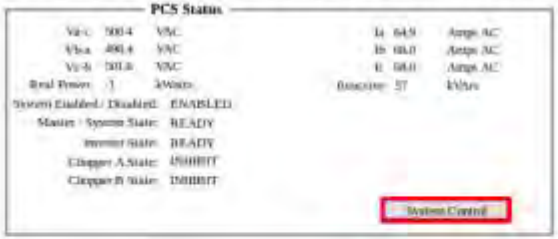

2. Click on the Firefox Web Browser.
sandc
Browser Based HMI
Firefox Web Browser
2. The web browser opens with SMS System Menu.
3. Verify the SMS status is enabled and ready.
3. SMS System status is enabled and system state is ready.
SMS Status
Real Power -3 kWatts
Reactive 54 kVArs
System Enabled / Disabled: ENABLED
Master / System State: READY
System Control

4. Click on the SMS PCS Oneline tab.

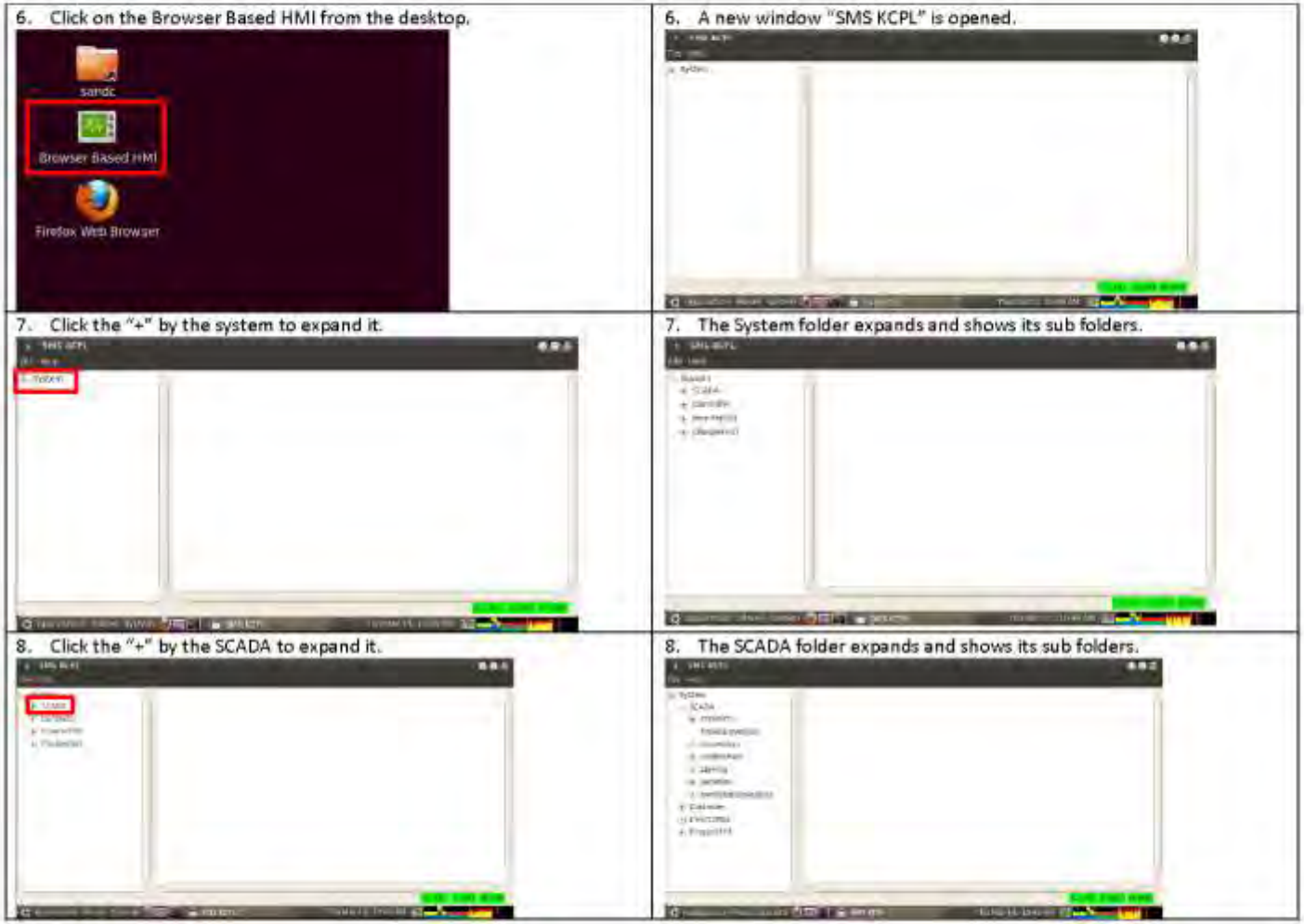
4. SMS PCS Oneline page opens with a single line diagram of the battery connection.



5. Click on the System Control to verify the system control.



5. The System is verified to be running in "Local" mode in normal condition.


6. Click on the Browser Based HMI from the desktop.
sandc
Browser Based HMI
Firefox Web Browser
6. A new window "SMS KCPL" is opened.
7. Click the "+" by the system to expand it.
7. The System folder expands and shows its sub folders.
8. Click the "+" by the SCADA to expand it.
8. The SCADA folder expands and shows its sub folders.

9. Click the "+" by the NonVolatileVariables to expand it.

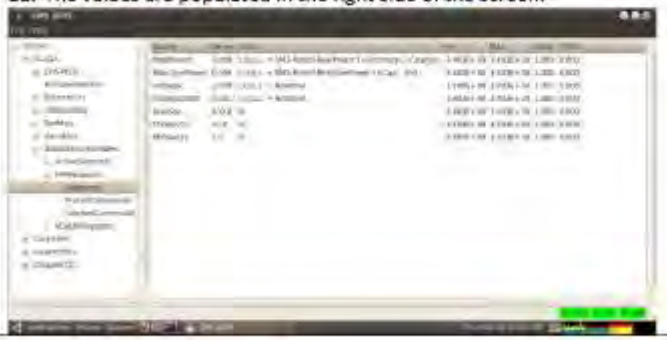
9. The NonVolatileVariables folder expands and shows its sub folders.

10. Click the "+" by the HMIRequests to expand it.

10. The HMIRequests folder expands and shows its sub folders.

11. Click on the Setpoints.

11. The values are populated in the right side of the screen.



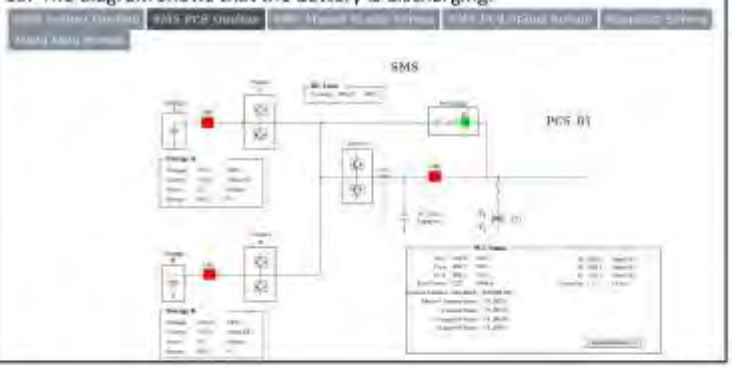

12. Select value column of the "RealPower".
12. A pointer appears in the value column to change the value.
13. In the "Value" column of the "RealPower", enter "1" for discharge.
13. A window pops up to confirm the change.

14. Press "Ok" to confirm the changes.

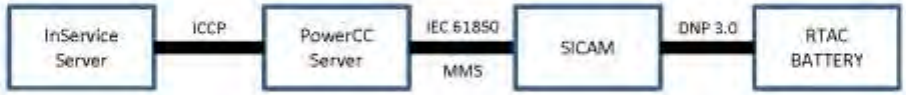
14. The Battery starts to discharge.

15. Open web browser opens with SMS System Menu.

15. The diagram shows that the battery is discharging.

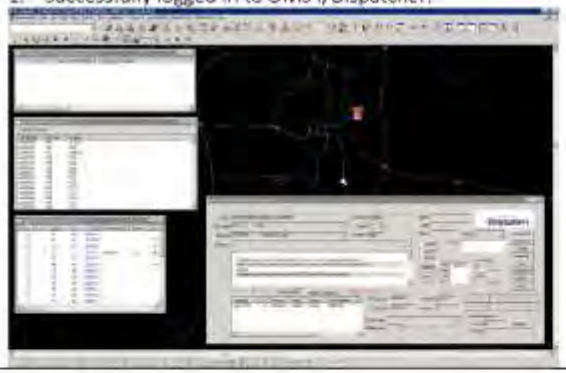


Battery Grid Operation – Fixed kW (Discharge)

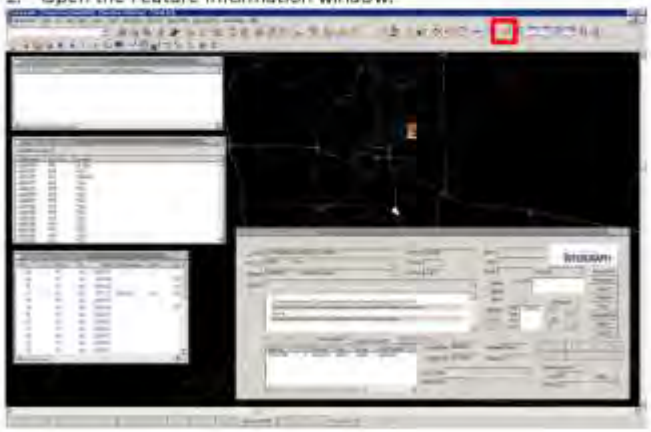


Fixed kW – Battery Discharging in Power Mode

Precondition: Battery is fully charged.

Steps	Expected Results
1. Log in to OMS I/Dispatcher. 	1. Successfully logged in to OMS I/Dispatcher. 

2. Open the Feature Information window.

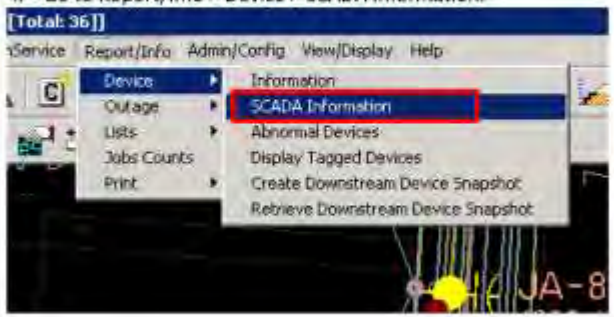


2. A new window is opened.

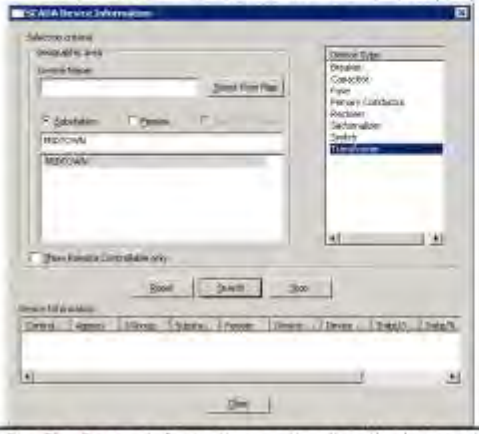
3. In the Feature Information window, enter the battery UODID (1888105).

3. The feature information displays the SCADA value for battery.

4. Go to Report/Info > Device > SCADA Information.



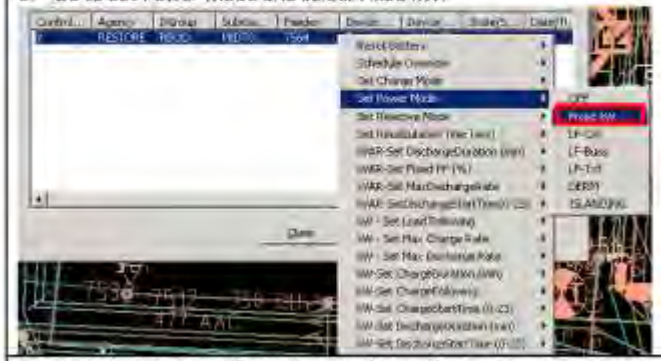
4. A new window "SCADA Device Information (SDI)" is opened.



5. In the Device Name, type the UODID of battery. Select Midtown as substation and in Device Type, select transformer and press Search.

5. The Device Information section lists the battery information.

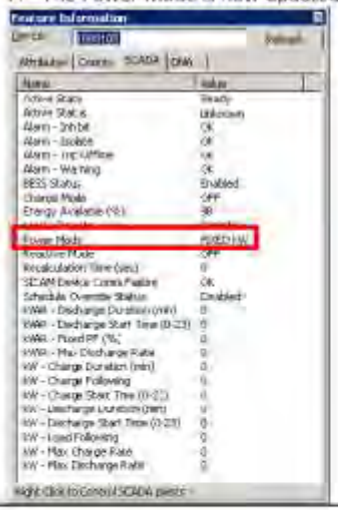
6. Go to Set Power Mode and select Fixed kW.



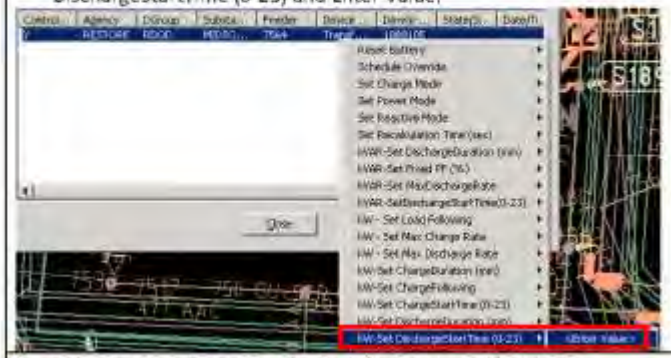
6. The Battery is now set to Fixed kW Discharge mode

7. Open the Feature Information window and note that the Power Mode is "OFF". Click Refresh to update the Power Mode to Fixed kW.

7. The Power Mode is now updated to "Fixed kW".

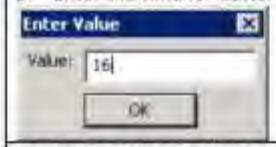


8. Open SDI and right click the battery. Select kW-Set DischargeStartTime (0-23) and Enter Value.



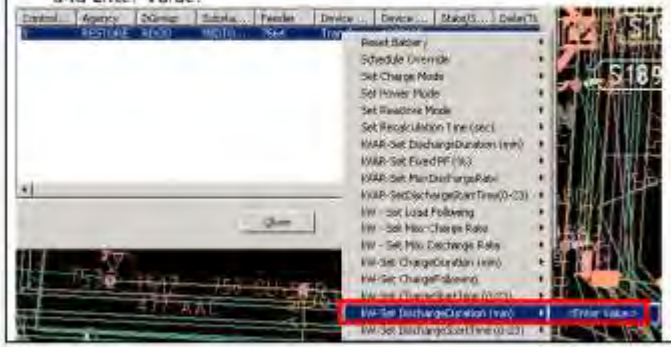
8. A window pops up to enter the value.

9. Enter the time for battery to start discharging and click OK.

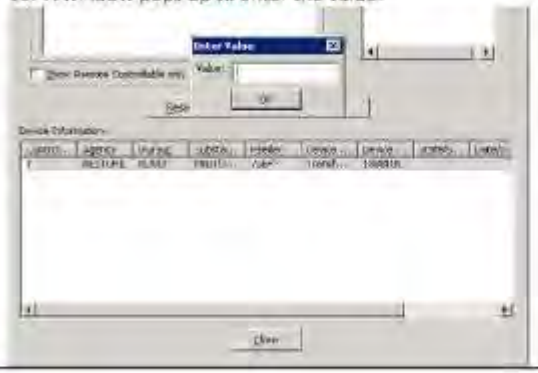


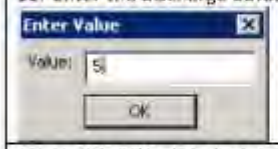
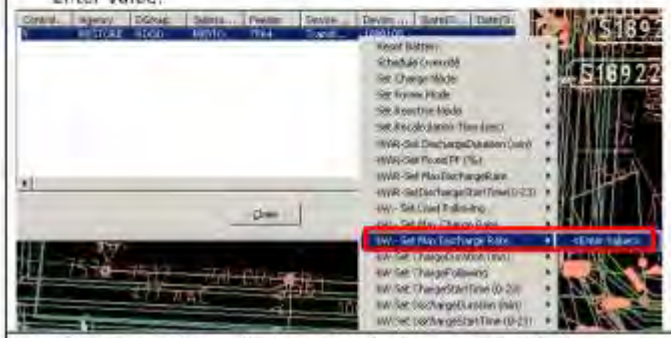
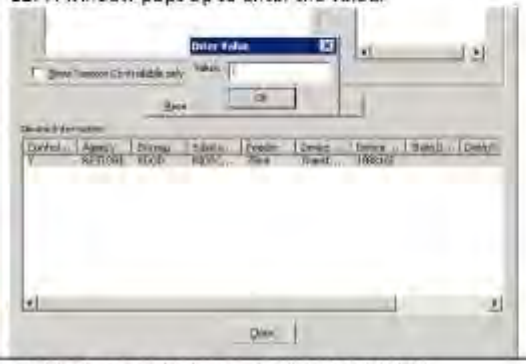
9. The battery discharge time is set to 16:00.

10. In SDI, right click the battery. Select kW-Set DischargeDuration (min) and Enter Value.



10. A window pops up to enter the value.



11. Enter the discharge duration for battery and click OK. 	11. The battery discharge duration is set to 5 minutes.
12. In SDI, right click the battery. Select kW-Set Max Discharge Rate and Enter Value. 	12. A window pops up to enter the value. 
13. Enter the maximum discharge rate for battery and click OK. 	13. The battery discharge rate is set to 800kW.

14. Open the feature information window and verify that the values entered above are reflected in the SCADA tab. Press Refresh.

14. Note that the kW – Discharge Duration is 5 min, kW – Discharge time is 16:00 and kW – Max Discharge Rate is 800kW.

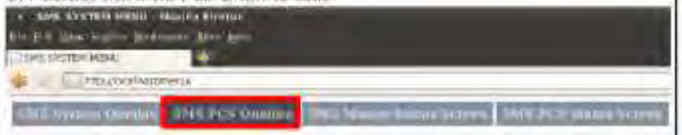
15. Log in to the S&C SMS for battery.

15. Successfully logged in to the system.

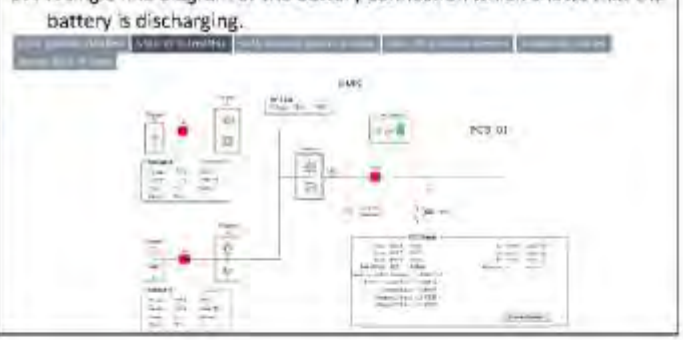
16. Click on the Firefox Web Browser.

16. The web browser opens with SMS System Menu.

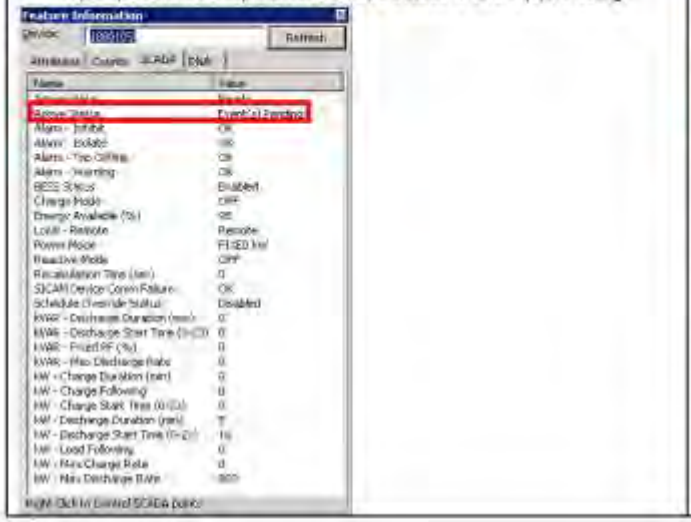
17. Select the SMS PCS Oneline tab.



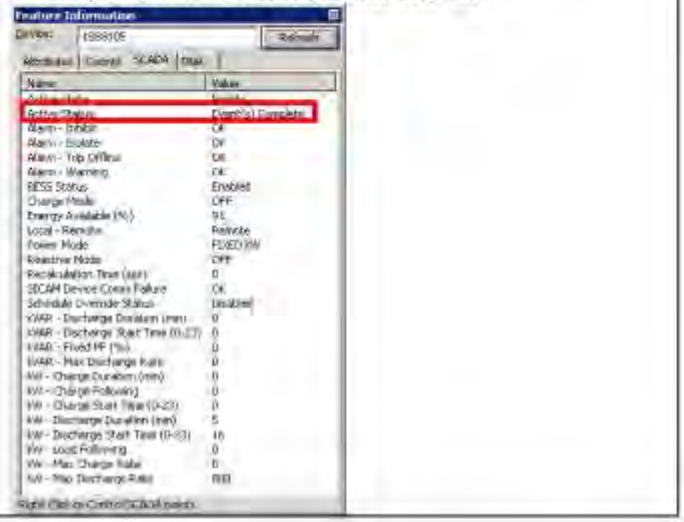
17. A single line diagram of the battery connection which shows that the battery is discharging.



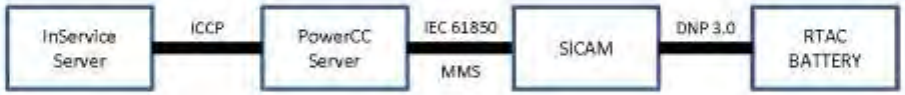
18. When the event is in process, open the feature information window in I/Dispatcher. Verify that the Active Status is Event(s) Pending.



18. The Active Status changes from Event(s) Pending to Event(s) Complete once the event duration has occurred.

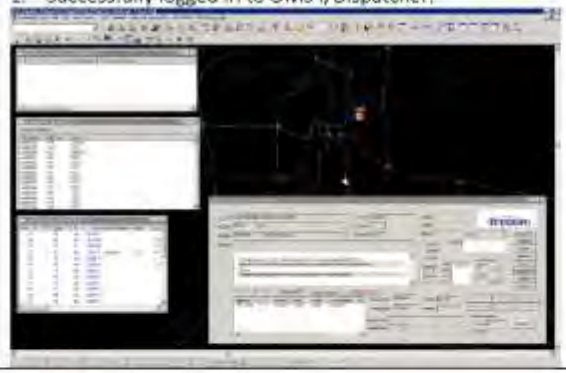


Battery Grid Operation – Load Following (Discharge)

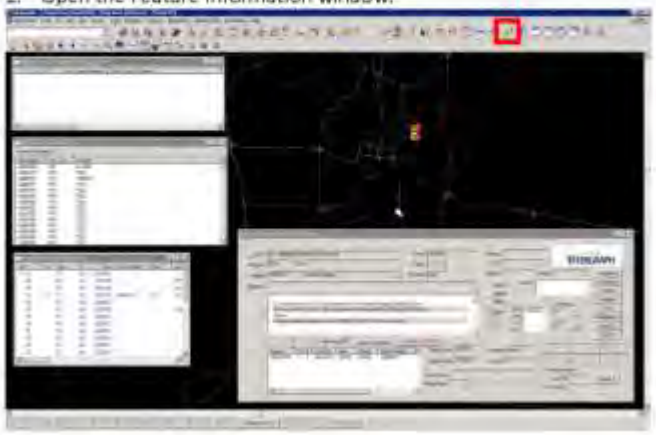


Load Following – Battery Discharging in Power Mode

Precondition: Battery is fully charged.

Steps	Expected Results
1. Log in to OMS I/Dispatcher. 	1. Successfully logged in to OMS I/Dispatcher. 

2. Open the Feature Information window.

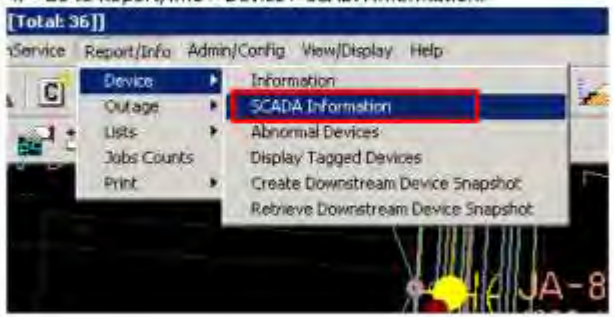


2. A new window is opened.

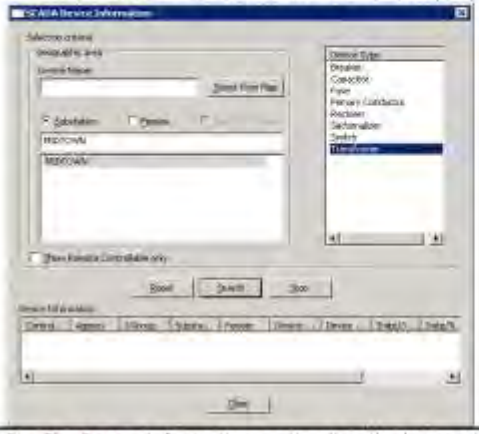
3. In the Feature Information window, enter the battery UODID (1888105).

3. The feature information displays the SCADA value for battery.

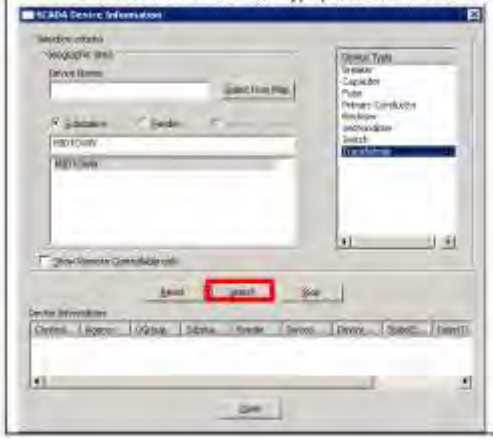
4. Go to Report/Info > Device > SCADA Information.



4. A new window "SCADA Device Information (SDI)" is opened.

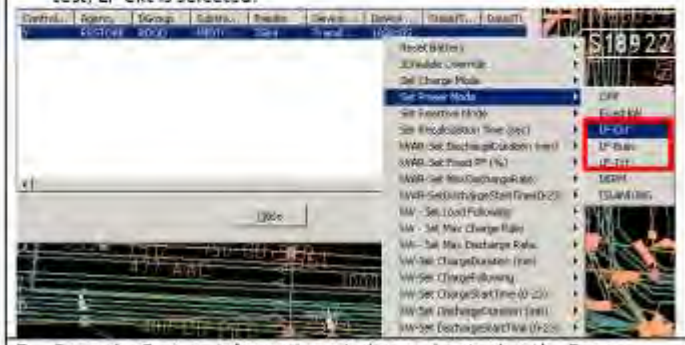


5. In the Device Name, type the UODID of battery. Select Midtown as substation and in Device Type, select transformer. Click Search.



5. The Device Information section lists the battery information.

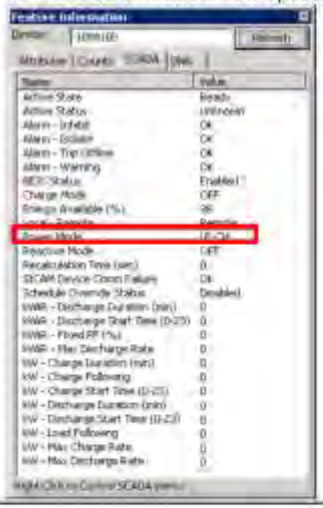
6. Go to Set Power Mode and select LF-Ckt or LF-Buss or LF-Txf. For this test, LF-Ckt is selected.



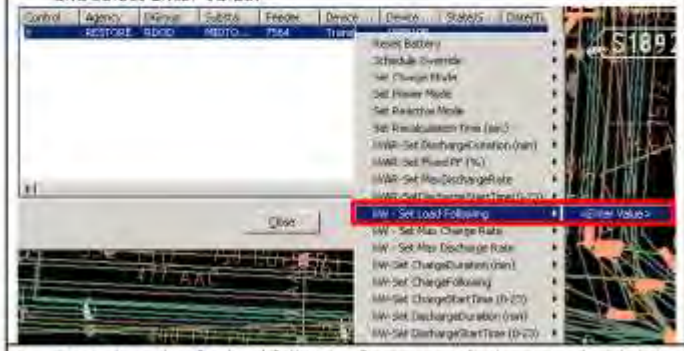
6. The Battery is now set to Load Following - Circuit (LF-Ckt) Discharge mode.

7. Open the Feature Information window and note that the Power Mode is "OFF". Click Refresh to update the Power Mode to Fixed kW.

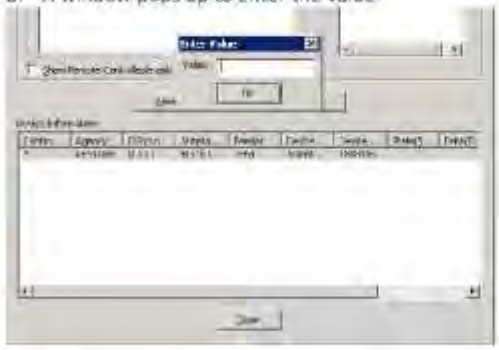
7. The Power Mode is now updated to "LF-Ckt".



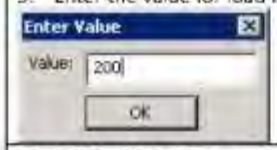
8. Open SDI and right click the battery. Select kW-Set Load Following and select Enter Value.



8. A window pops up to enter the value.

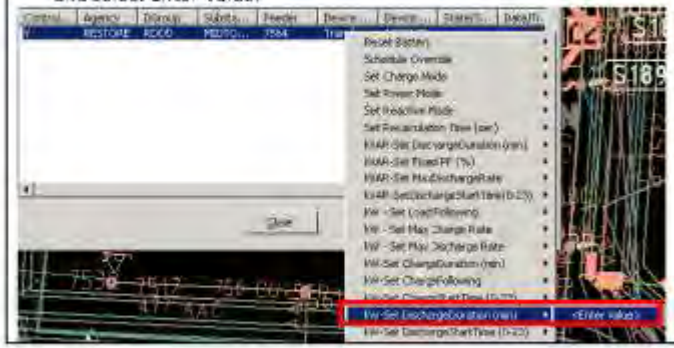


9. Enter the value for load following for battery discharge and click OK.

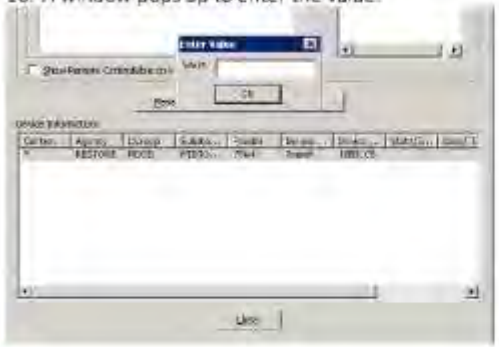


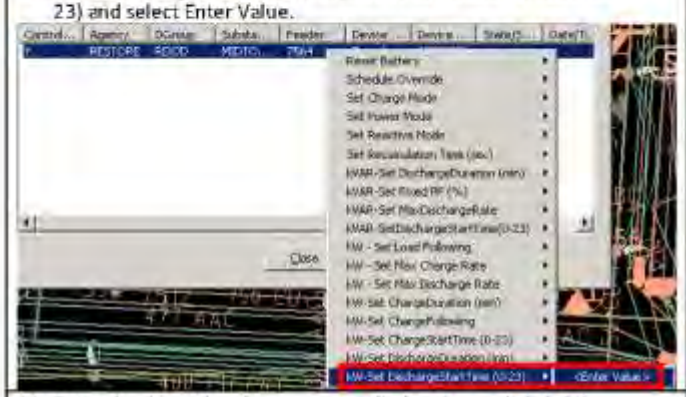
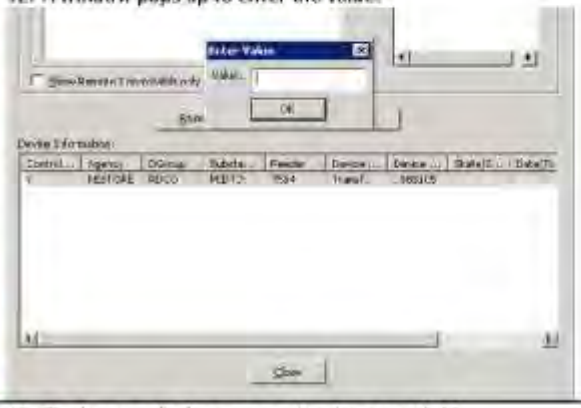
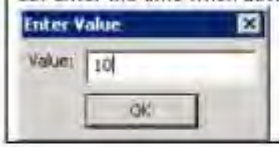
9. The battery Load Following is set to 200kW.

10. In SDI, right click the battery. Select kW-Set DischargeDuration (min) and select Enter Value.



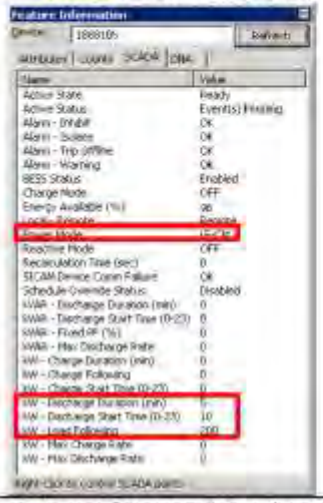
10. A window pops up to enter the value.



11. Enter the discharge duration for battery and click OK. 	11. The battery discharge duration is set to 5 minutes.
12. In SDI, right click the battery. Select kW-Set DischargeStartTime (0-23) and select Enter Value. 	12. A window pops up to enter the value. 
13. Enter the time when battery starts discharging and click OK. 	13. The battery discharge start time is set to 10:00.

14. Open the feature information window and to verify that the values entered above are reflected in the SCADA tab, press Refresh.

14. Note that the kW – Discharge Duration is 5 min, kW – Discharge time is 10:00 and kW – Load Following is 200.



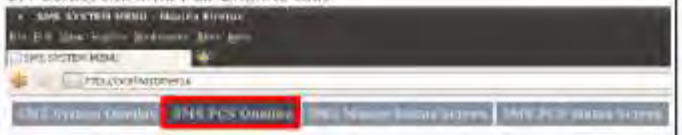
15. Log in to the S&C SMS for battery.

15. Successfully logged in to the system.

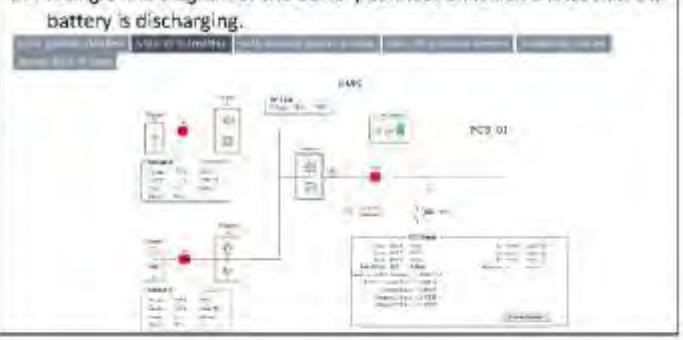
16. Click on the Firefox Web Browser.

16. The web browser opens with SMS System Menu.

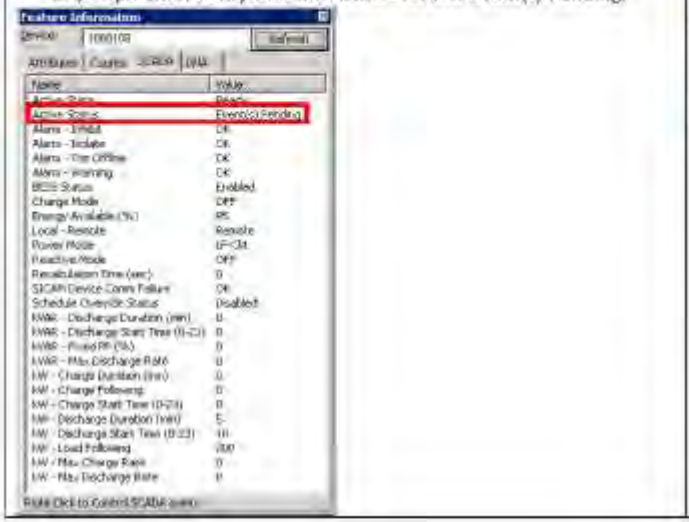
17. Select the SMS PCS Oneline tab.



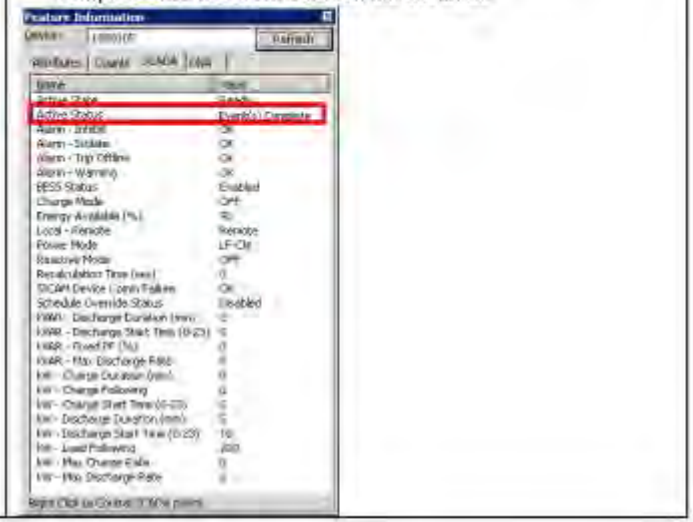
17. A single line diagram of the battery connection which shows that the battery is discharging.



18. When the event is in process, open the feature information window in I/Dispatcher. Verify that the Active Status is Event(s) Pending.



18. The Active Status changes from Event(s) Pending to Event(s) Complete once the event duration has occurred.



This page intentionally blank.

Appendix K Interoperability Field Demonstration Scripts

This page intentionally blank.

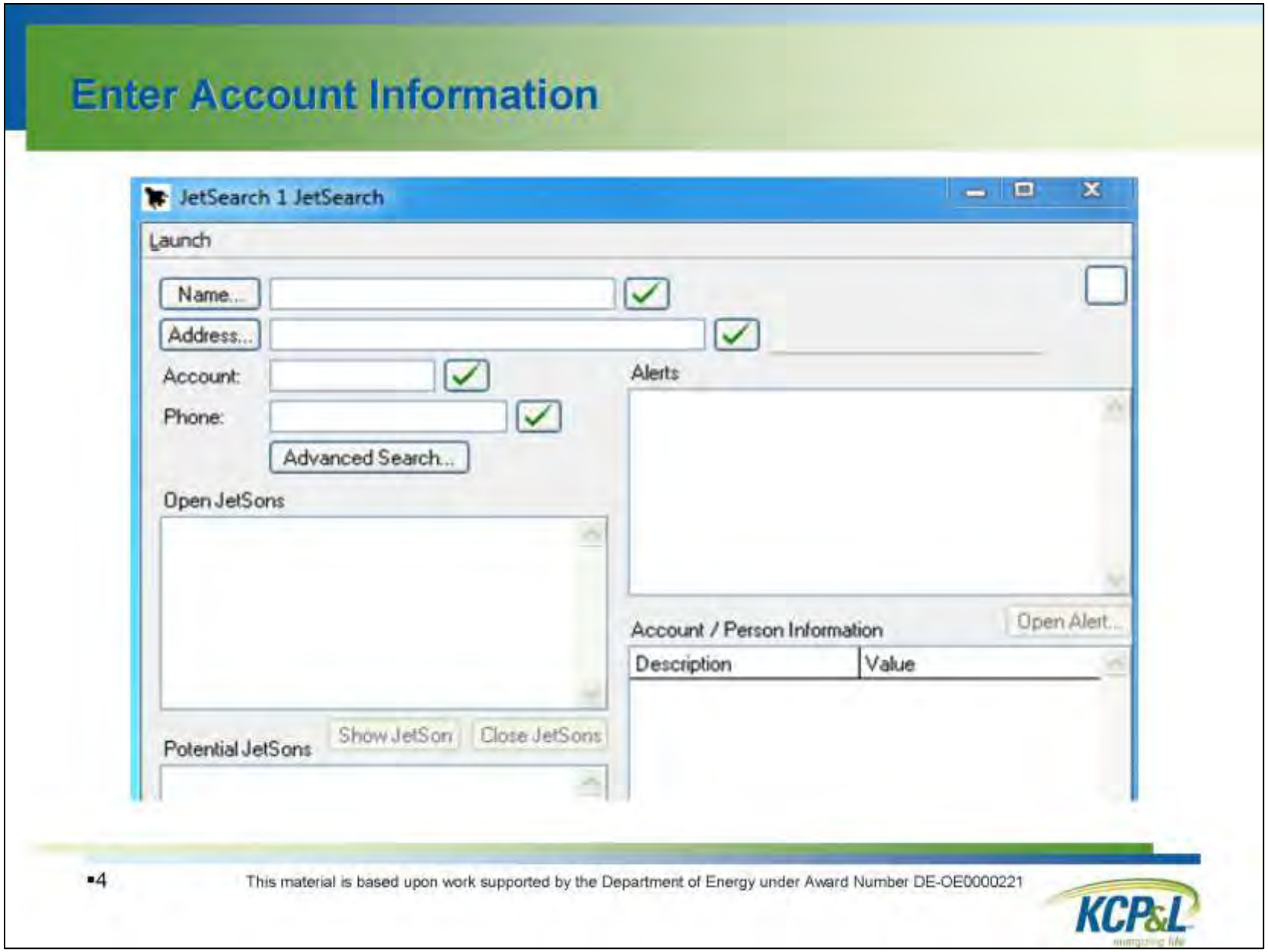

Remote Connect
- KC Green Impact Zone Initiative
- DOE Regional SmartGrid Demonstration Program
- EPRI SmartGrid Demonstration Program
KCP&L
SmartGrid
the future of energy

Launch CIS

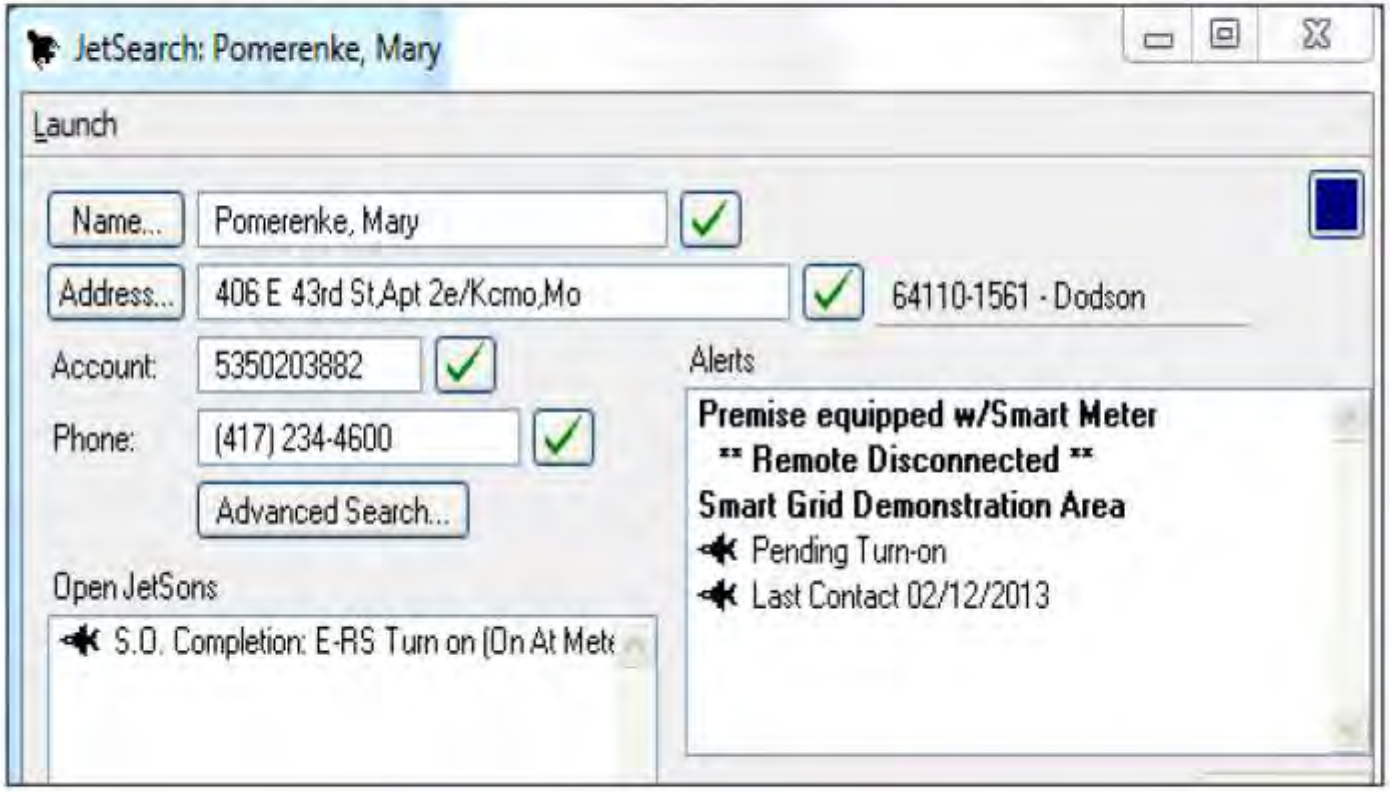
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Select "Jet" Search Button

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

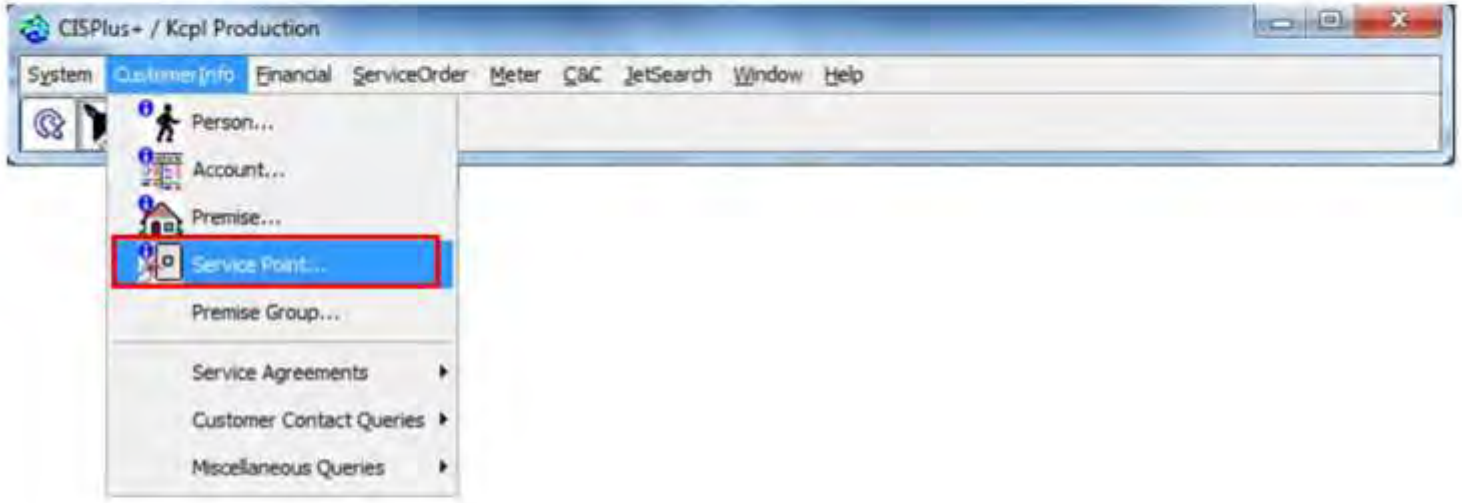

Enter Account Information
JetSearch 1 JetSearch
Launch
Name...
Address...
Account:
Phone:
Advanced Search...
Open JetSons
Potential JetSons
Show JetSon
Close JetSons
Alerts
Account / Person Information
Open Alert...
Description
Value
4
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

Account Information is Displayed



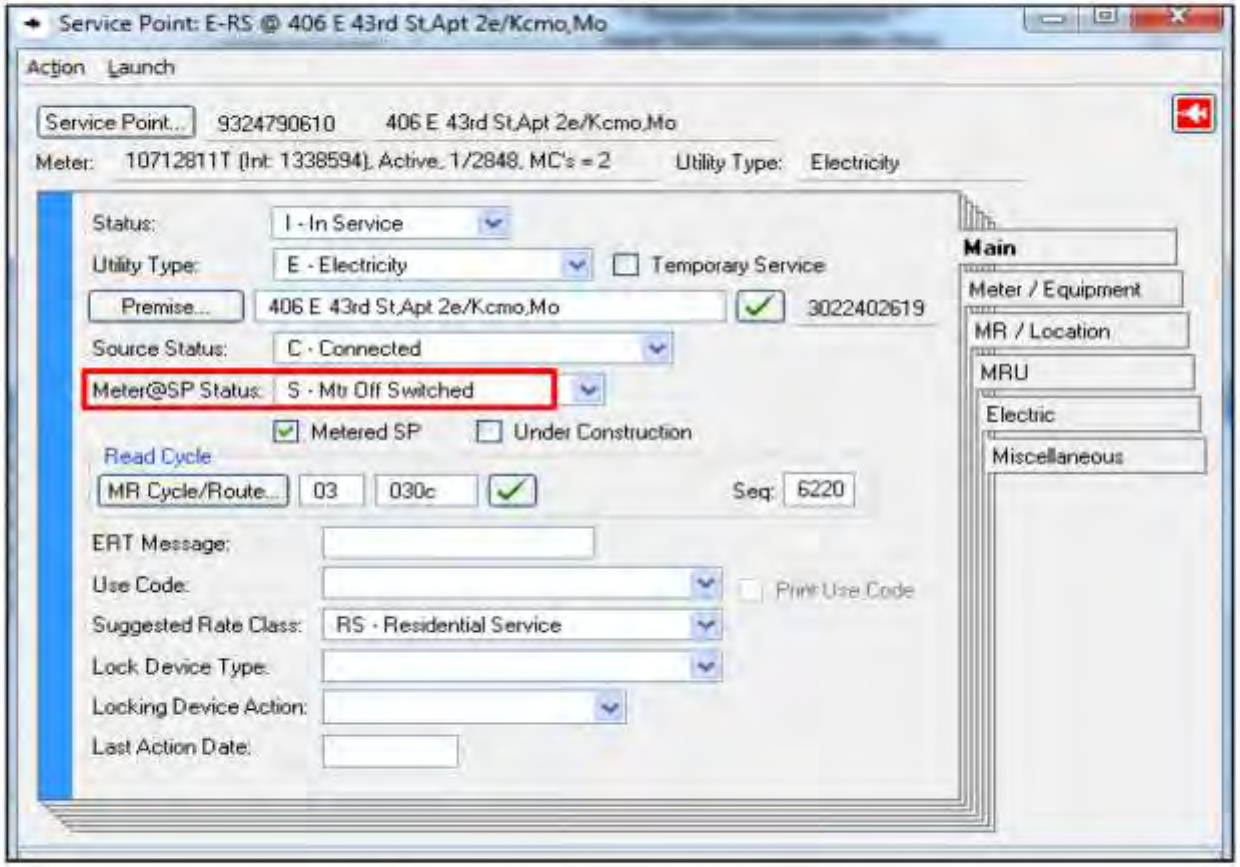
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Go to Service Point



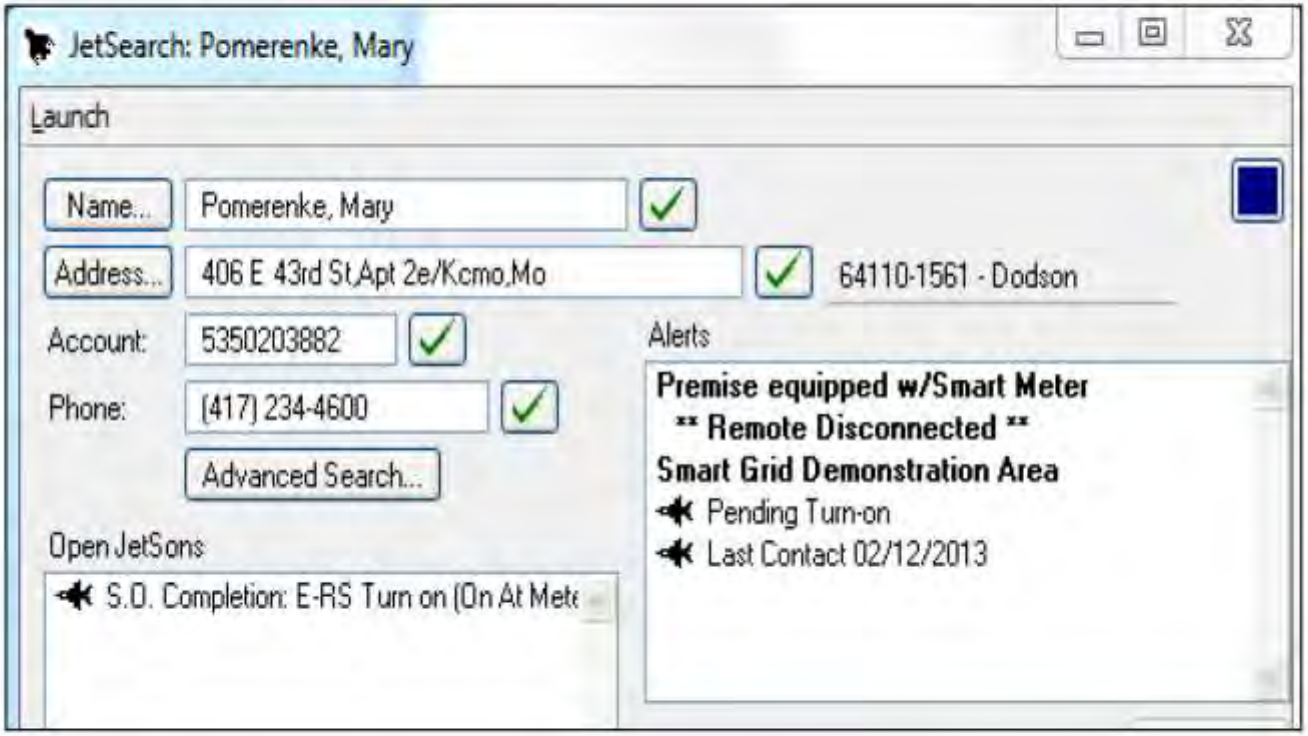
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Service Point Information of Entered Account Number

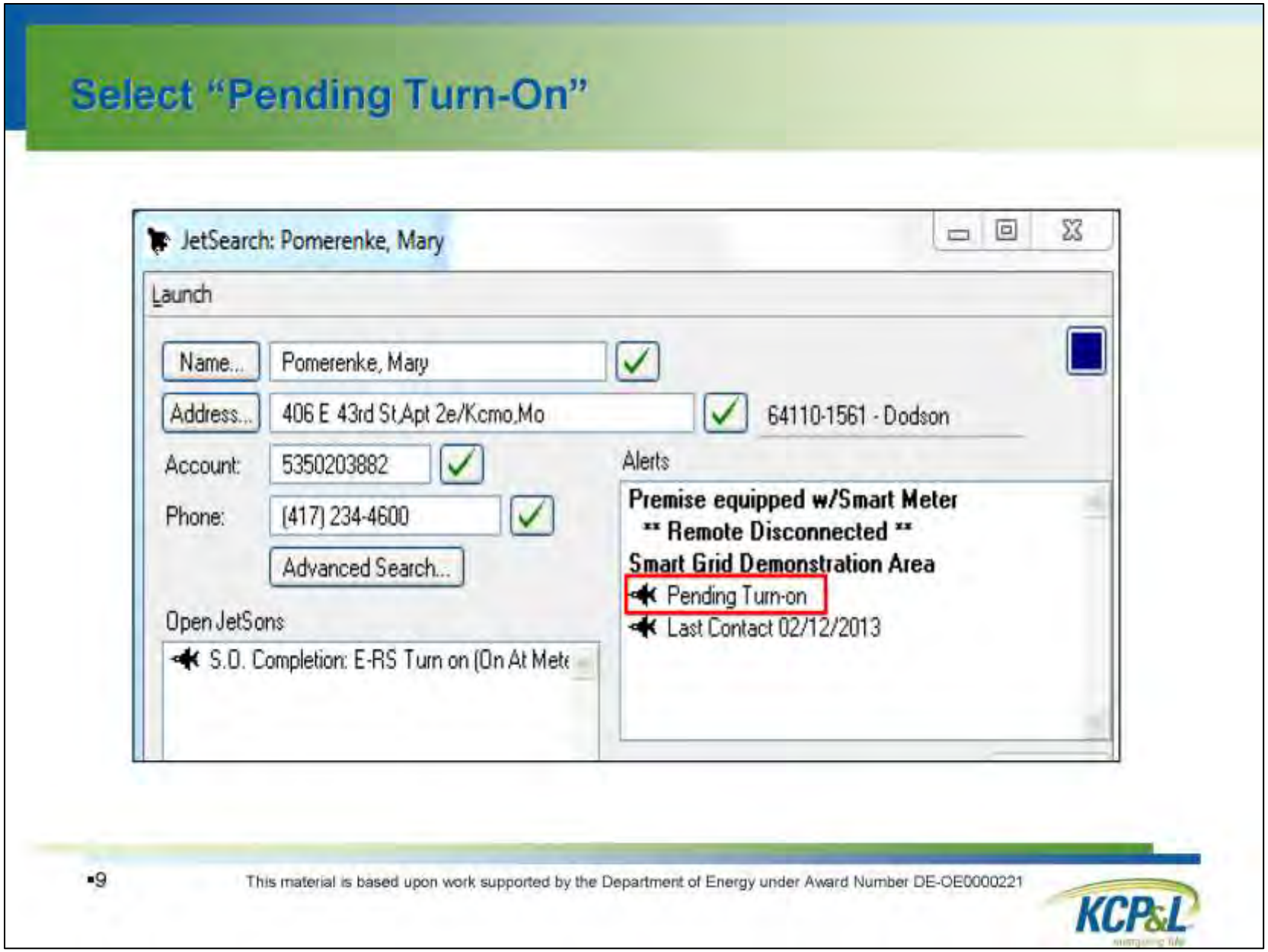


This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

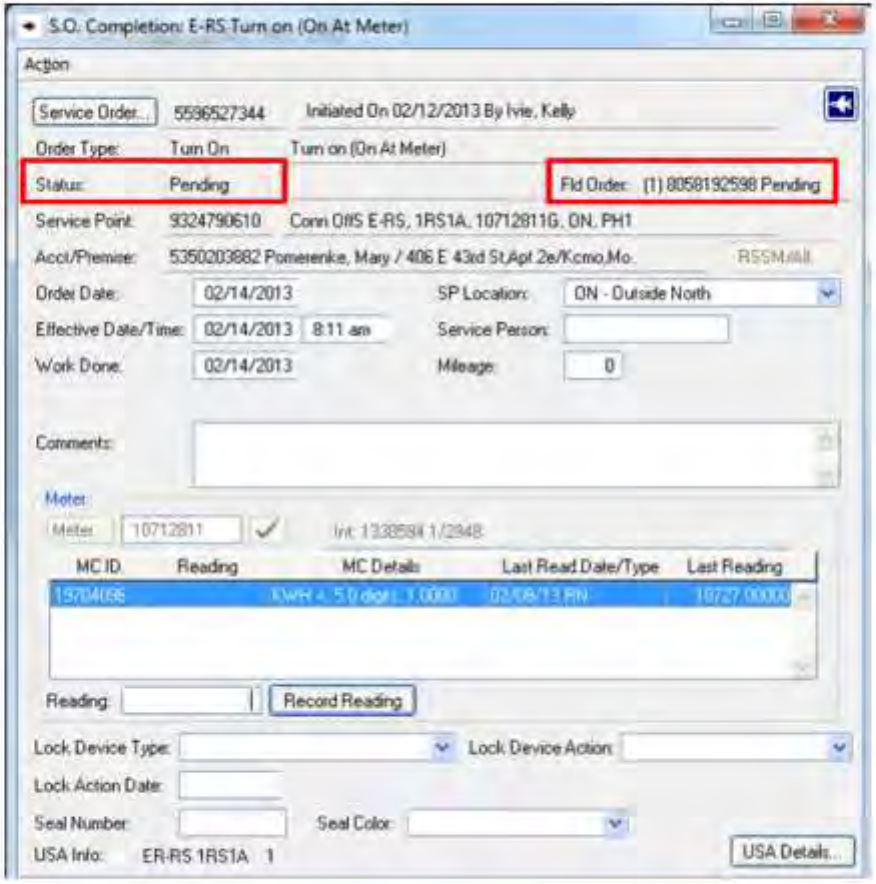
Go to Jet Search Window: Updated Information



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221


Select "Pending Turn-On"
JetSearch: Pomerenke, Mary
Launch
Name...
Pomerenke, Mary
Address...
406 E 43rd St,Apt 2e/Kcmo,Mo
64110-1561 - Dodson
Account:
5350203882
Phone:
(417) 234-4600
Advanced Search...
Alerts
Premise equipped w/Smart Meter
** Remote Disconnected **
Smart Grid Demonstration Area
Pending Turn-on
Last Contact 02/12/2013
Open JetSons
S.O. Completion: E-RS Turn on (On At Mete
9
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

Status of Service Order "Pending"

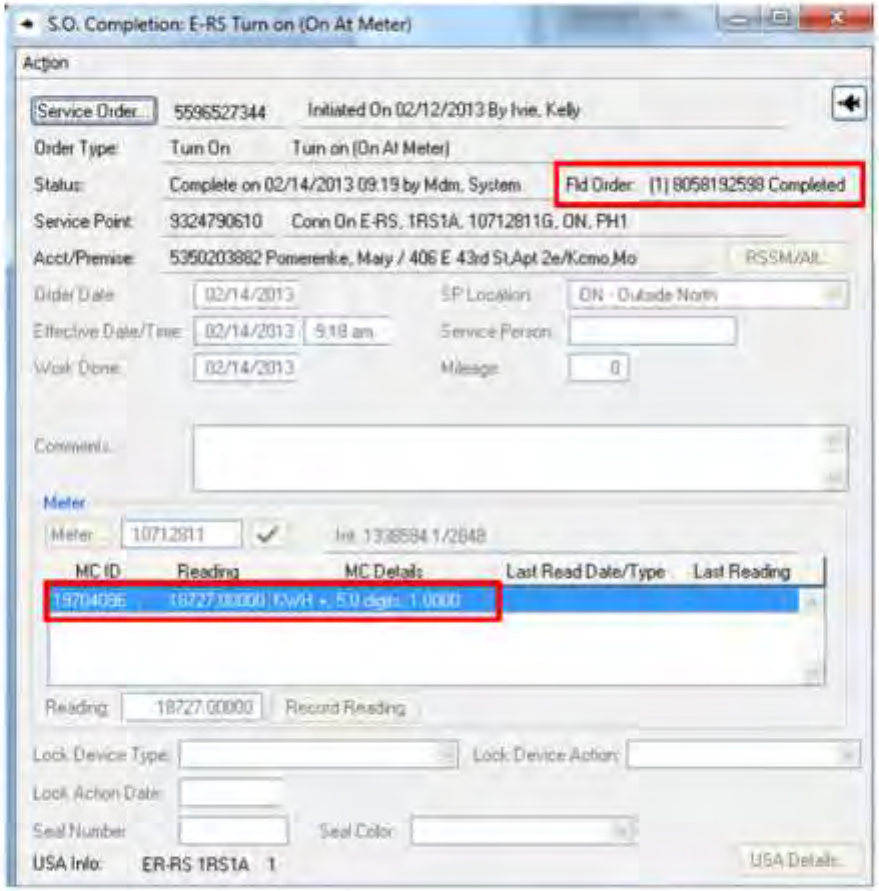


This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Status "Acknowledged" After Process is Started

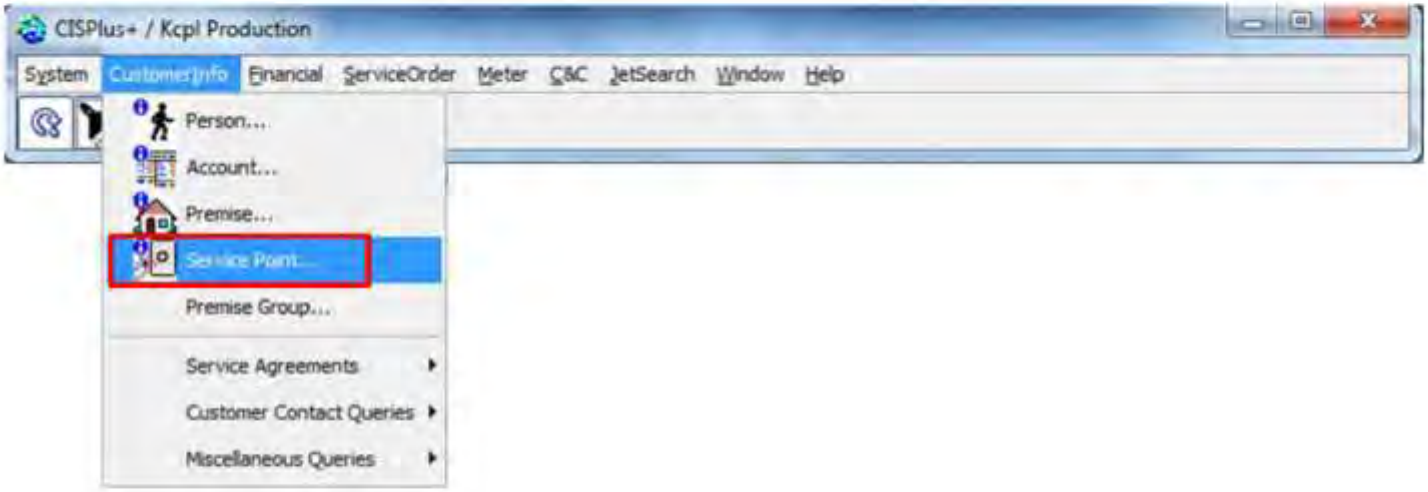
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

After Connect, Status of Service Order "Completed"



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Go to "Service Point"



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Service Point Displays "Meter On"

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

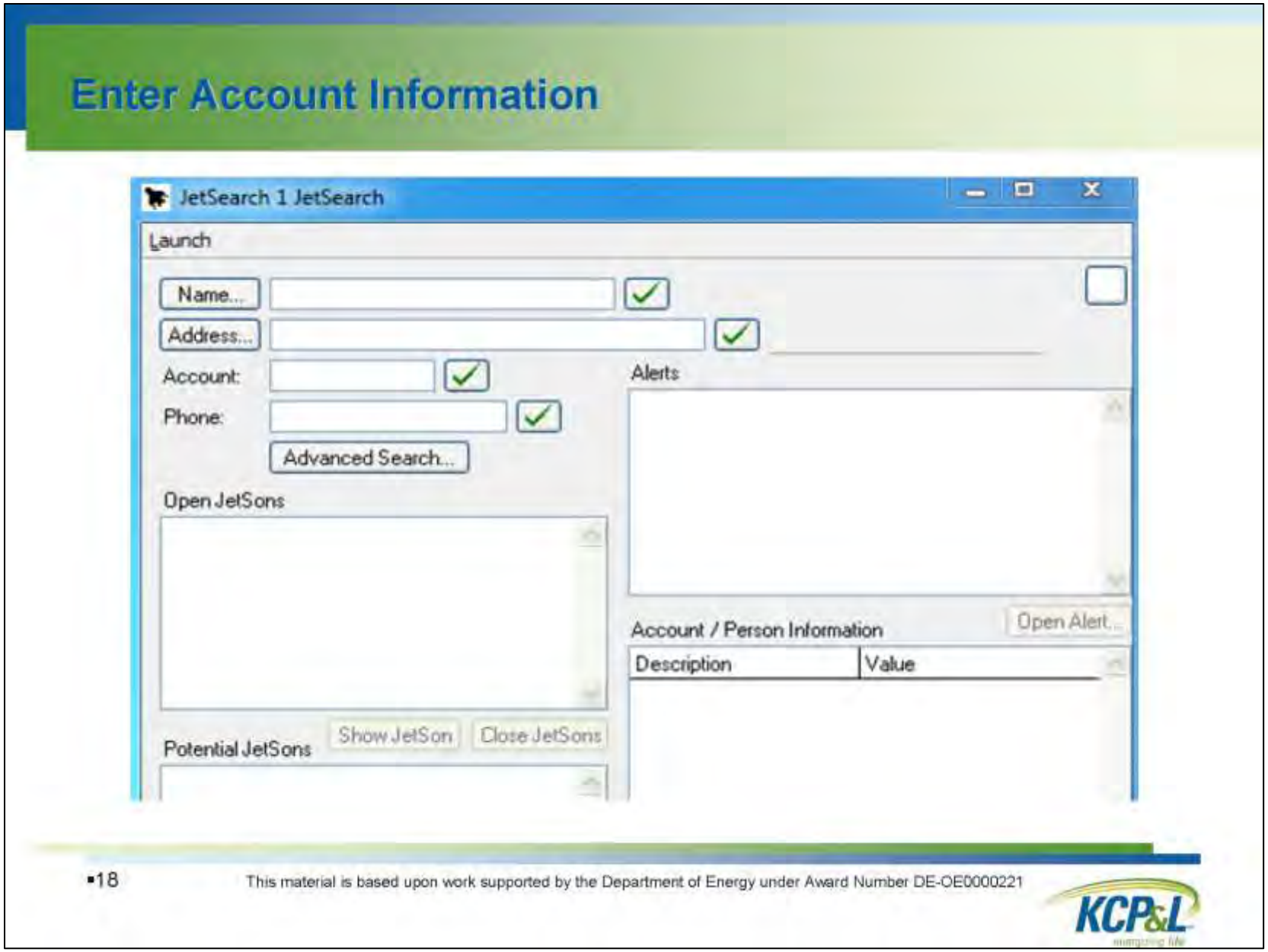

Remote Disconnect
- KC Green Impact Zone Initiative
- DOE Regional SmartGrid Demonstration Program
- EPRI SmartGrid Demonstration Program
KCP&L
SmartGrid
the future of energy

Launch CIS

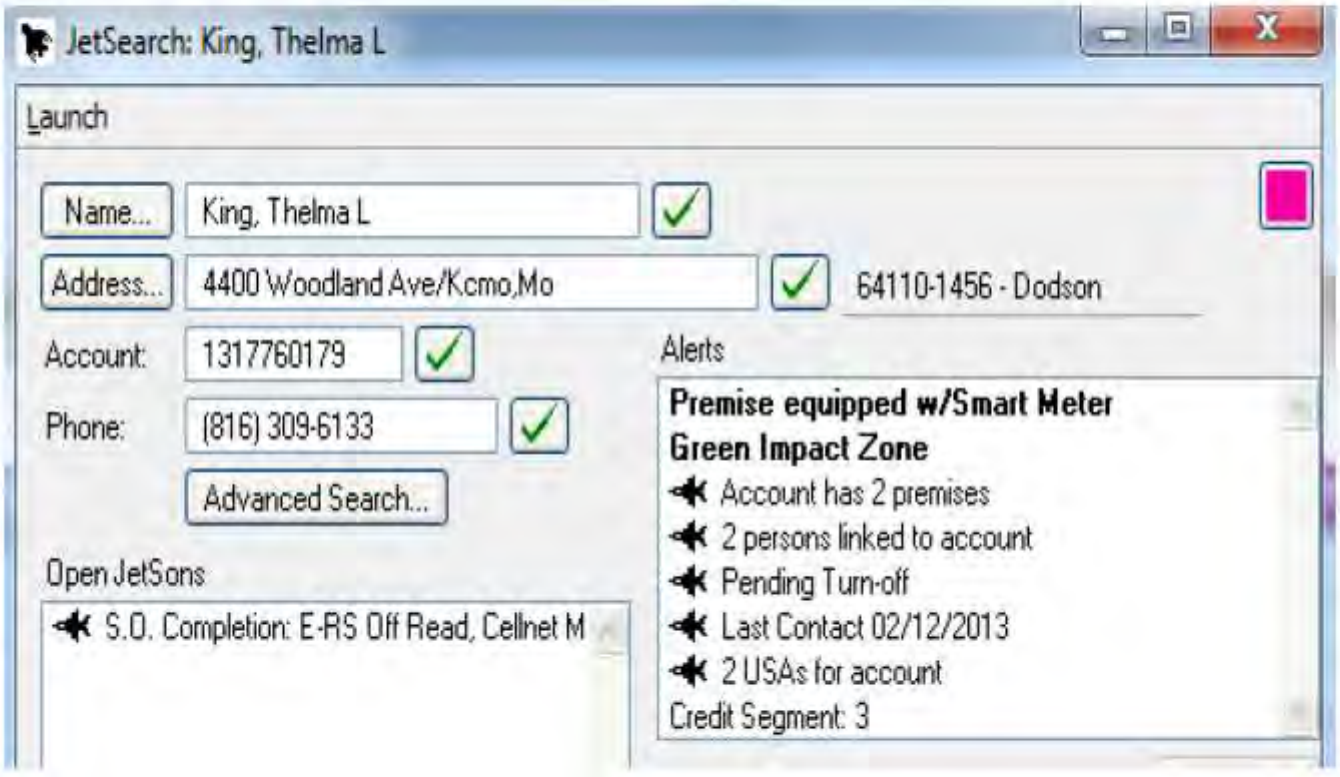
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Select "Jet" Search Button

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221


Enter Account Information
JetSearch 1 JetSearch
Launch
Name...
Address...
Account:
Phone:
Advanced Search...
Alerts
Open JetSons
Account / Person Information
Open Alert...
Description
Value
Show JetSon
Close JetSons
Potential JetSons
18
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

Account Information is Displayed



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

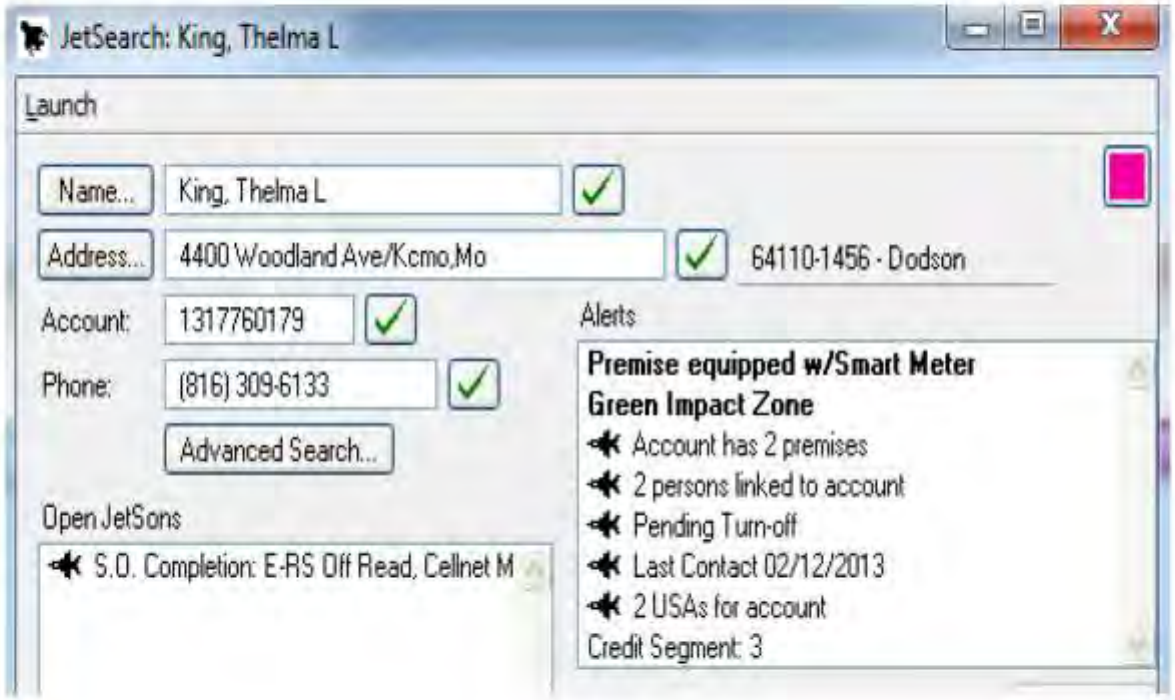
Go to Service Point

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Service Point Information of Entered Account Number

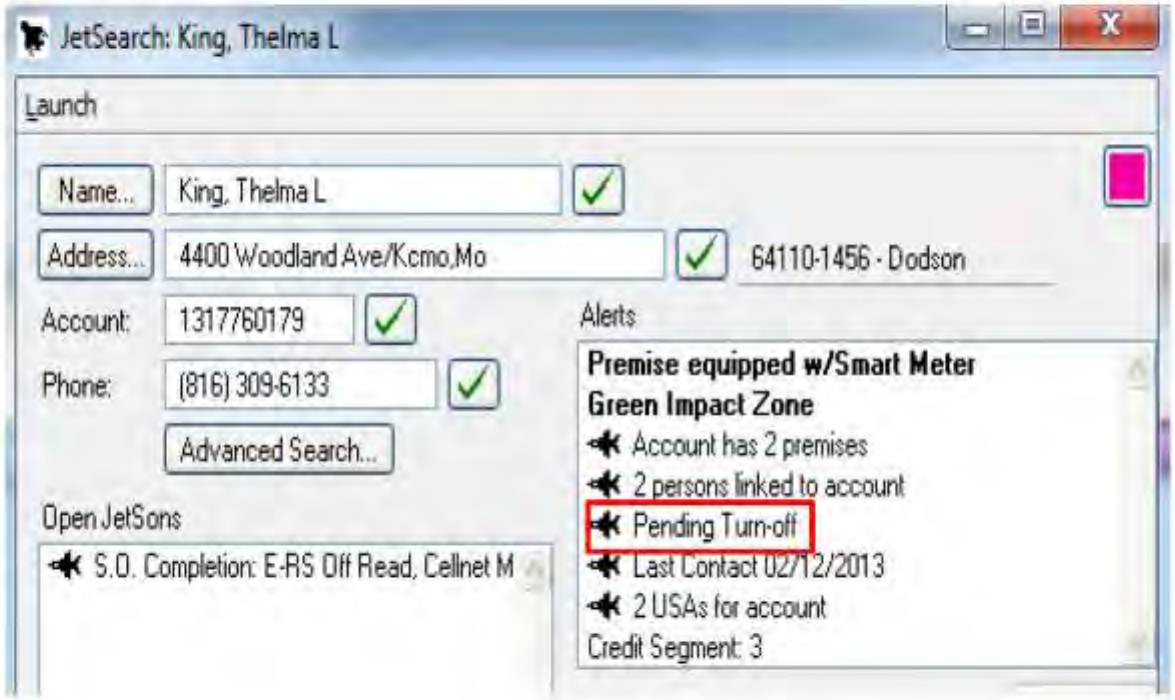
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Go to Jet Search Window: Updated Information



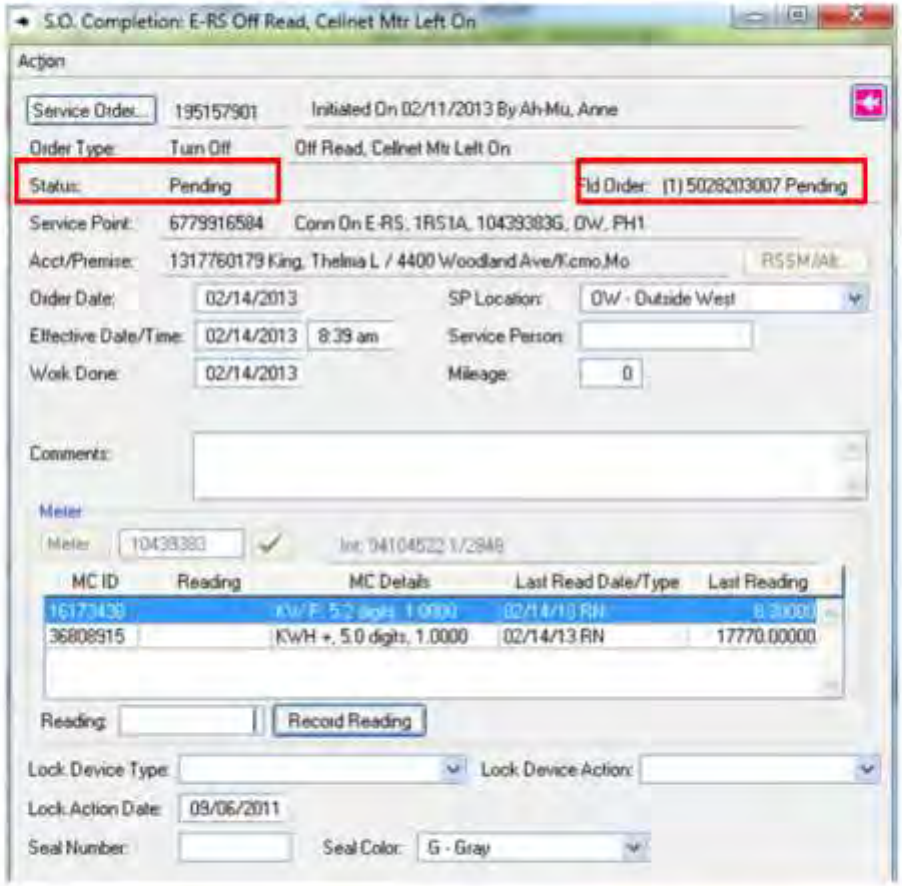
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Select "Pending Turn-Off"



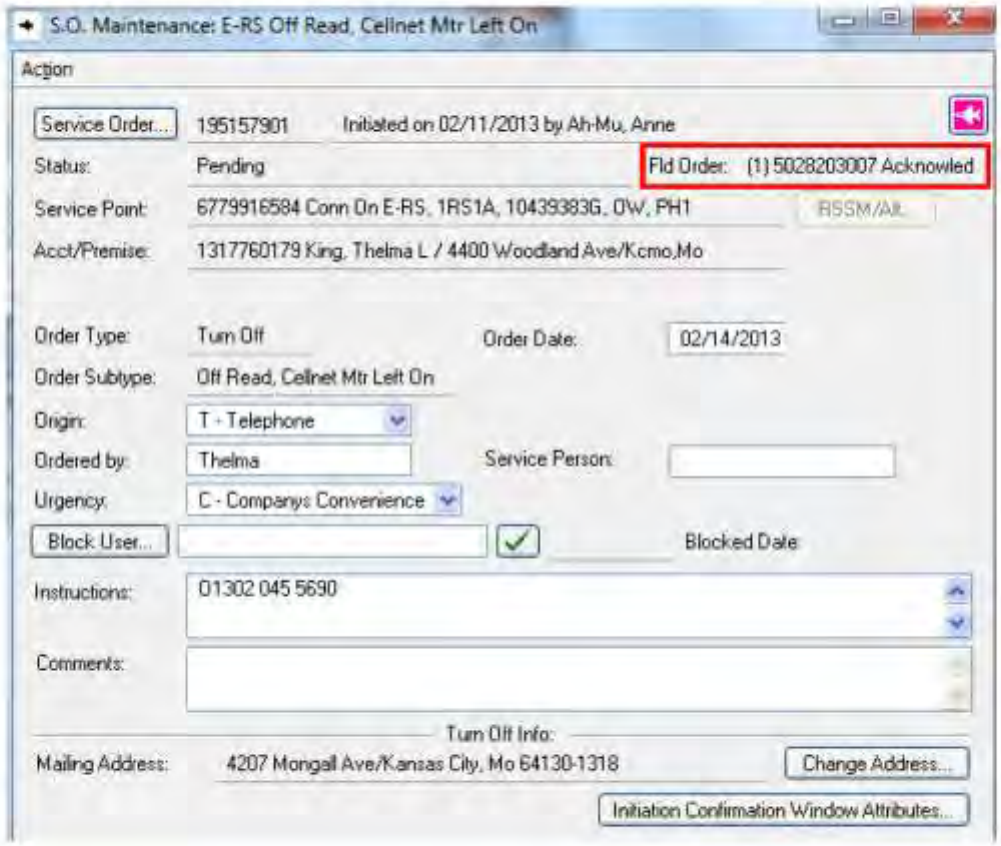
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Status of Service Order "Pending"



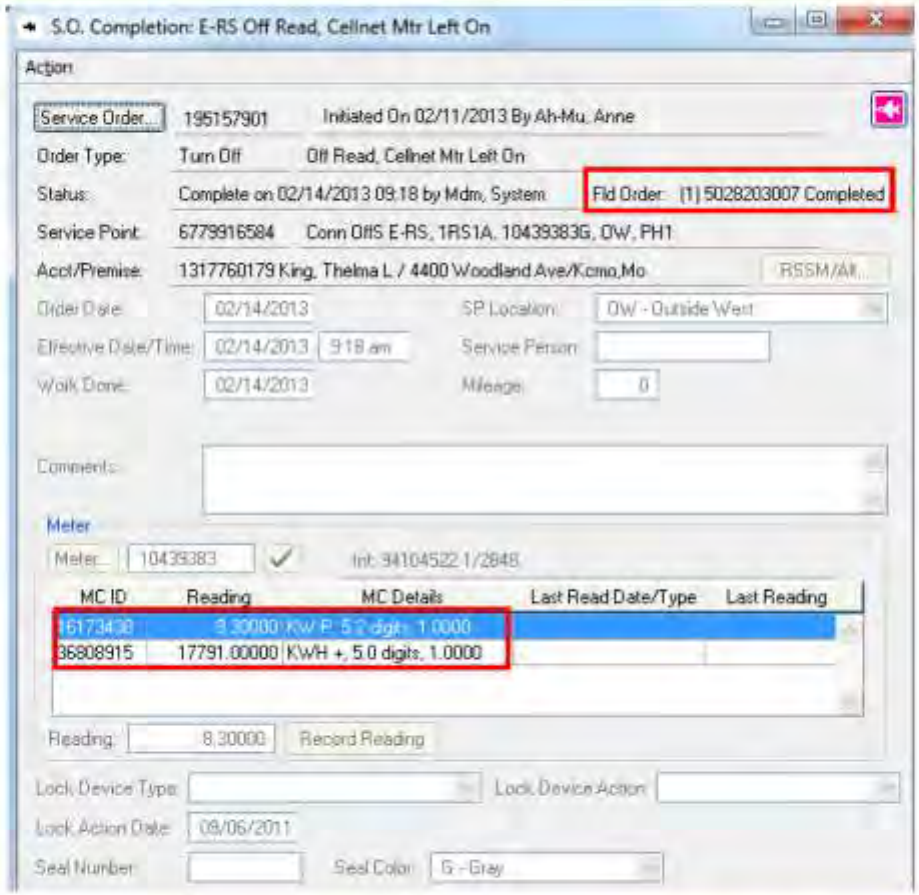
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Status "Acknowledged" After Process is Started



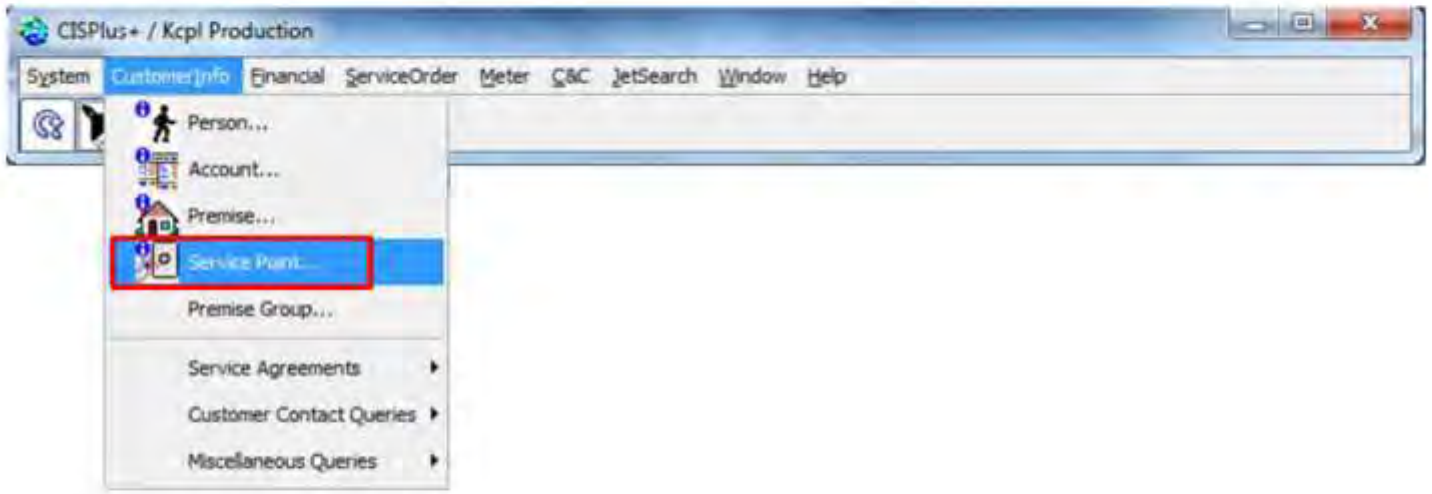
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

After Disconnect, Status of Service Order "Completed"



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

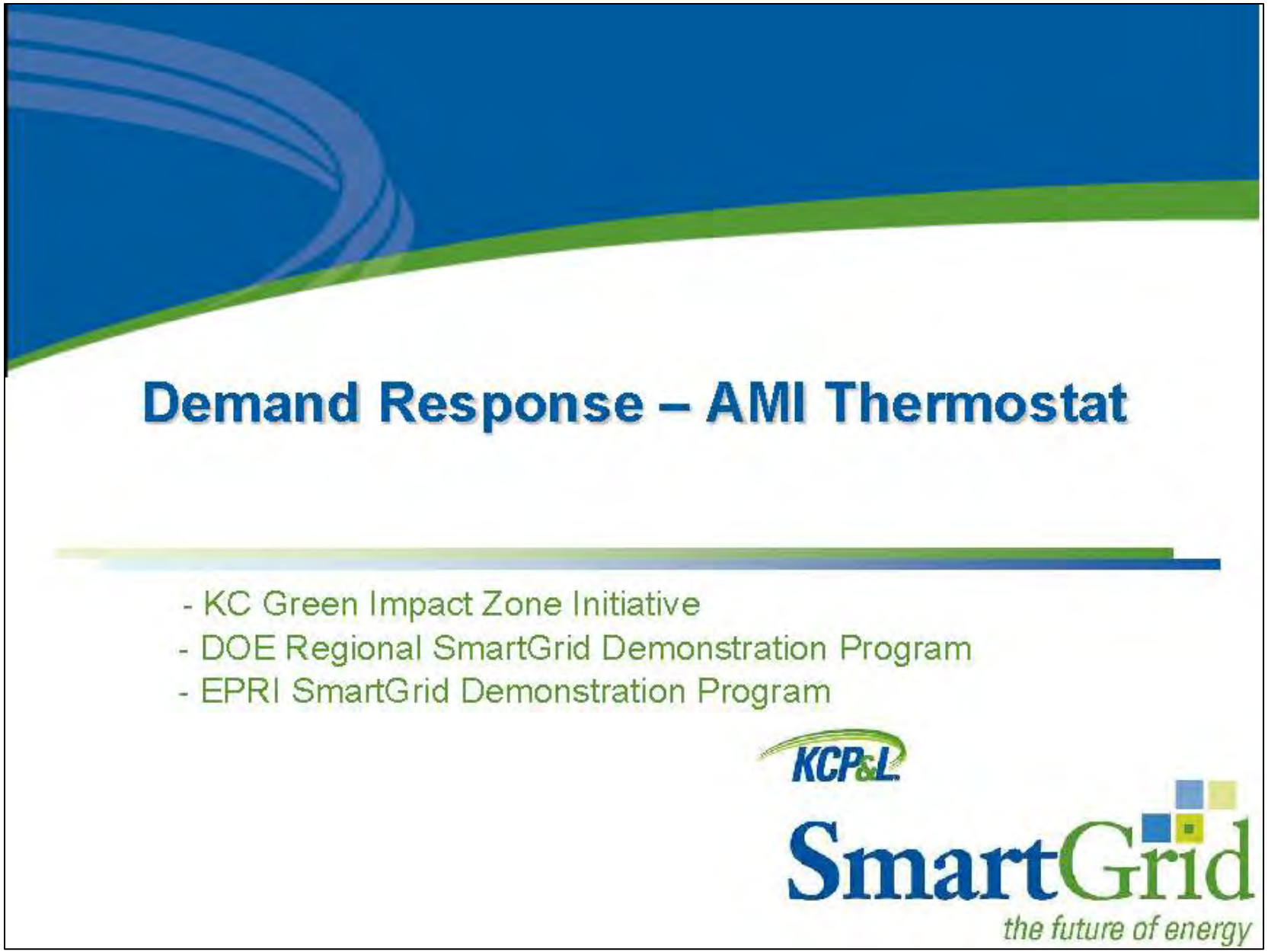
Go to "Service Point"



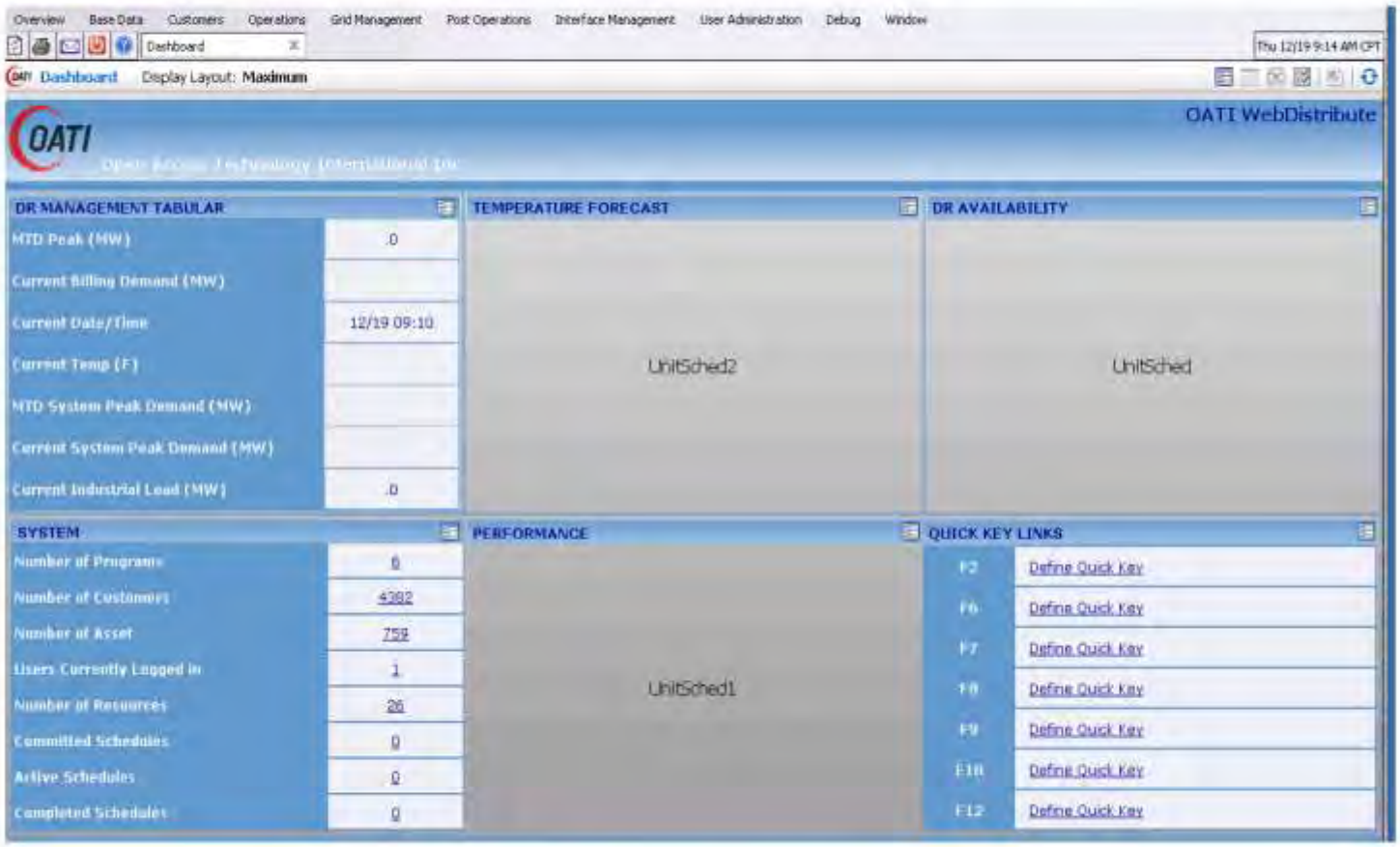
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Service Point Displays "Meter On"

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

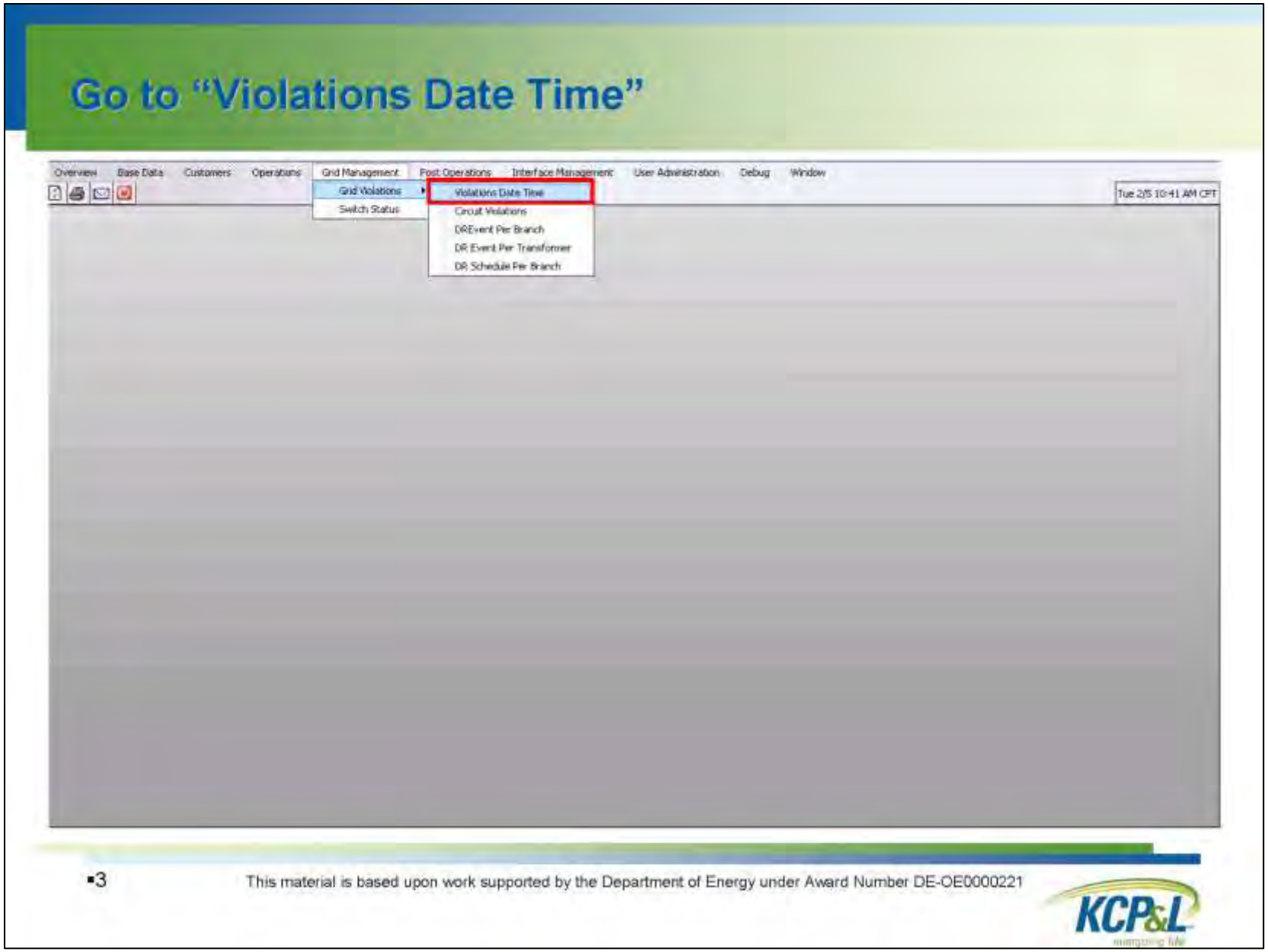

Demand Response – AMI Thermostat
- KC Green Impact Zone Initiative
- DOE Regional SmartGrid Demonstration Program
- EPRI SmartGrid Demonstration Program
KCP&L
SmartGrid
the future of energy

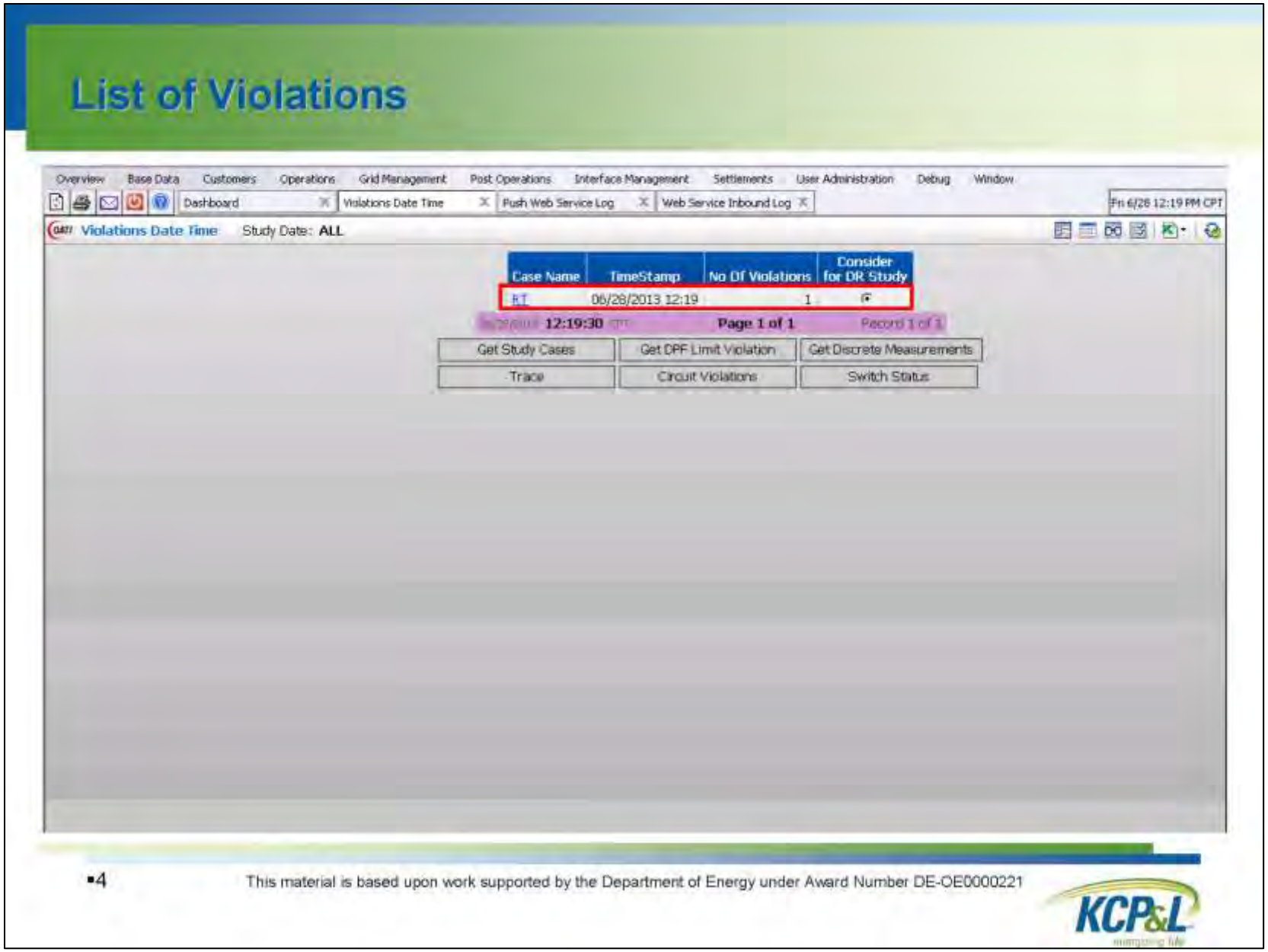
Launch DERM WebUI

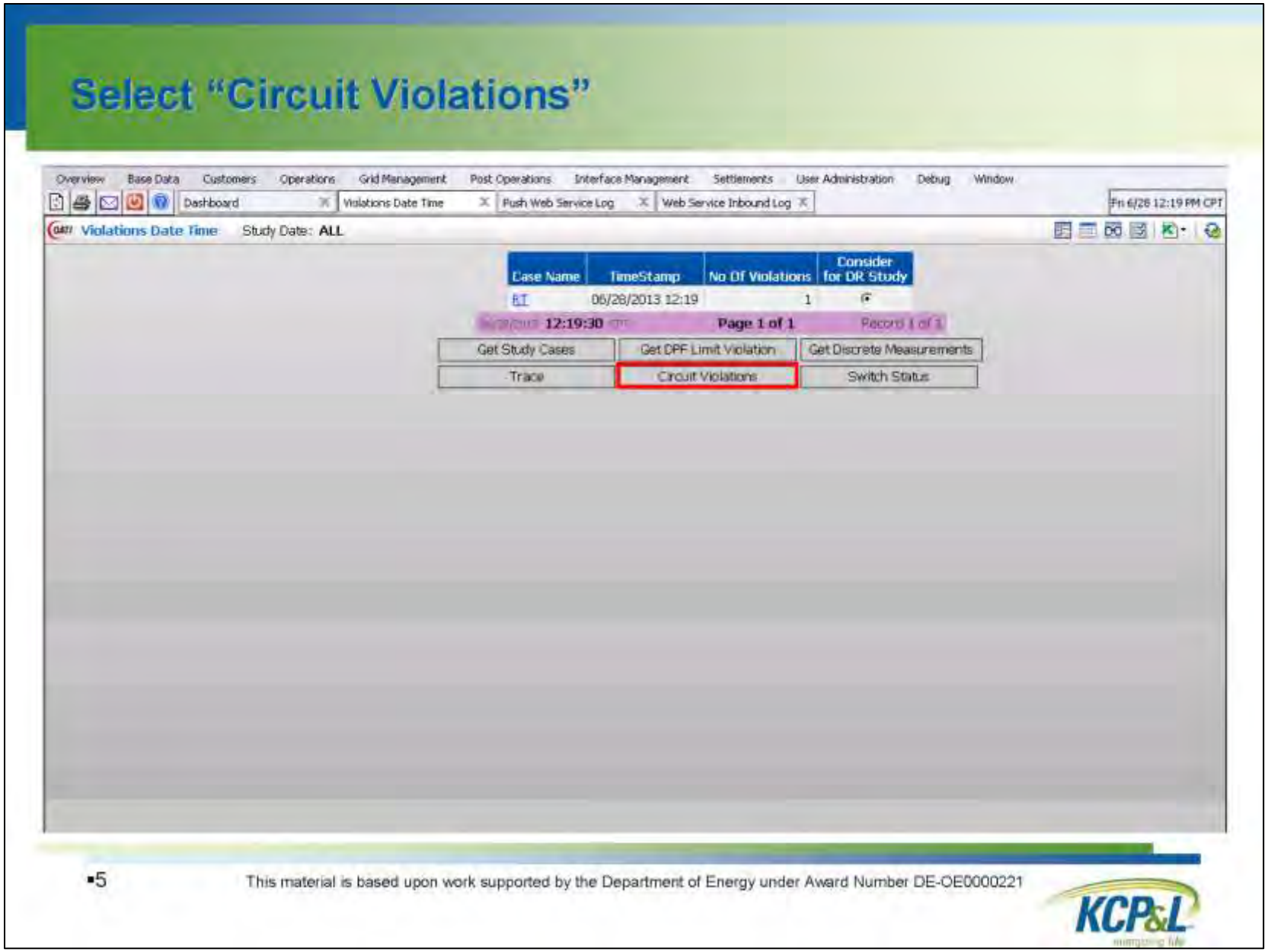


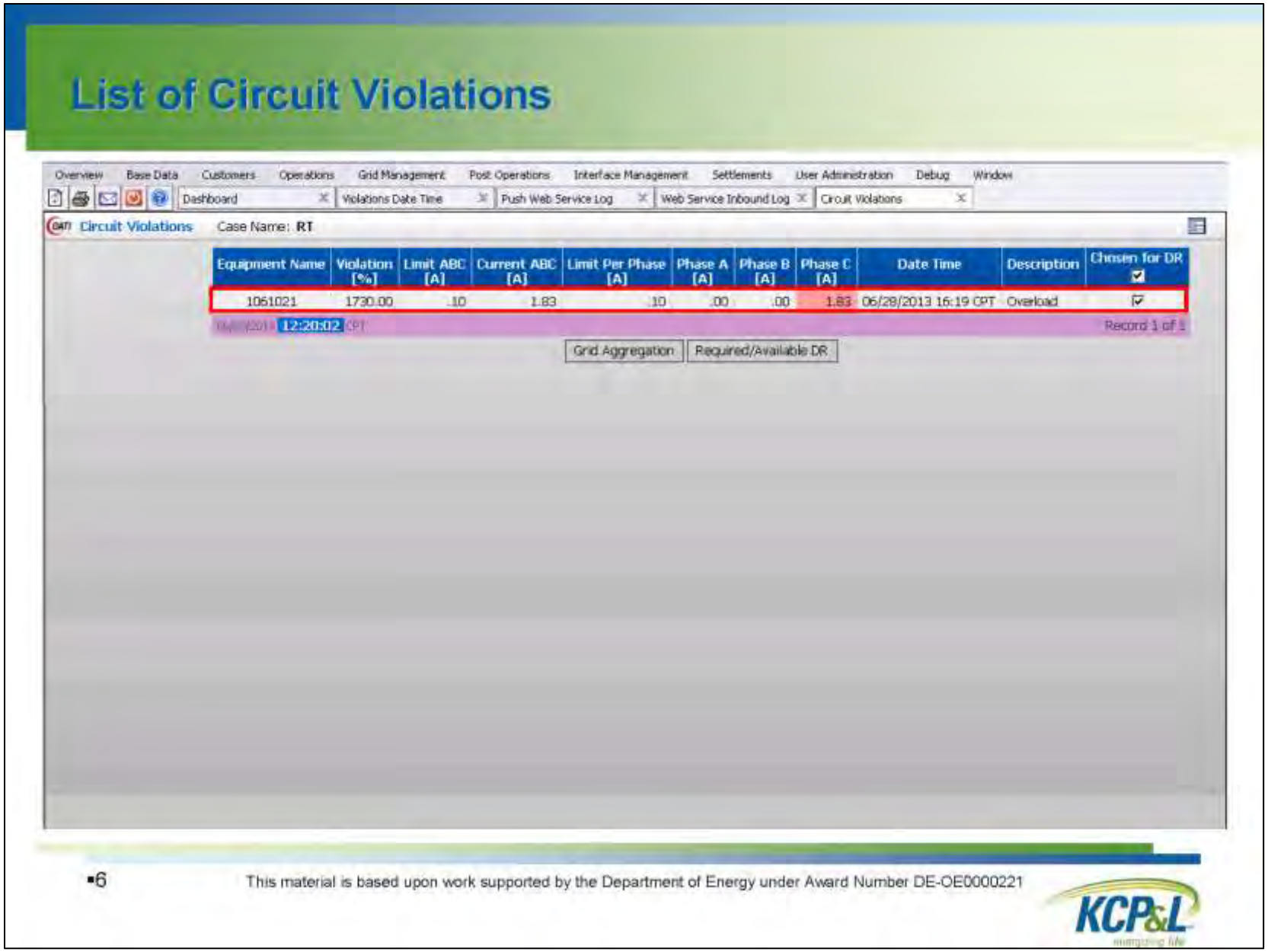
▪2

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

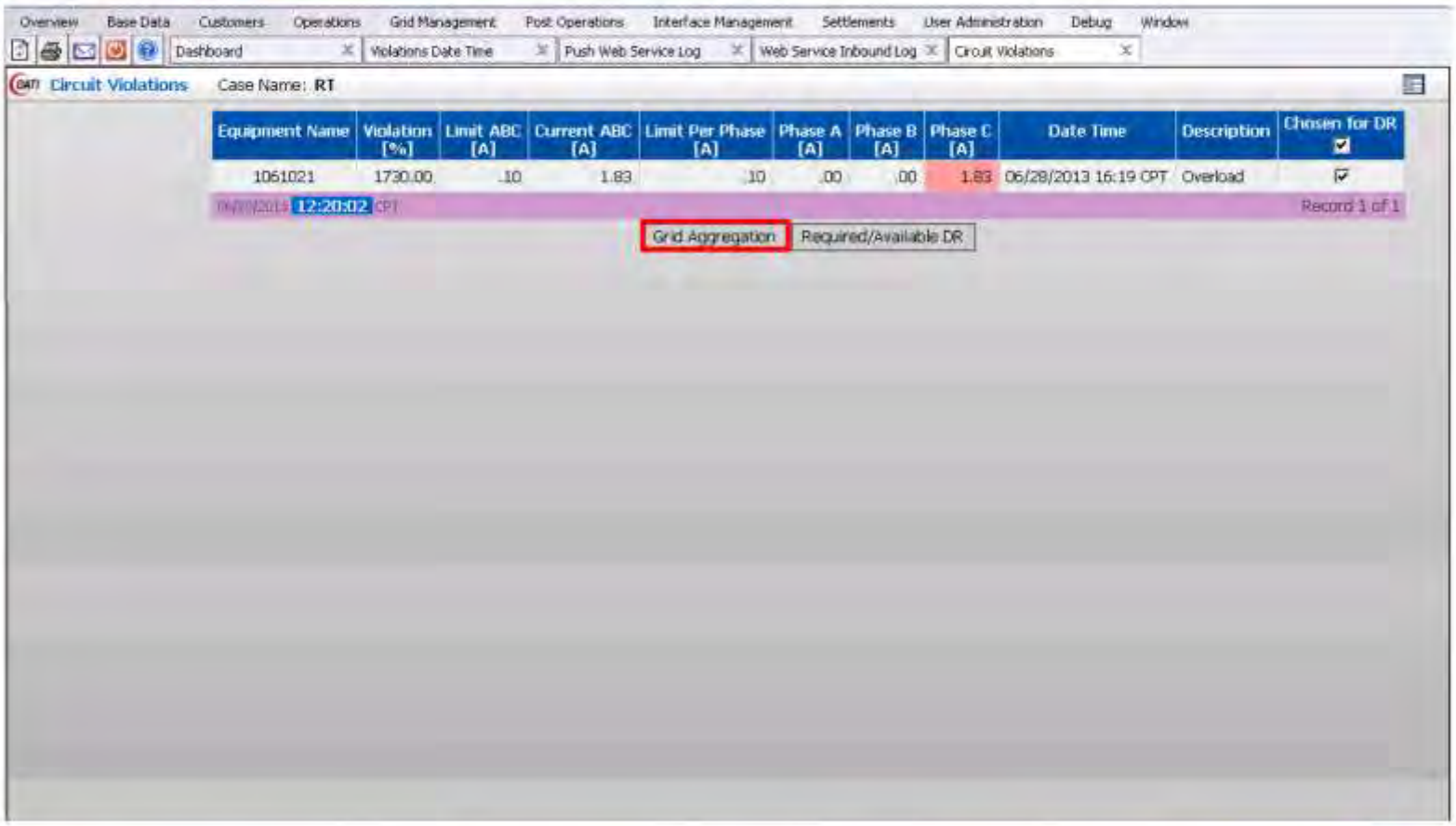

Go to "Violations Date Time"
Overview
Base Data
Customers
Operations
Grid Management
Post Operations
Interface Management
User Administration
Debug
Window
Grid Violations
Switch Status
Violations Date Time
Circuit Violations
DREvent Per Branch
DR Event Per Transformer
DR Schedule Per Branch
Tue 2/5 10:41 AM CPT
3
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L


List of Violations
Overview
Base Data
Customers
Operations
Grid Management
Post Operations
Interface Management
Settlements
User Administration
Debug
Window
Dashboard
Violations Date Time
Push Web Service Log
Web Service Inbound Log
Fri 6/28 12:19 PM CPT
Violations Date Time
Study Date: ALL
Case Name
TimeStamp
No Of Violations
Consider for DR Study
RT
06/28/2013 12:19
1
12:19:30
Page 1 of 1
Record 1 of 1
Get Study Cases
Get DPF Limit Violation
Get Discrete Measurements
Trace
Circuit Violations
Switch Status
4
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

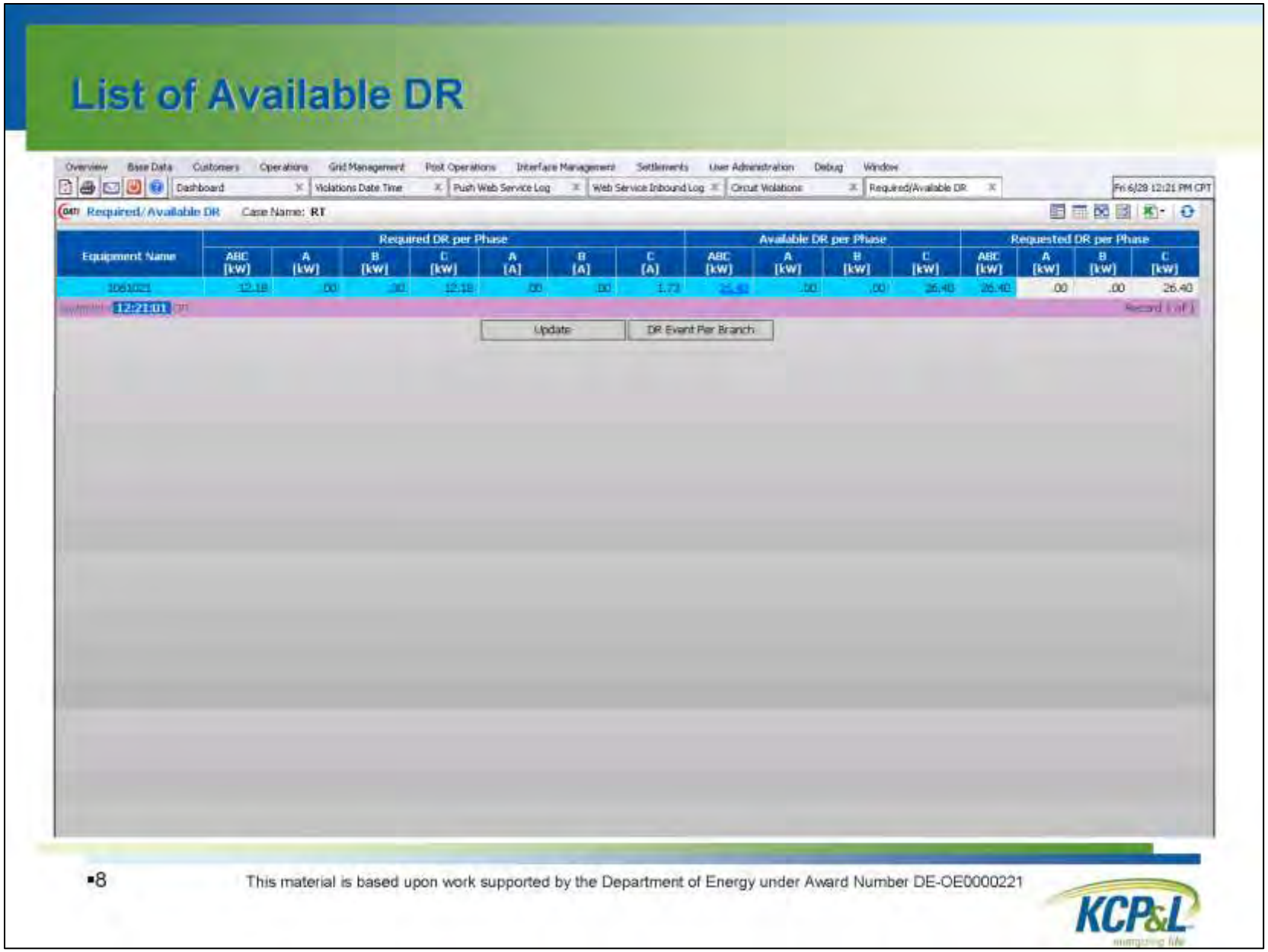

Select "Circuit Violations"
Overview
Base Data
Customers
Operations
Grid Management
Post Operations
Interface Management
Settlements
User Administration
Debug
Window
Dashboard
Violations Date Time
Push Web Service Log
Web Service Inbound Log
Violations Date Time
Study Date: ALL
Case Name
TimeStamp
No Of Violations
Consider for DR Study
RT
06/28/2013 12:19
1
12:19:30
Page 1 of 1
Get Study Cases
Get DPF Limit Violation
Get Discrete Measurements
Trace
Circuit Violations
Switch Status
5
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

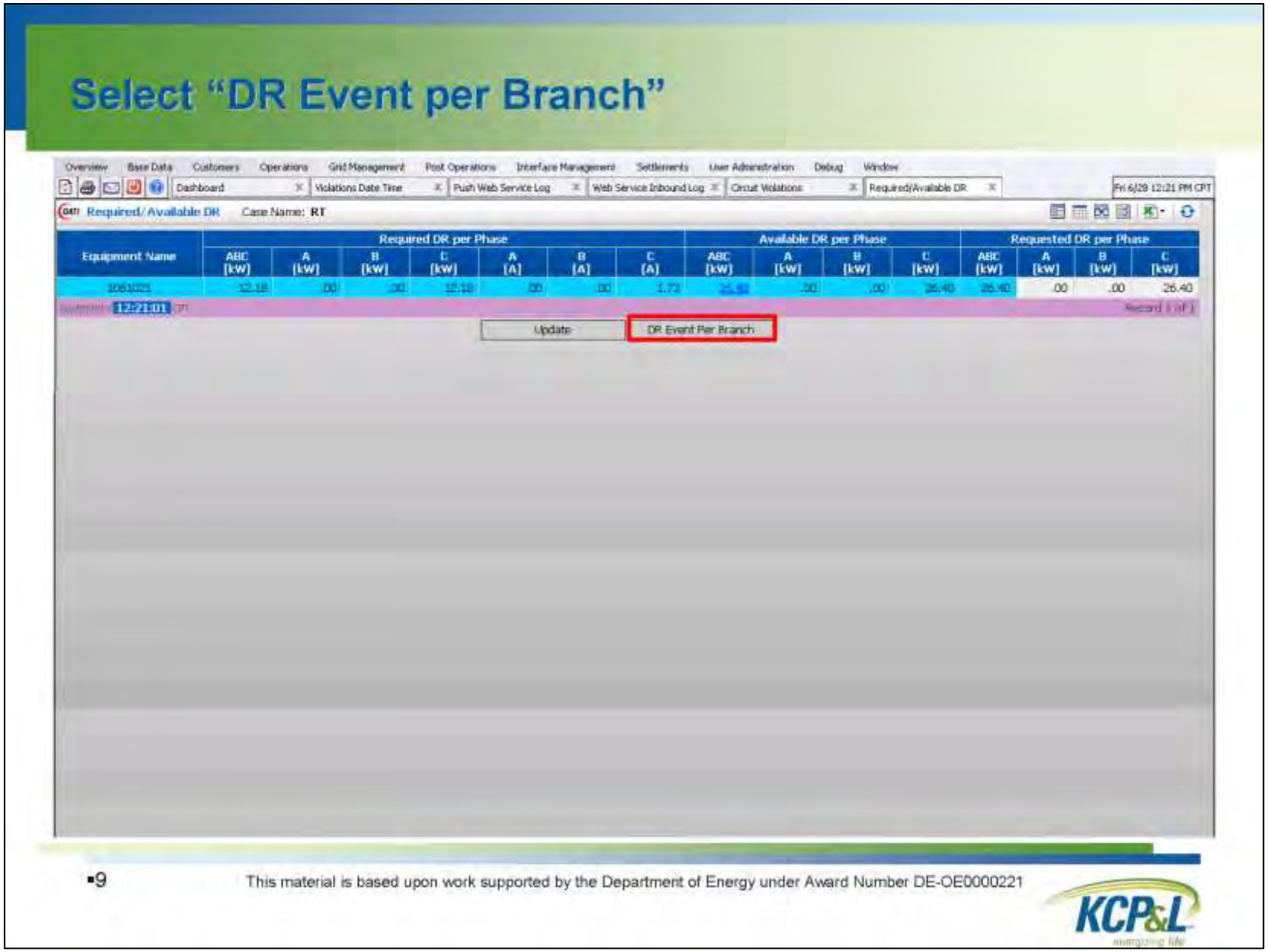

List of Circuit Violations
Overview
Base Data
Customers
Operations
Grid Management
Post Operations
Interface Management
Settlements
User Administration
Debug
Window
Dashboard
Violations Date Time
Push Web Service Log
Web Service Inbound Log
Circuit Violations
Circuit Violations
Case Name: RT
Equipment Name
Violation [%]
Limit ABC [A]
Current ABC [A]
Limit Per Phase [A]
Phase A [A]
Phase B [A]
Phase C [A]
Date Time
Description
Chosen for DR
1061021
1730.00
.10
1.83
.10
.00
.00
1.83
06/28/2013 16:19 CPT
Overload
12:20:02 CPT
Record 1 of 1
Grid Aggregation
Required/Available DR
6
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L
energizing life

Select "Grid Aggregation"

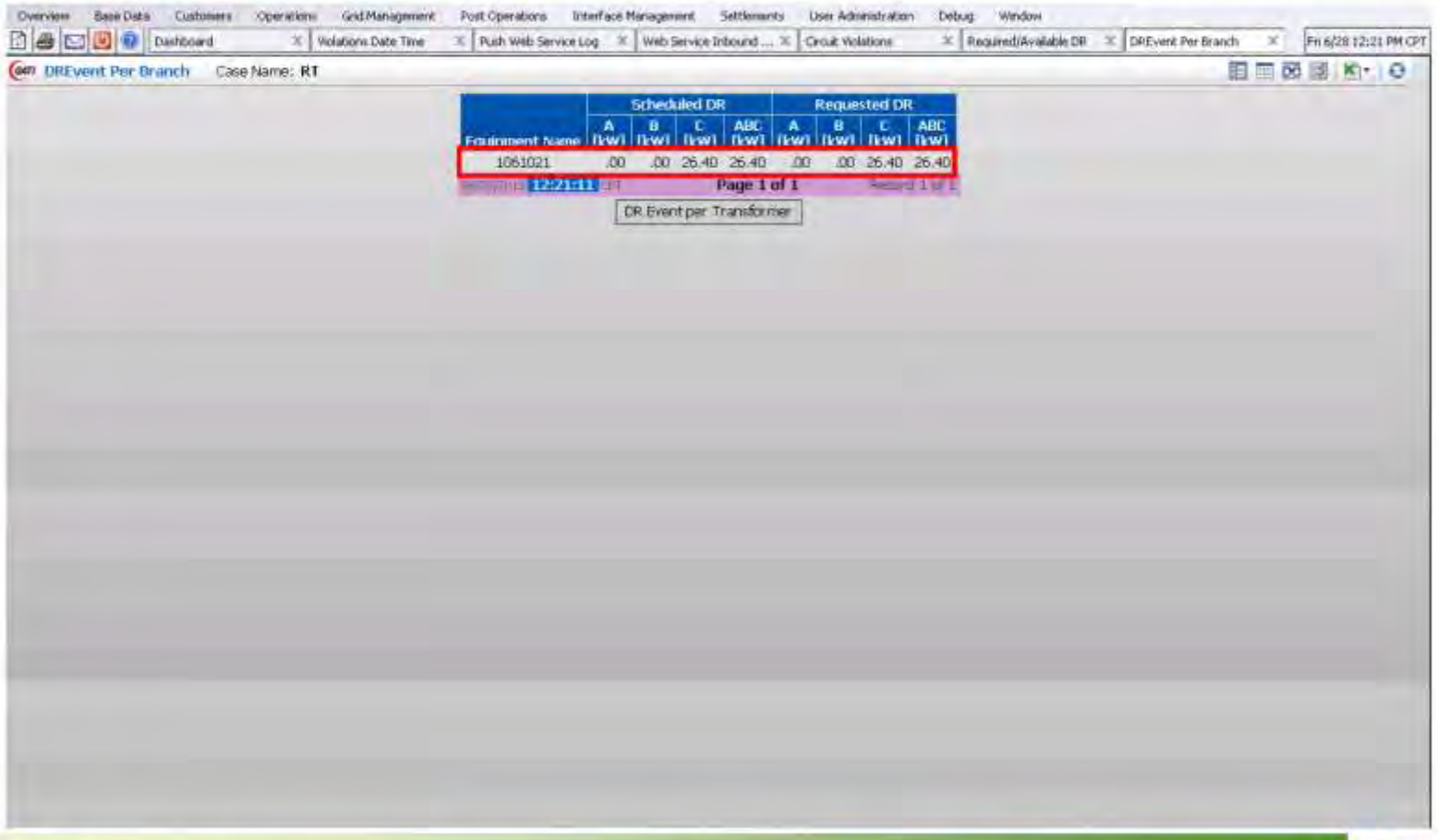


This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

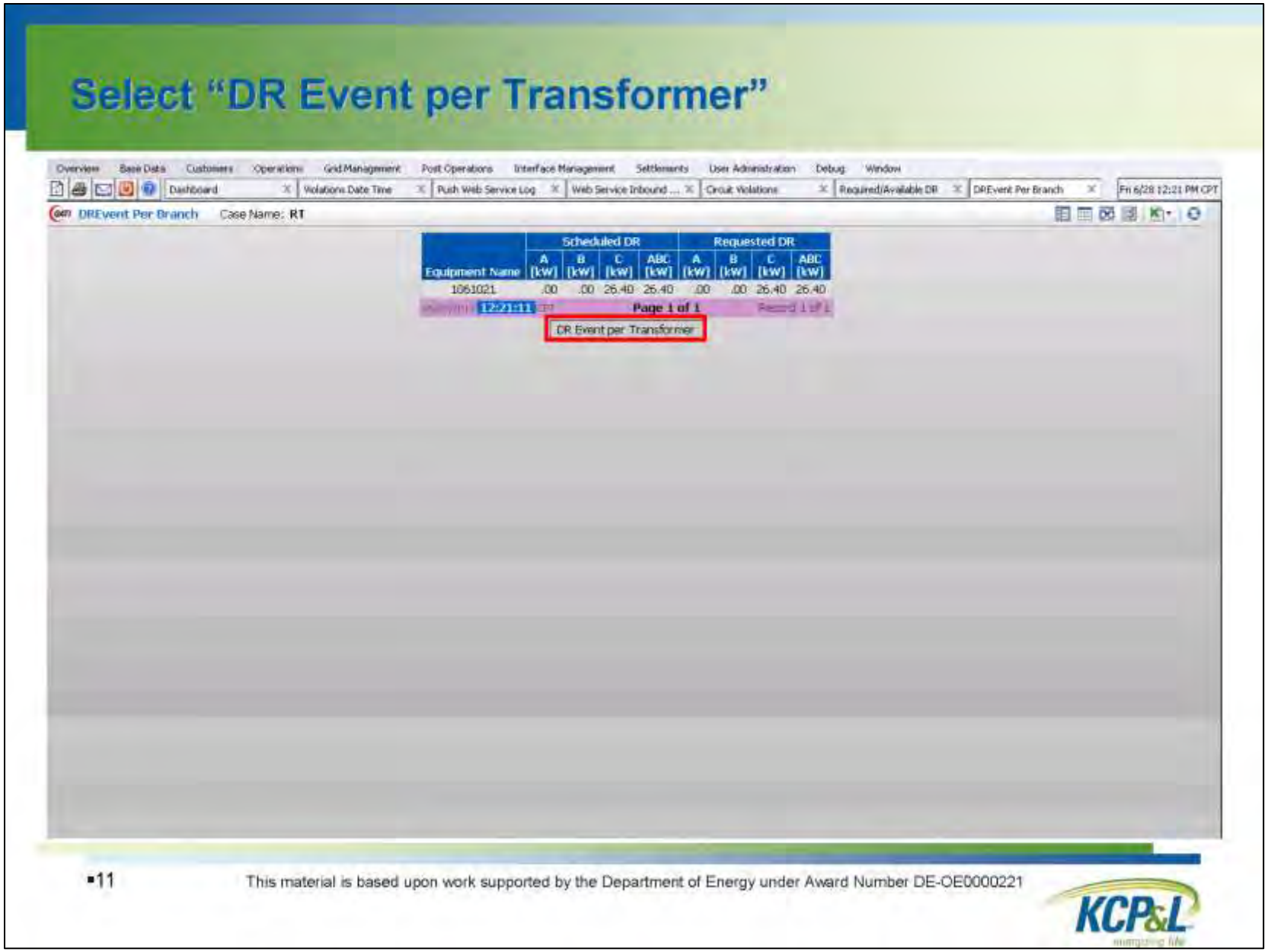

List of Available DR
Overview Base Data Customers Operations Grid Management Post Operations Interface Management Settlements User Administration Debug Window
Dashboard
Violations Date Time
Push Web Service Log
Web Service Inbound Log
Circuit Violations
Required/Available DR
Fri 6/28 12:21 PM CPT
Required/Available DR Case Name: RT
Equipment Name
Required DR per Phase
Available DR per Phase
Requested DR per Phase
ABC [kW] A [kW] B [kW] C [kW] A [A] B [A] C [A]
1061021 12.18 .00 .00 12.18 .00 .00 1.73 26.40 .00 .00 26.40 26.40 .00 .00 26.40
12:21:01
Update
DR Event Per Branch
8
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L
energizing life


Select "DR Event per Branch"
Overview Base Data Customers Operations Grid Management Post Operations Interface Management Settlements User Administration Debug Window
Dashboard
Violations Date Time
Push Web Service Log
Web Service Inbound Log
Circuit Violations
Required/Available DR
Fri 6/28 12:21 PM CPT
Required/Available DR Case Name: RT
Equipment Name
Required DR per Phase
Available DR per Phase
Requested DR per Phase
ABC [kW]
A [kW]
B [kW]
C [kW]
A [A]
B [A]
C [A]
1061021
12:21:01
Update
DR Event Per Branch
9
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L
energizing life

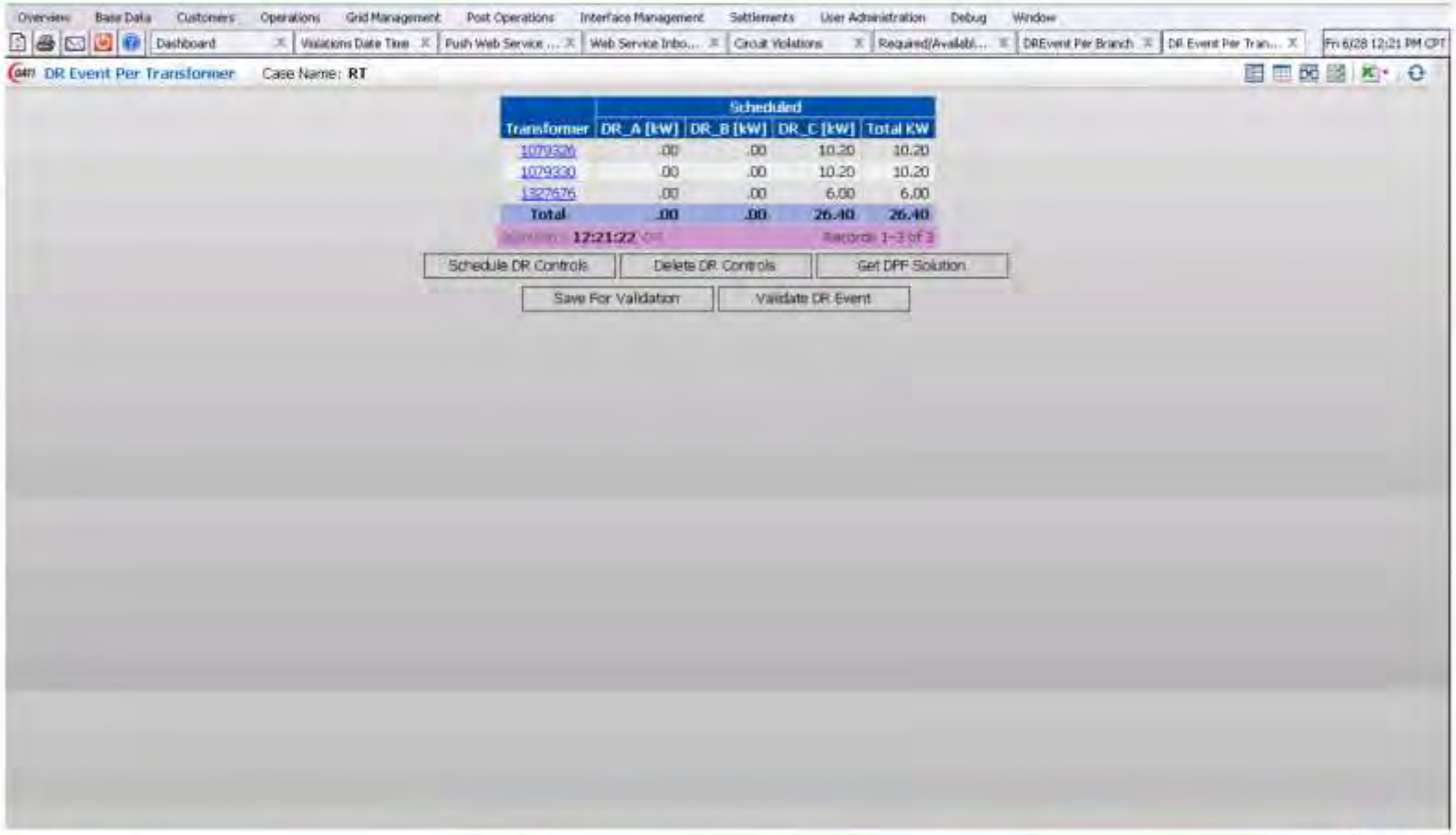
List of DR Events per Branch



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

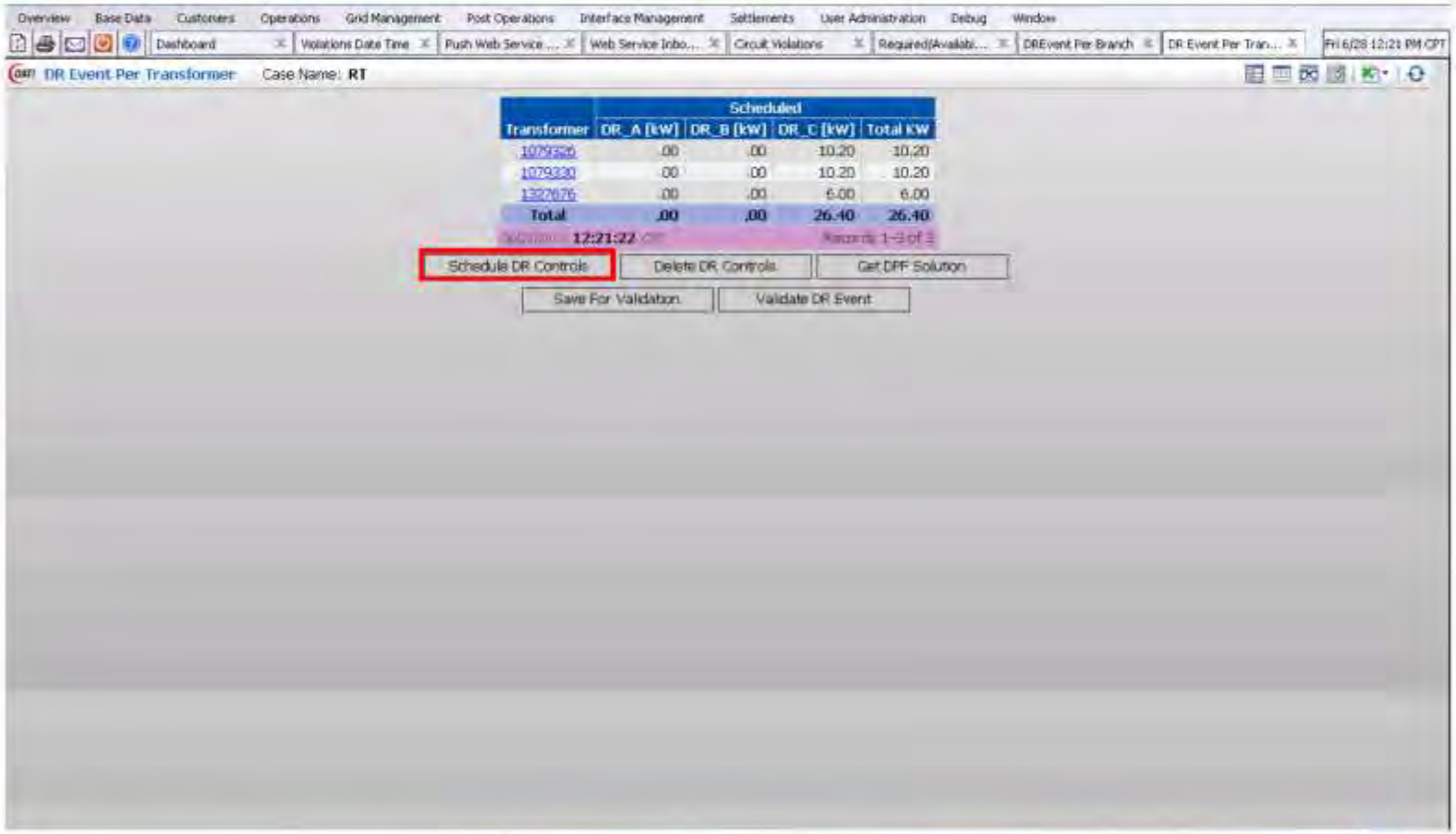

Select "DR Event per Transformer"
Overview Base Data Customers Operations Grid Management Post Operations Interface Management Settlements User Administration Debug Window
Dashboard
Violations Date Time
Push Web Service Log
Web Service Inbound ...
Circuit Violations
Required/Available DR
DREvent Per Branch
Fri 6/28 12:21 PM CPT
DREvent Per Branch
Case Name: RT
Scheduled DR
Requested DR
Equipment Name
A [kW]
B [kW]
C [kW]
ABC [kW]
A [kW]
B [kW]
C [kW]
ABC [kW]
1061021
.00
.00
26.40
26.40
.00
.00
26.40
26.40
12:21:11
Page 1 of 1
DR Event per Transformer
11
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

List of DR Event per Transformer

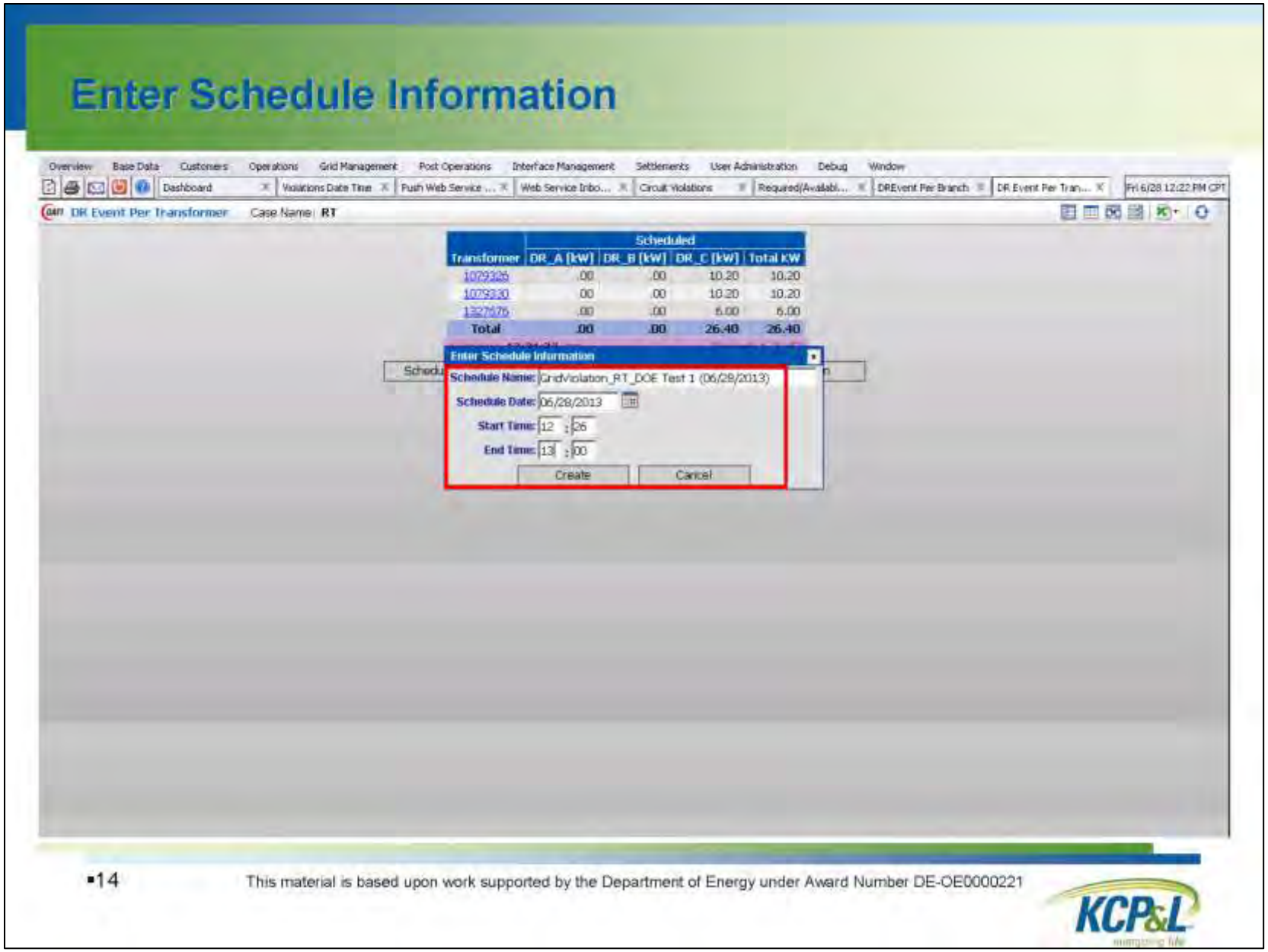


This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

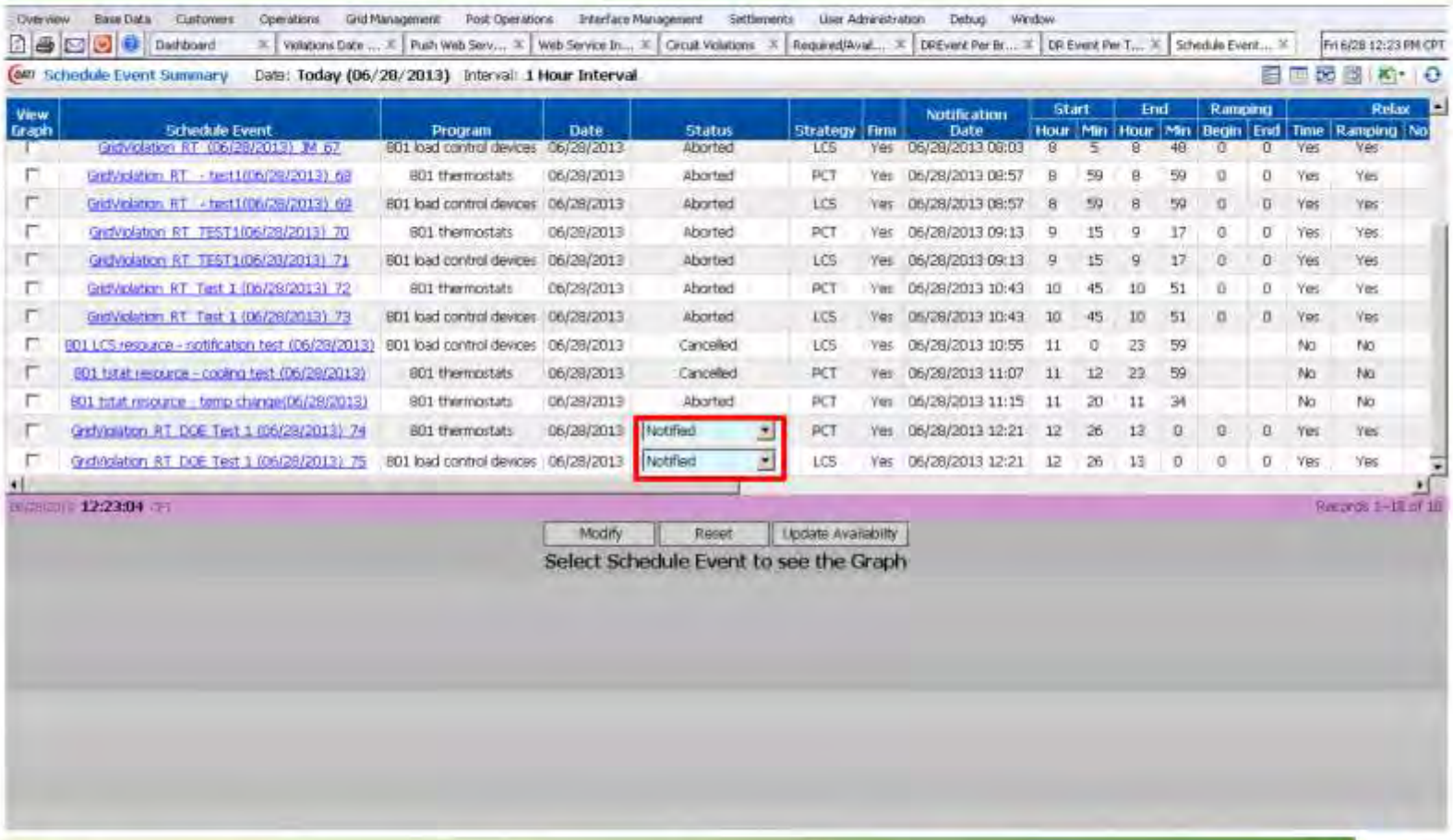
Select "Schedule DR Controls"



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221


Enter Schedule Information
Overview Base Data Customers Operations Grid Management Post Operations Interface Management Settlements User Administration Debug Window
Dashboard
Violations Date Time
Push Web Service ...
Web Service Inbo...
Circuit Violations
Required(Availabl...
DREvent Per Branch
DR Event Per Tran...
Fri 6/28 12:22 PM CDT
DR Event Per Transformer
Case Name: RT
Scheduled
Transformer
DR_A [kW]
DR_B [kW]
DR_C [kW]
Total KW
1079326 .00 .00 10.20 10.20
1079330 .00 .00 10.20 10.20
1327676 .00 .00 6.00 6.00
Total .00 .00 26.40 26.40
Enter Schedule Information
Schedule Name: GridViolation_RT_DOE Test 1 (06/28/2013)
Schedule Date: 06/28/2013
Start Time: 12 : 26
End Time: 13 : 00
Create
Cancel
14
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

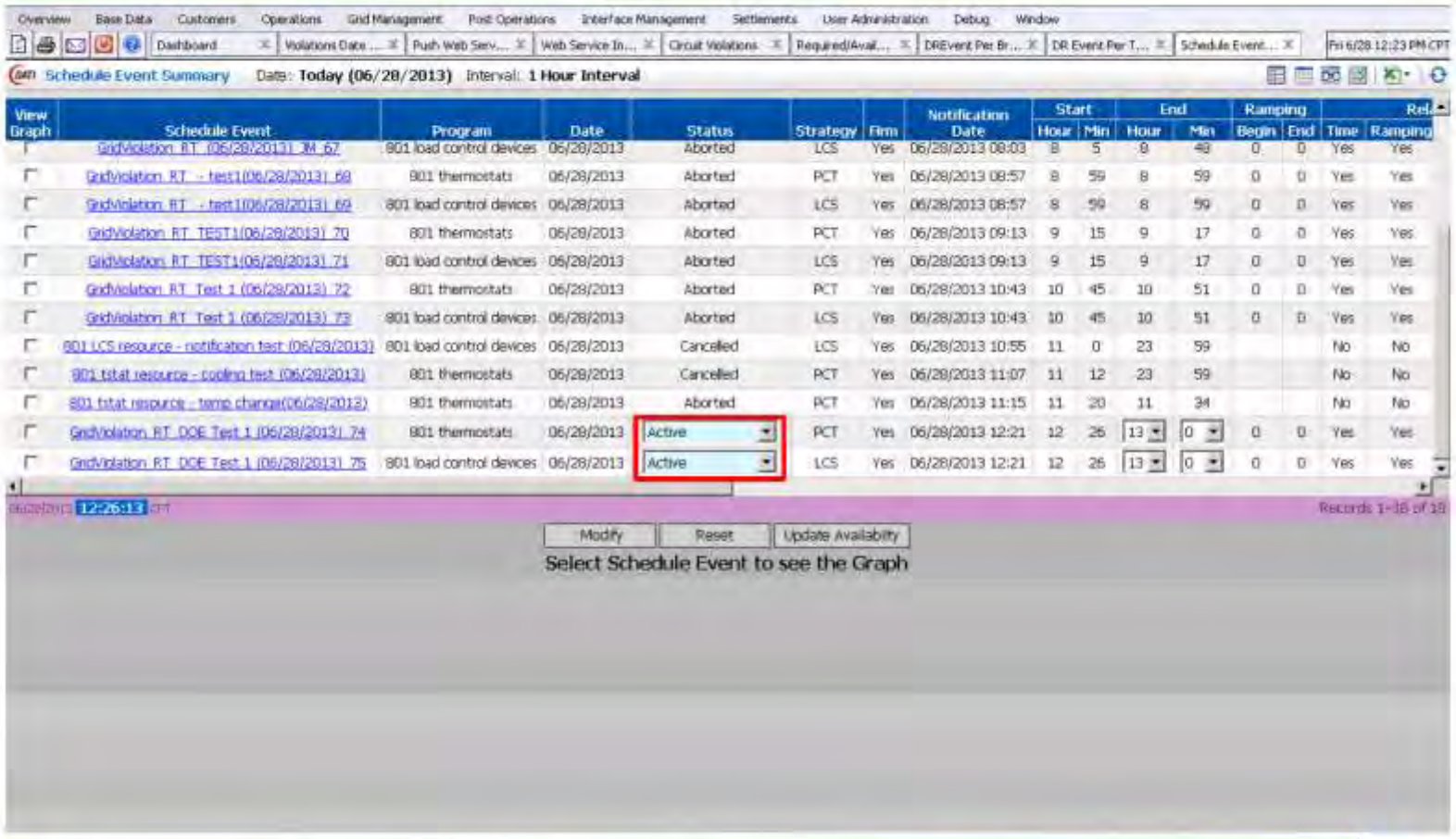
List of Committed DR Events



View Graph	Schedule Event	Program	Date	Status	Strategy	Firm	Notification Date	Start Hour	Start Min	End Hour	End Min	Ramping Begin	Ramping End	Relax Time	Relax Ramping
	GridViolation_RT_(06/28/2013)_JM_67	801 load control devices	06/28/2013	Aborted	LCS	Yes	06/28/2013 08:03	8	5	8	40	0	0	Yes	Yes
	GridViolation_RT_-test1(06/28/2013)_68	801 thermostats	06/28/2013	Aborted	PCT	Yes	06/28/2013 08:57	8	59	8	59	0	0	Yes	Yes
	GridViolation_RT_-test1(06/28/2013)_69	801 load control devices	06/28/2013	Aborted	LCS	Yes	06/28/2013 08:57	8	59	8	59	0	0	Yes	Yes
	GridViolation_RT_TEST1(06/28/2013)_70	801 thermostats	06/28/2013	Aborted	PCT	Yes	06/28/2013 09:13	9	15	9	17	0	0	Yes	Yes
	GridViolation_RT_TEST1(06/28/2013)_71	801 load control devices	06/28/2013	Aborted	LCS	Yes	06/28/2013 09:13	9	15	9	17	0	0	Yes	Yes
	GridViolation_RT_Test 1 (06/28/2013)_72	801 thermostats	06/28/2013	Aborted	PCT	Yes	06/28/2013 10:43	10	45	10	51	0	0	Yes	Yes
	GridViolation_RT_Test 1 (06/28/2013)_73	801 load control devices	06/28/2013	Aborted	LCS	Yes	06/28/2013 10:43	10	45	10	51	0	0	Yes	Yes
	801 LCS resource - notification test (06/28/2013)	801 load control devices	06/28/2013	Cancelled	LCS	Yes	06/28/2013 10:55	11	0	23	59			No	No
	801 tstat resource - cooling test (06/28/2013)	801 thermostats	06/28/2013	Cancelled	PCT	Yes	06/28/2013 11:07	11	12	23	59			No	No
	801 tstat resource - temp change(06/28/2013)	801 thermostats	06/28/2013	Aborted	PCT	Yes	06/28/2013 11:15	11	20	11	34			No	No
	GridViolation_RT_DOE Test 1 (06/28/2013)_74	801 thermostats	06/28/2013	Notified	PCT	Yes	06/28/2013 12:21	12	26	13	0	0	0	Yes	Yes
	GridViolation_RT_DOE Test 1 (06/28/2013)_75	801 load control devices	06/28/2013	Notified	LCS	Yes	06/28/2013 12:21	12	26	13	0	0	0	Yes	Yes

15 This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Status Changes to Active After Event Starts



View Graph	Schedule Event	Program	Date	Status	Strategy	Firm	Notification Date	Start Hour	Start Min	End Hour	End Min	Ramping Begin	Ramping End	Time	Ramping
	GridViolation_RT_(06/28/2013)_3M_67	801 load control devices	06/28/2013	Aborted	LCS	Yes	06/28/2013 08:03	8	5	9	49	0	0	Yes	Yes
	GridViolation_RT_-_test1(06/28/2013)_68	801 thermostats	06/28/2013	Aborted	PCT	Yes	06/28/2013 08:57	8	59	8	59	0	0	Yes	Yes
	GridViolation_RT_-_test1(06/28/2013)_69	801 load control devices	06/28/2013	Aborted	LCS	Yes	06/28/2013 08:57	8	59	8	59	0	0	Yes	Yes
	GridViolation_RT_TEST1(06/28/2013)_70	801 thermostats	06/28/2013	Aborted	PCT	Yes	06/28/2013 09:13	9	15	9	17	0	0	Yes	Yes
	GridViolation_RT_TEST1(06/28/2013)_71	801 load control devices	06/28/2013	Aborted	LCS	Yes	06/28/2013 09:13	9	15	9	17	0	0	Yes	Yes
	GridViolation_RT_Test_1_(06/28/2013)_72	801 thermostats	06/28/2013	Aborted	PCT	Yes	06/28/2013 10:43	10	45	10	51	0	0	Yes	Yes
	GridViolation_RT_Test_1_(06/28/2013)_73	801 load control devices	06/28/2013	Aborted	LCS	Yes	06/28/2013 10:43	10	45	10	51	0	0	Yes	Yes
	801 LCS resource - notification test (06/28/2013)	801 load control devices	06/28/2013	Cancelled	LCS	Yes	06/28/2013 10:55	11	0	23	59			No	No
	801 tstat resource - cooling test (06/28/2013)	801 thermostats	06/28/2013	Cancelled	PCT	Yes	06/28/2013 11:07	11	12	23	59			No	No
	801 tstat resource - temp change(06/28/2013)	801 thermostats	06/28/2013	Aborted	PCT	Yes	06/28/2013 11:15	11	20	11	34			No	No
	GridViolation_RT_DOE_Test_1_(06/28/2013)_74	801 thermostats	06/28/2013	Active	PCT	Yes	06/28/2013 12:21	12	26	13	0	0	0	Yes	Yes
	GridViolation_RT_DOE_Test_1_(06/28/2013)_75	801 load control devices	06/28/2013	Active	LCS	Yes	06/28/2013 12:21	12	26	13	0	0	0	Yes	Yes

▪16 This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Launch AHE Command Center

▪17

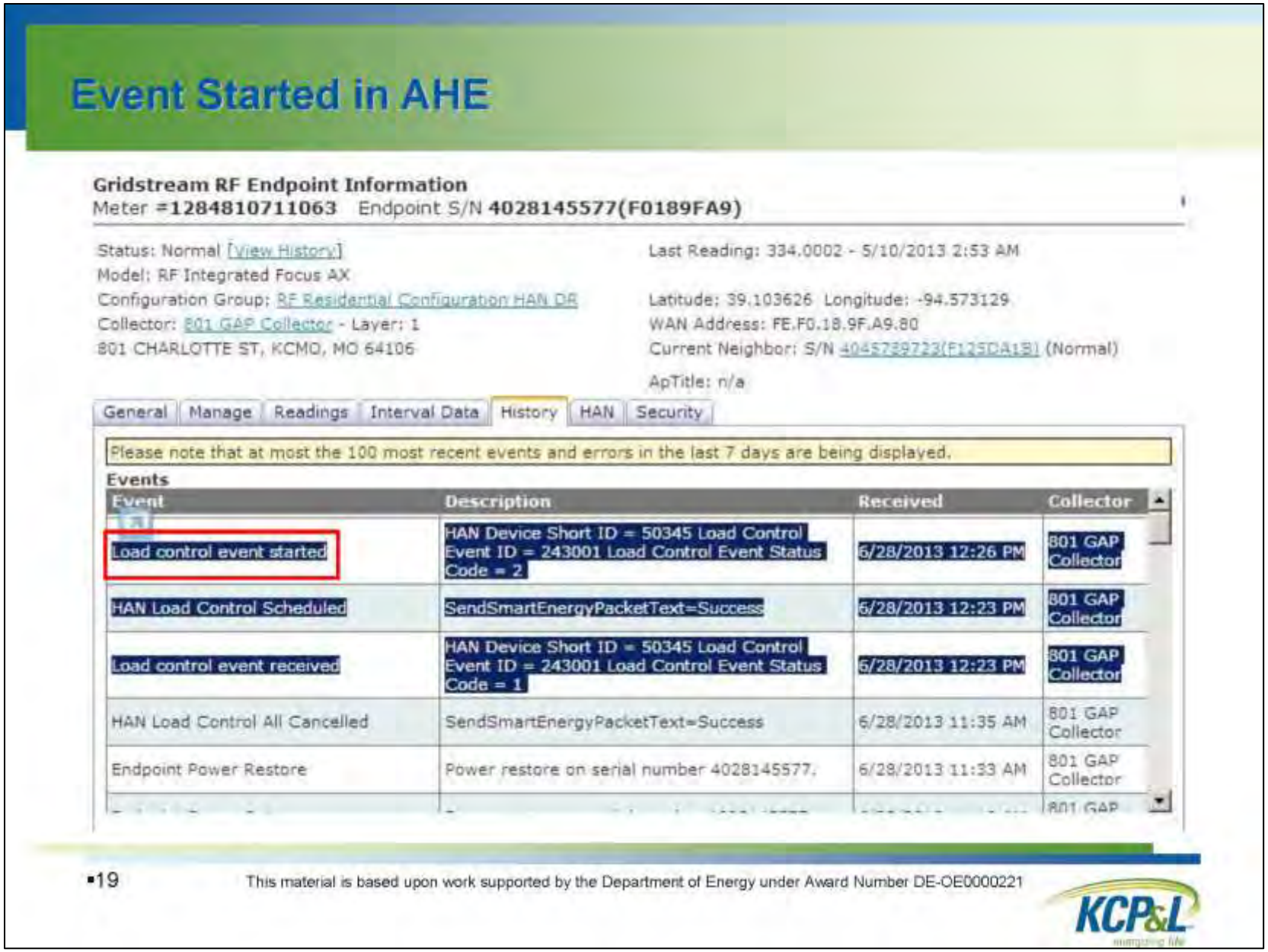
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

KCP&L energizing life

Enter Meter Number

▪18

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221


Event Started in AHE
Gridstream RF Endpoint Information
Meter #1284810711063 Endpoint S/N 4028145577(F0189FA9)
Status: Normal [View History]
Model: RF Integrated Focus AX
Configuration Group: RF Residential Configuration HAN DR
Collector: 801 GAP Collector - Layer: 1
801 CHARLOTTE ST, KCMO, MO 64106
Last Reading: 334.0002 - 5/10/2013 2:53 AM
Latitude: 39.103626 Longitude: -94.573129
WAN Address: FE.F0.18.9F.A9.80
Current Neighbor: S/N 4045739723(F125DA1B) (Normal)
ApTitle: n/a
General
Manage
Readings
Interval Data
History
HAN
Security
Please note that at most the 100 most recent events and errors in the last 7 days are being displayed.
Events
Event
Description
Received
Collector
Load control event started
HAN Device Short ID = 50345 Load Control Event ID = 243001 Load Control Event Status Code = 2
6/28/2013 12:26 PM
801 GAP Collector
HAN Load Control Scheduled
SendSmartEnergyPacketText=Success
6/28/2013 12:23 PM
801 GAP Collector
Load control event received
HAN Device Short ID = 50345 Load Control Event ID = 243001 Load Control Event Status Code = 1
6/28/2013 12:23 PM
801 GAP Collector
HAN Load Control All Cancelled
SendSmartEnergyPacketText=Success
6/28/2013 11:35 AM
801 GAP Collector
Endpoint Power Restore
Power restore on serial number 4028145577.
6/28/2013 11:33 AM
801 GAP Collector
19
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

Event Completed in AHE

Gridstream RF Endpoint Information
Meter #**1284810711063** Endpoint S/N **4028145577(F0189FA9)**

Status: Normal [View History]
Model: RF Integrated Focus AX
Configuration Group: RF Residential Configuration HAN DR
Collector: 801 GAP Collector - Layer: 2
801 CHARLOTTE ST, KCMO, MO 64106

Last Reading: 334.0002 - 5/10/2013 2:53 AM
Latitude: 39.103626 Longitude: -94.573129
WAN Address: FE.F0.18.9F.A9.80
Current Neighbor: S/N 4045789723(F125DA1B) (Normal)
ApTitle: n/a

General | Manage | Readings | Interval Data | History | HAN | Security

Please note that at most the 100 most recent events and errors in the last 7 days are being displayed.

Events

Event	Description	Received	Collector
Load control event completed	HAN Device Short ID = 50345 Load Control Event ID = 243001 Load Control Event Status Code = 3	6/28/2013 1:00 PM	801 GAP Collector
Load control event started	HAN Device Short ID = 50345 Load Control Event ID = 243001 Load Control Event Status Code = 2	6/28/2013 12:26 PM	801 GAP Collector
HAN Load Control Scheduled	SendSmartEnergyPacketText=Success	6/28/2013 12:23 PM	801 GAP Collector
Load control event received	HAN Device Short ID = 50345 Load Control Event ID = 243001 Load Control Event Status Code = 1	6/28/2013 12:23 PM	801 GAP Collector
HAN Load Control All Cancelled	SendSmartEnergyPacketText=Success	6/28/2013 11:35 AM	801 GAP Collector

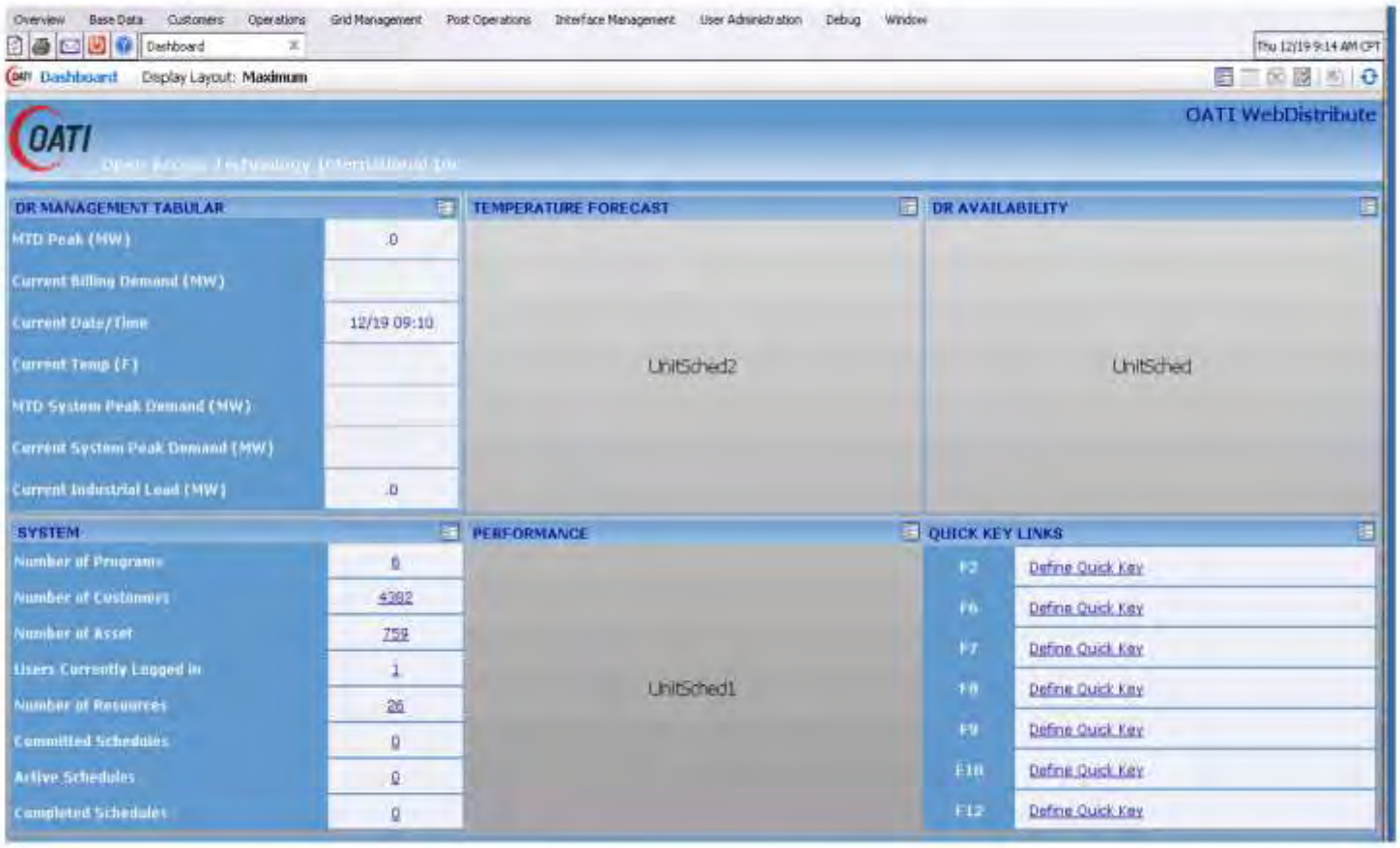
▪20

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

KCP&L energizing life

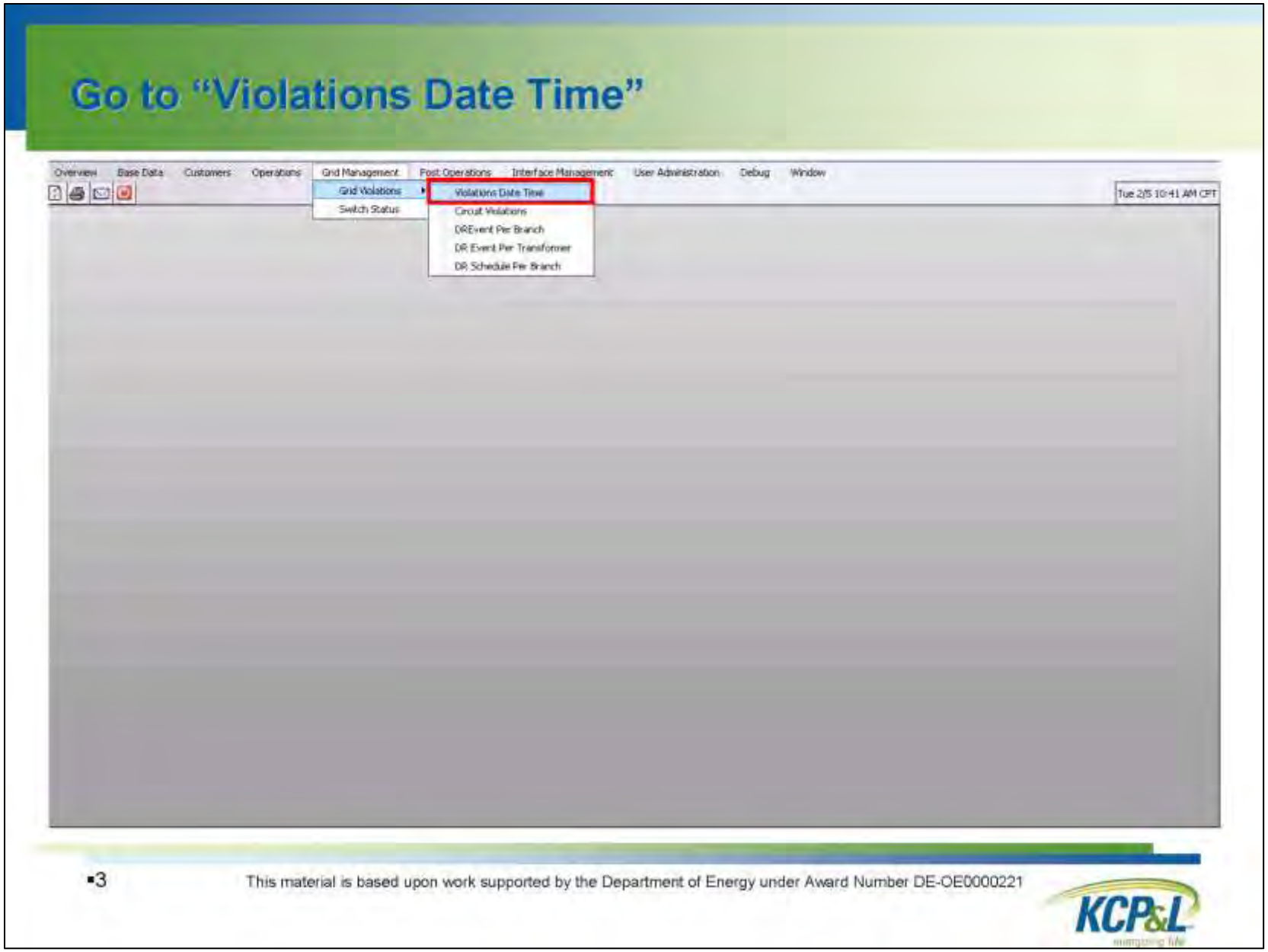

Demand Response – HAN Devices
- KC Green Impact Zone Initiative
- DOE Regional SmartGrid Demonstration Program
- EPRI SmartGrid Demonstration Program
KCP&L
SmartGrid
the future of energy

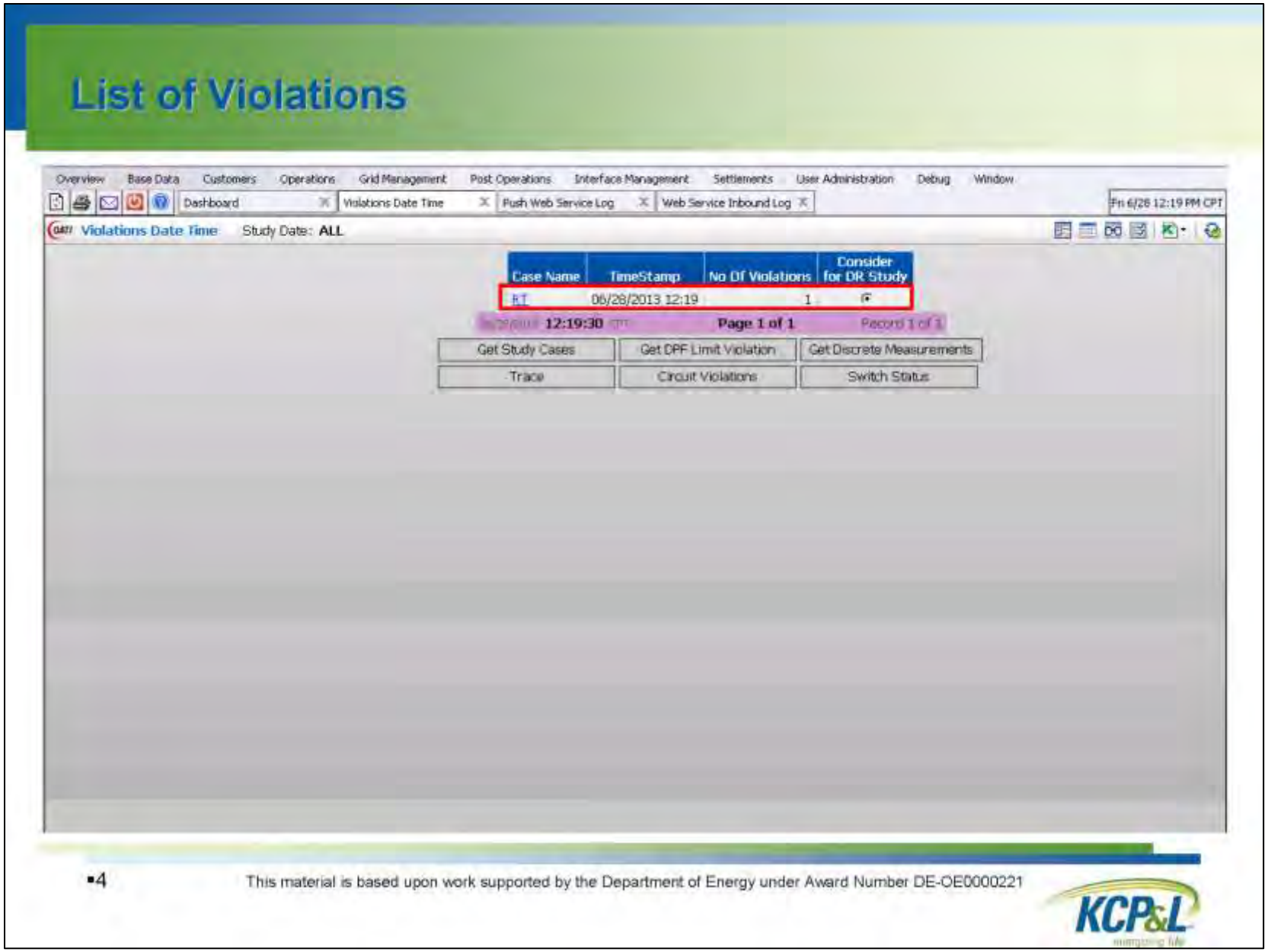
Launch DERM WebUI

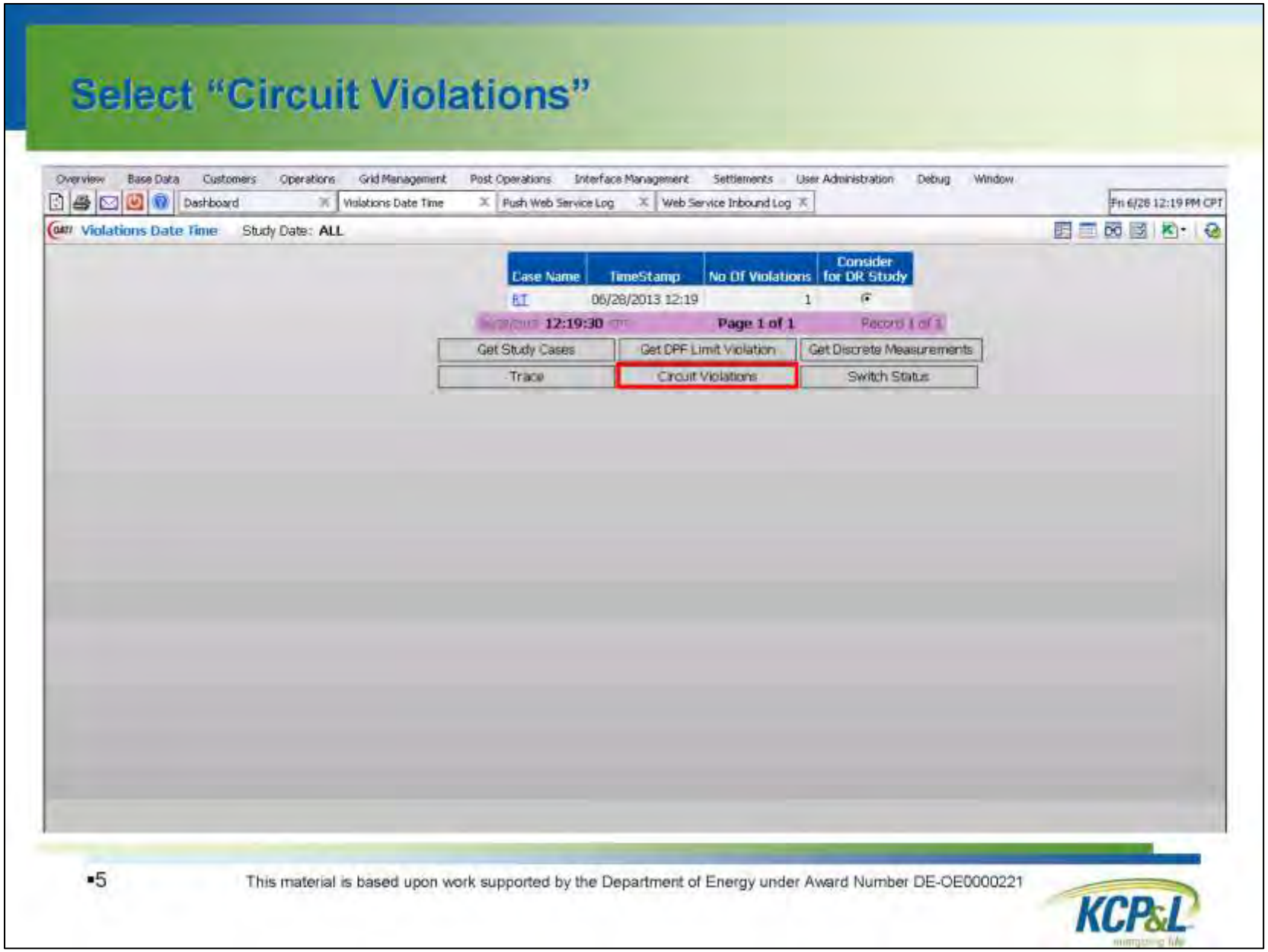


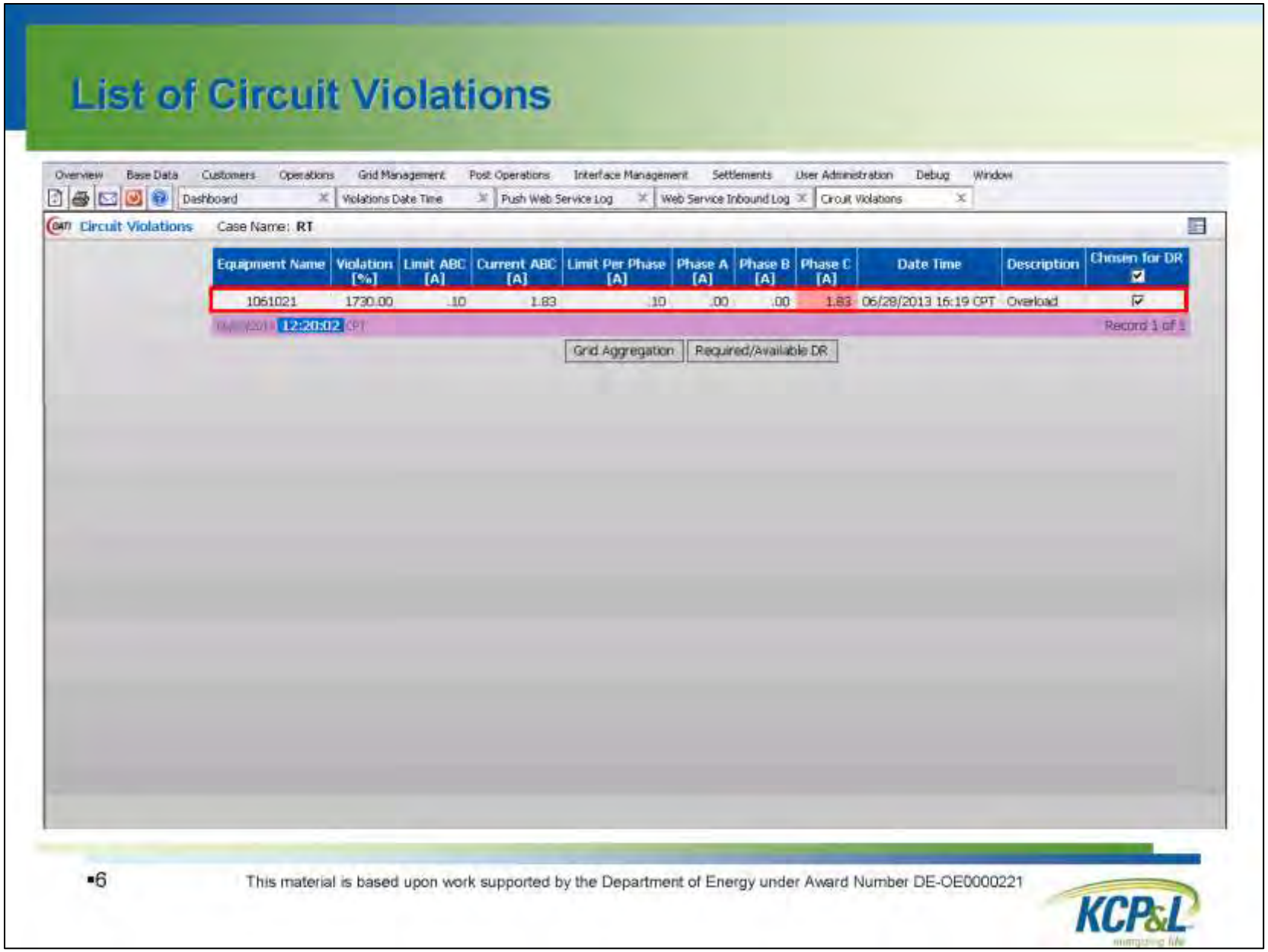
▪2

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

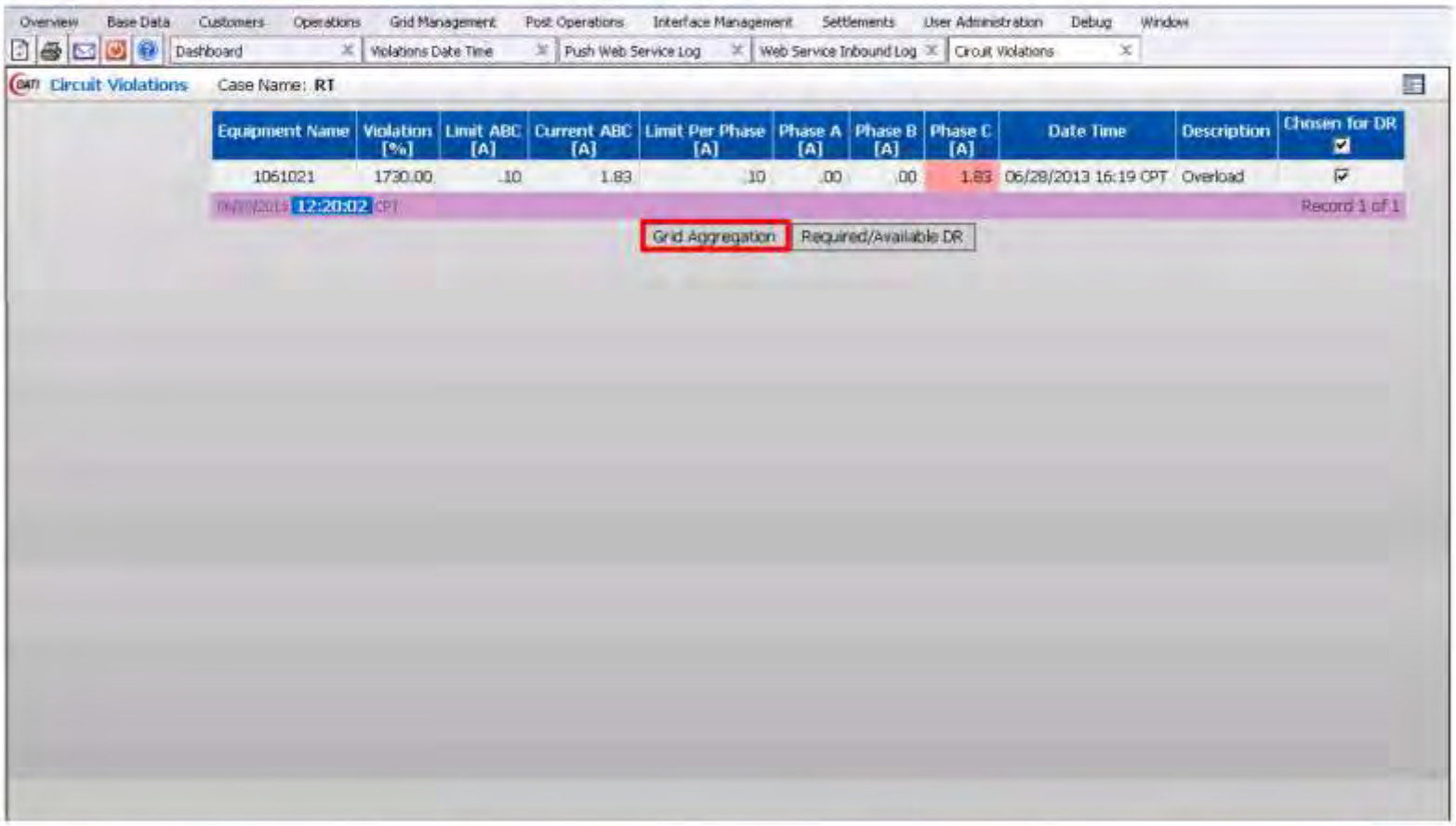

Go to "Violations Date Time"
Overview
Base Data
Customers
Operations
Grid Management
Post Operations
Interface Management
User Administration
Debug
Window
Grid Violations
Switch Status
Violations Date Time
Circuit Violations
DREvent Per Branch
DR Event Per Transformer
DR Schedule Per Branch
Tue 2/5 10:41 AM CPT
3
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L


List of Violations
Overview
Base Data
Customers
Operations
Grid Management
Post Operations
Interface Management
Settlements
User Administration
Debug
Window
Dashboard
Violations Date Time
Push Web Service Log
Web Service Inbound Log
Fri 6/28 12:19 PM CPT
Violations Date Time
Study Date: ALL
Case Name
TimeStamp
No Of Violations
Consider for DR Study
RT
06/28/2013 12:19
1
12:19:30
Page 1 of 1
Record 1 of 1
Get Study Cases
Get DPF Limit Violation
Get Discrete Measurements
Trace
Circuit Violations
Switch Status
4
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

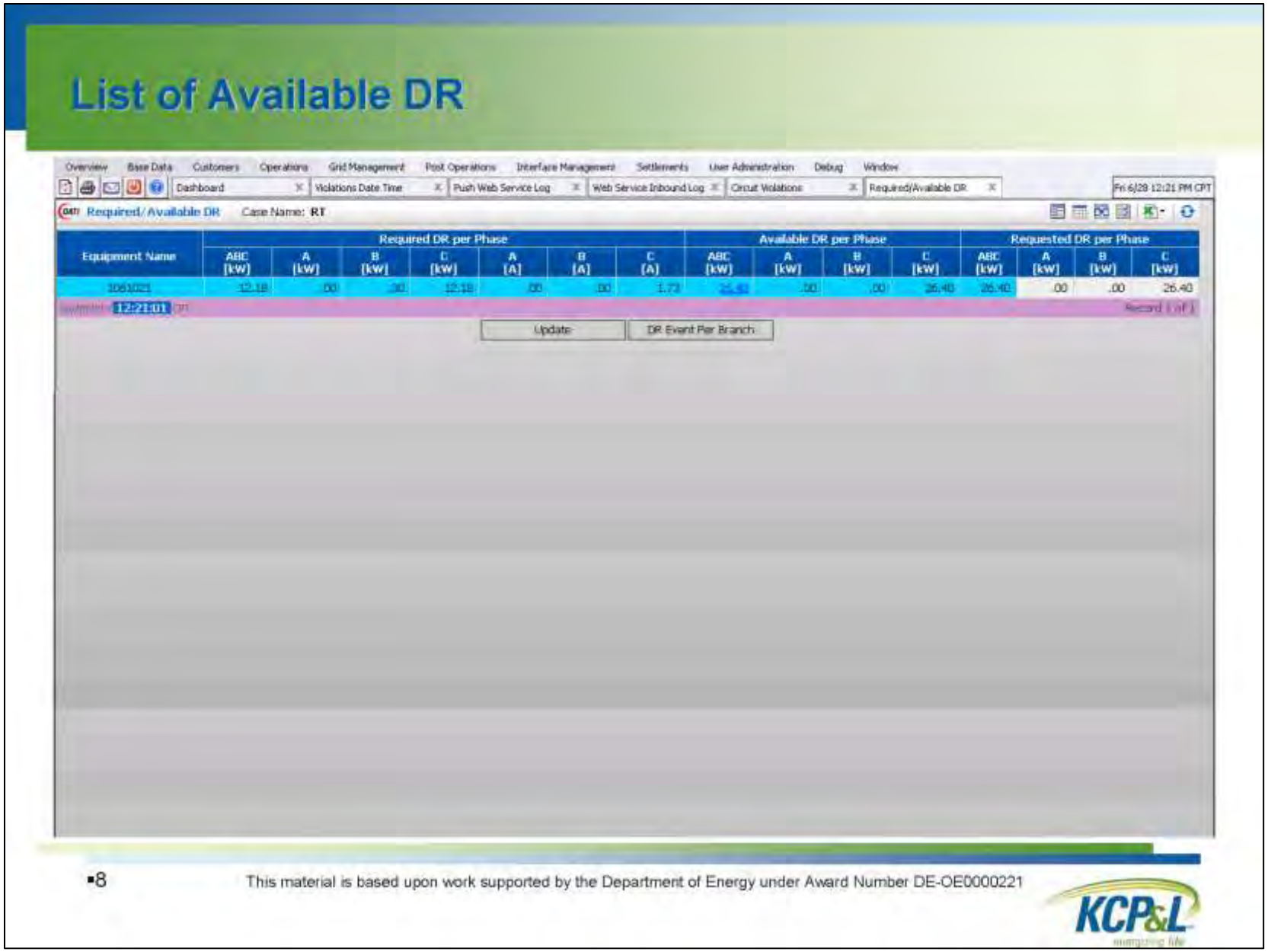

Select "Circuit Violations"
Overview
Base Data
Customers
Operations
Grid Management
Post Operations
Interface Management
Settlements
User Administration
Debug
Window
Dashboard
Violations Date Time
Push Web Service Log
Web Service Inbound Log
Violations Date Time
Study Date: ALL
Case Name
TimeStamp
No Of Violations
Consider for DR Study
RT
06/28/2013 12:19
1
12:19:30
Page 1 of 1
Get Study Cases
Get DPF Limit Violation
Get Discrete Measurements
Trace
Circuit Violations
Switch Status
5
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

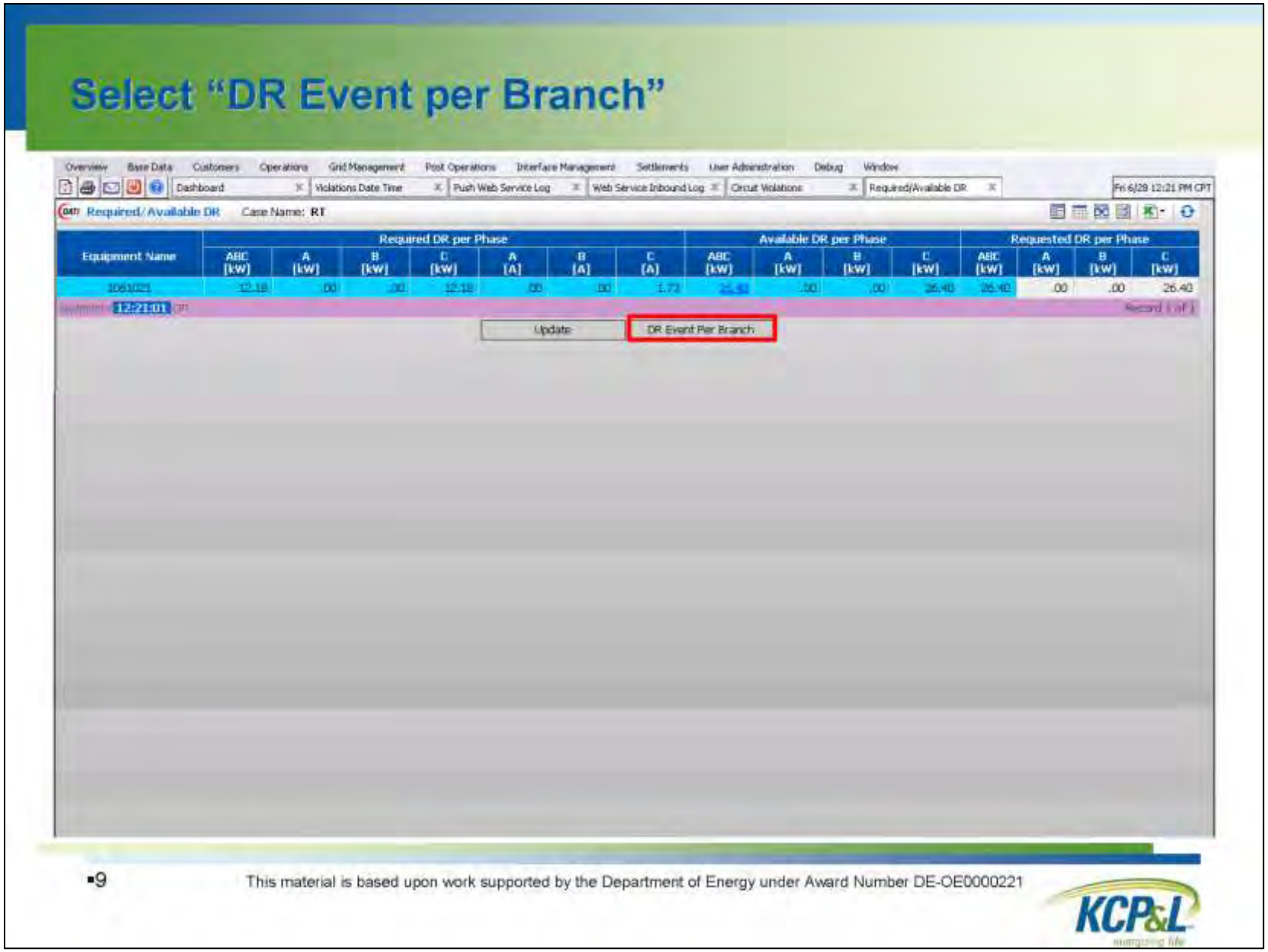

List of Circuit Violations
Overview
Base Data
Customers
Operations
Grid Management
Post Operations
Interface Management
Settlements
User Administration
Debug
Window
Dashboard
Violations Date Time
Push Web Service Log
Web Service Inbound Log
Circuit Violations
Circuit Violations
Case Name: RT
Equipment Name
Violation [%]
Limit ABC [A]
Current ABC [A]
Limit Per Phase [A]
Phase A [A]
Phase B [A]
Phase C [A]
Date Time
Description
Chosen for DR
1061021
1730.00
.10
1.83
.10
.00
.00
1.83
06/28/2013 16:19 CPT
Overload
12:20:02 CPT
Record 1 of 1
Grid Aggregation
Required/Available DR
6
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

Select "Grid Aggregation"

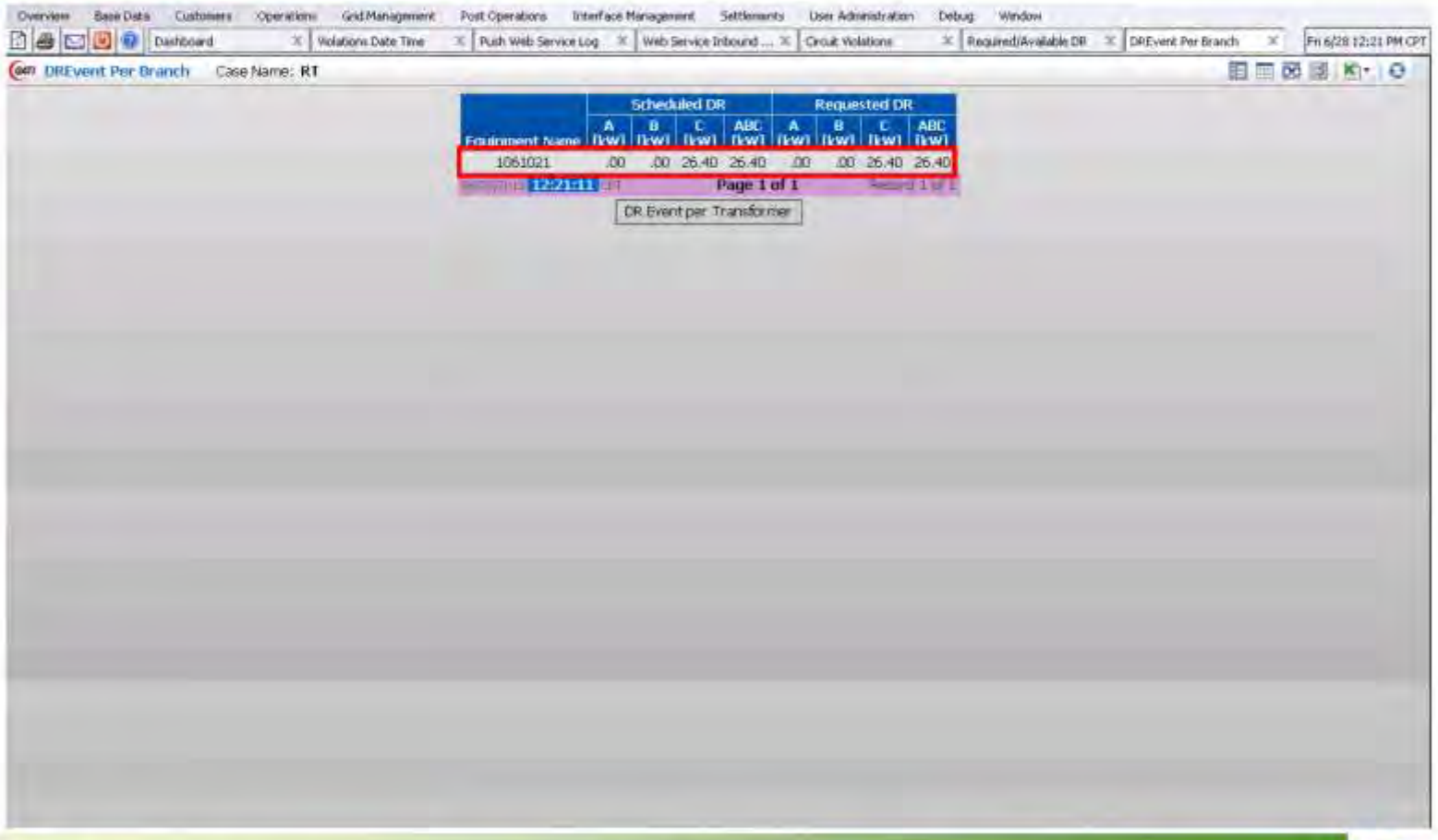


This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

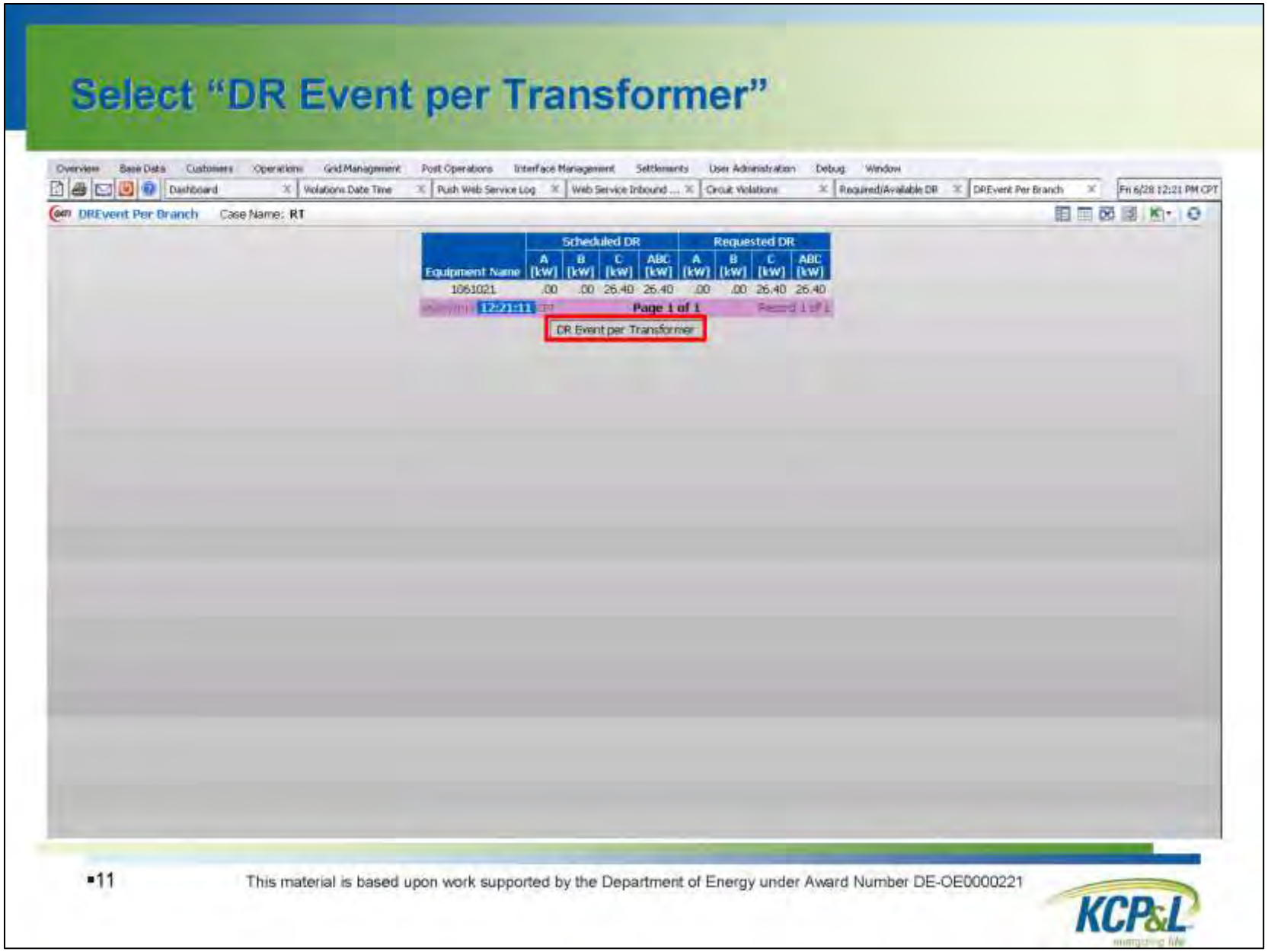

List of Available DR
Overview Base Data Customers Operations Grid Management Post Operations Interface Management Settlements User Administration Debug Window
Dashboard
Violations Date Time
Push Web Service Log
Web Service Inbound Log
Circuit Violations
Required/Available DR
Fri 6/28 12:21 PM CPT
Required/Available DR Case Name: RT
Equipment Name
Required DR per Phase
Available DR per Phase
Requested DR per Phase
ABC [kW] A [kW] B [kW] C [kW] A [A] B [A] C [A]
1061021 12.18 .00 .00 12.18 .00 .00 1.73 26.40 .00 .00 26.40 26.40 .00 .00 26.40
12:21:01
Update
DR Event Per Branch
8
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L
energizing life


Select "DR Event per Branch"
Overview Base Data Customers Operations Grid Management Post Operations Interface Management Settlements User Administration Debug Window
Dashboard
Violations Date Time
Push Web Service Log
Web Service Inbound Log
Circuit Violations
Required/Available DR
Fri 6/28 12:21 PM CPT
Required/Available DR Case Name: RT
Equipment Name
Required DR per Phase
Available DR per Phase
Requested DR per Phase
ABC [kW]
A [kW]
B [kW]
C [kW]
A [A]
B [A]
C [A]
1061021 12.18 .00 .00 12.18 .00 .00 1.73 26.40 .00 .00 26.40 26.40 .00 .00 26.40
12:21:01 CPT
Update
DR Event Per Branch
9
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

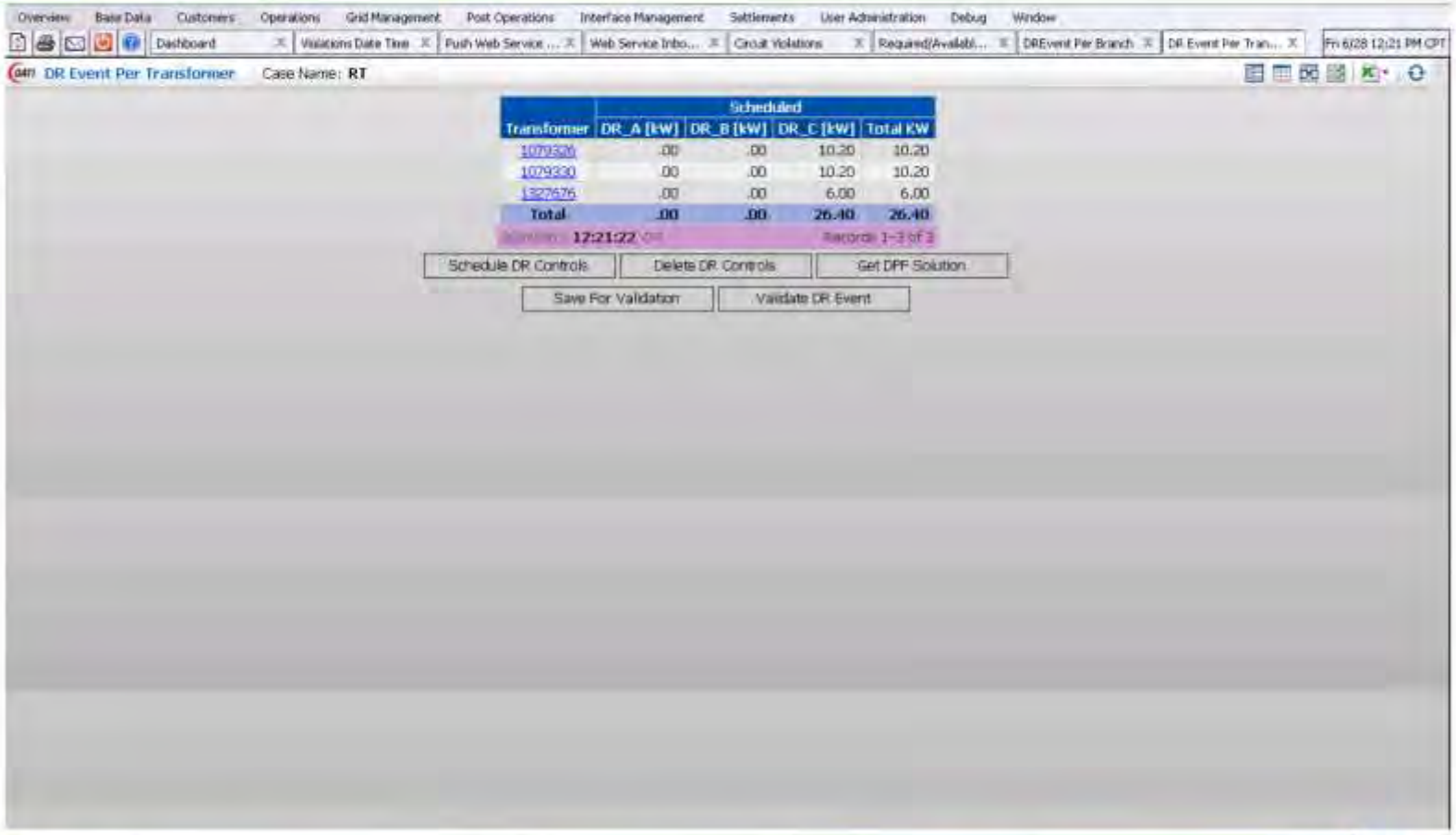
List of DR Events per Branch



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

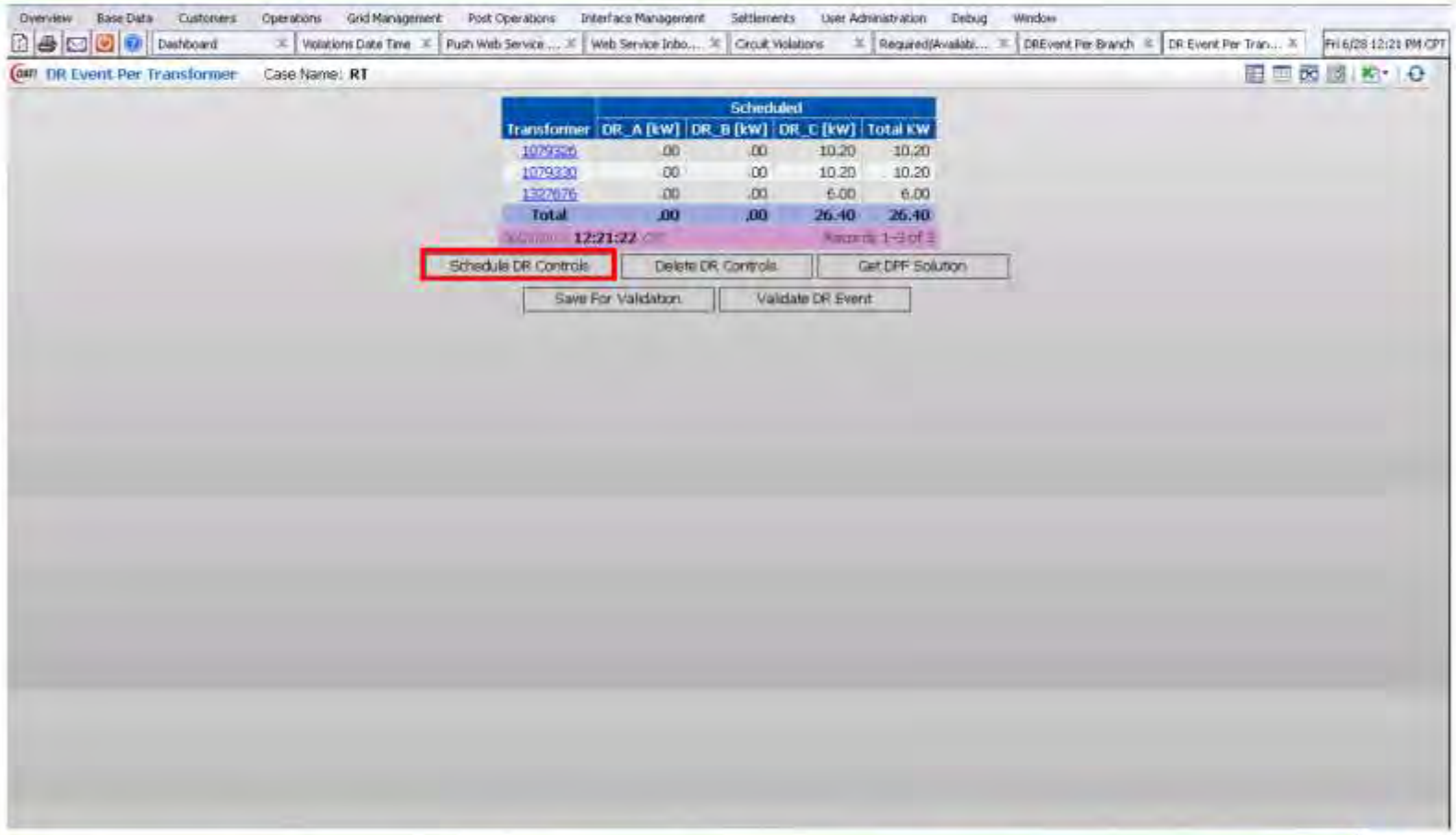

Select "DR Event per Transformer"
Overview Base Data Customers Operations Grid Management Post Operations Interface Management Settlements User Administration Debug Window
Dashboard
Violations Date Time
Push Web Service Log
Web Service Inbound ...
Circuit Violations
Required/Available DR
DREvent Per Branch
Fri 6/28 12:21 PM CPT
DREvent Per Branch
Case Name: RT
Scheduled DR
Requested DR
Equipment Name
A [kW]
B [kW]
C [kW]
ABC [kW]
A [kW]
B [kW]
C [kW]
ABC [kW]
1061021
.00
.00
26.40
26.40
.00
.00
26.40
26.40
12:21:11
Page 1 of 1
DR Event per Transformer
11
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

List of DR Event per Transformer

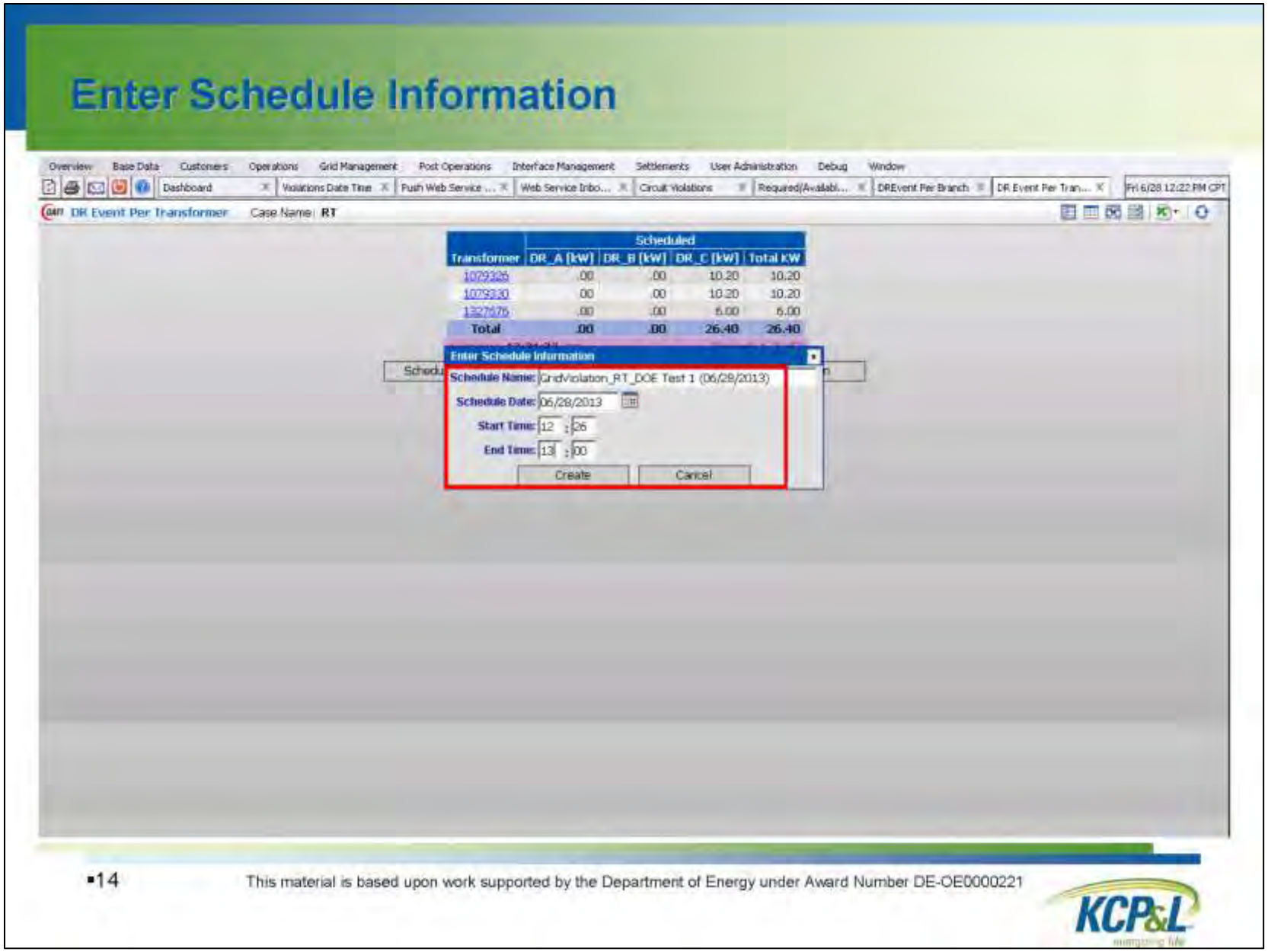


This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

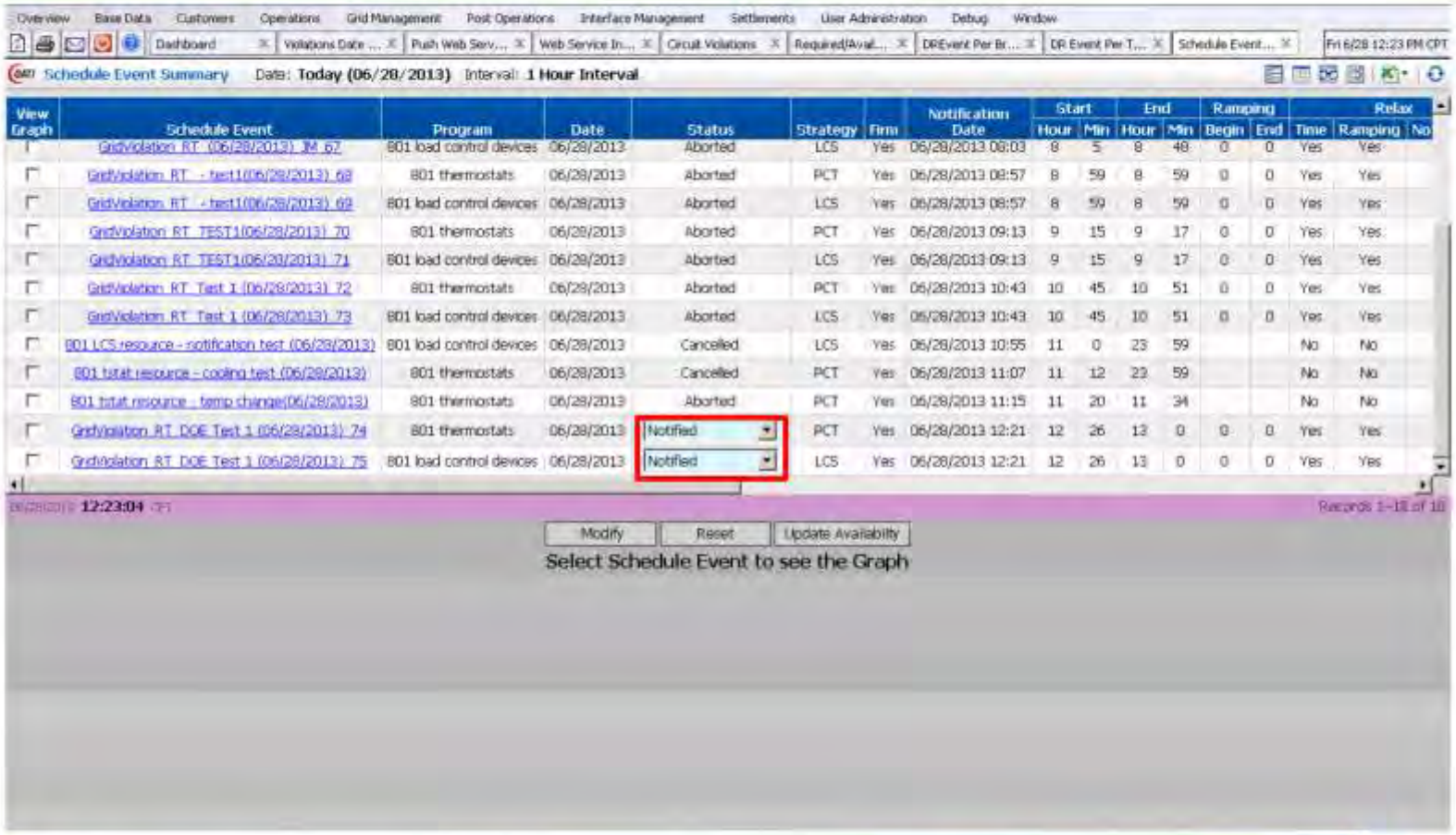
Select "Schedule DR Controls"



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221


Enter Schedule Information
Overview Base Data Customers Operations Grid Management Post Operations Interface Management Settlements User Administration Debug Window
Dashboard
Violations Date Time
Push Web Service ...
Web Service Inbo...
Circuit Violations
Required(Availabl...
DREvent Per Branch
DR Event Per Tran...
Fri 6/28 12:22 PM CDT
DR Event Per Transformer
Case Name: RT
Scheduled
Transformer
DR_A [kW]
DR_B [kW]
DR_C [kW]
Total KW
1079326 .00 .00 10.20 10.20
1079330 .00 .00 10.20 10.20
1327676 .00 .00 6.00 6.00
Total .00 .00 26.40 26.40
Enter Schedule Information
Schedule Name: GridViolation_RT_DOE Test 1 (06/28/2013)
Schedule Date: 06/28/2013
Start Time: 12 : 26
End Time: 13 : 00
Create
Cancel
14
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

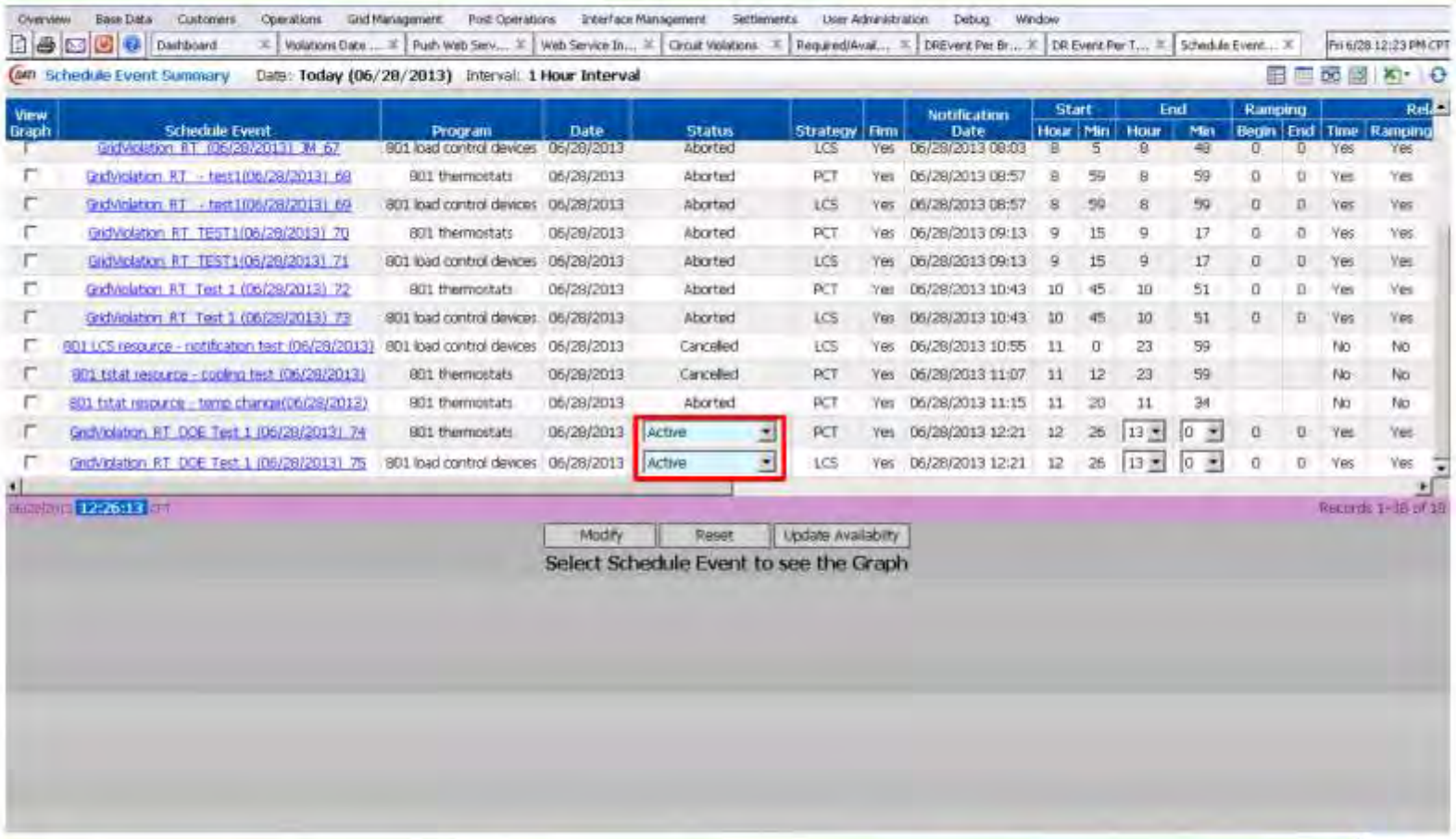
List of Committed DR Events



View Graph	Schedule Event	Program	Date	Status	Strategy	Firm	Notification Date	Start Hour	Start Min	End Hour	End Min	Ramping Begin	Ramping End	Relax Time	Relax Ramping	Relax No
	GridViolation_RT_(06/28/2013)_JM_67	801 load control devices	06/28/2013	Aborted	LCS	Yes	06/28/2013 08:03	8	5	8	40	0	0	Yes	Yes	
	GridViolation_RT_-test1(06/28/2013)_68	801 thermostats	06/28/2013	Aborted	PCT	Yes	06/28/2013 08:57	8	59	8	59	0	0	Yes	Yes	
	GridViolation_RT_-test1(06/28/2013)_69	801 load control devices	06/28/2013	Aborted	LCS	Yes	06/28/2013 08:57	8	59	8	59	0	0	Yes	Yes	
	GridViolation_RT_TEST1(06/28/2013)_70	801 thermostats	06/28/2013	Aborted	PCT	Yes	06/28/2013 09:13	9	15	9	17	0	0	Yes	Yes	
	GridViolation_RT_TEST1(06/28/2013)_71	801 load control devices	06/28/2013	Aborted	LCS	Yes	06/28/2013 09:13	9	15	9	17	0	0	Yes	Yes	
	GridViolation_RT_Test_1_(06/28/2013)_72	801 thermostats	06/28/2013	Aborted	PCT	Yes	06/28/2013 10:43	10	45	10	51	0	0	Yes	Yes	
	GridViolation_RT_Test_1_(06/28/2013)_73	801 load control devices	06/28/2013	Aborted	LCS	Yes	06/28/2013 10:43	10	45	10	51	0	0	Yes	Yes	
	801 LCS resource - notification test (06/28/2013)	801 load control devices	06/28/2013	Cancelled	LCS	Yes	06/28/2013 10:55	11	0	23	59			No	No	
	801 tstat resource - cooling test (06/28/2013)	801 thermostats	06/28/2013	Cancelled	PCT	Yes	06/28/2013 11:07	11	12	23	59			No	No	
	801 tstat resource - temp change(06/28/2013)	801 thermostats	06/28/2013	Aborted	PCT	Yes	06/28/2013 11:15	11	20	11	34			No	No	
	GridViolation_RT_DOE Test 1 (06/28/2013)_74	801 thermostats	06/28/2013	Notified	PCT	Yes	06/28/2013 12:21	12	26	13	0	0	0	Yes	Yes	
	GridViolation_RT_DOE Test 1 (06/28/2013)_75	801 load control devices	06/28/2013	Notified	LCS	Yes	06/28/2013 12:21	12	26	13	0	0	0	Yes	Yes	

▪15 This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Status Changes to Active After Event Starts

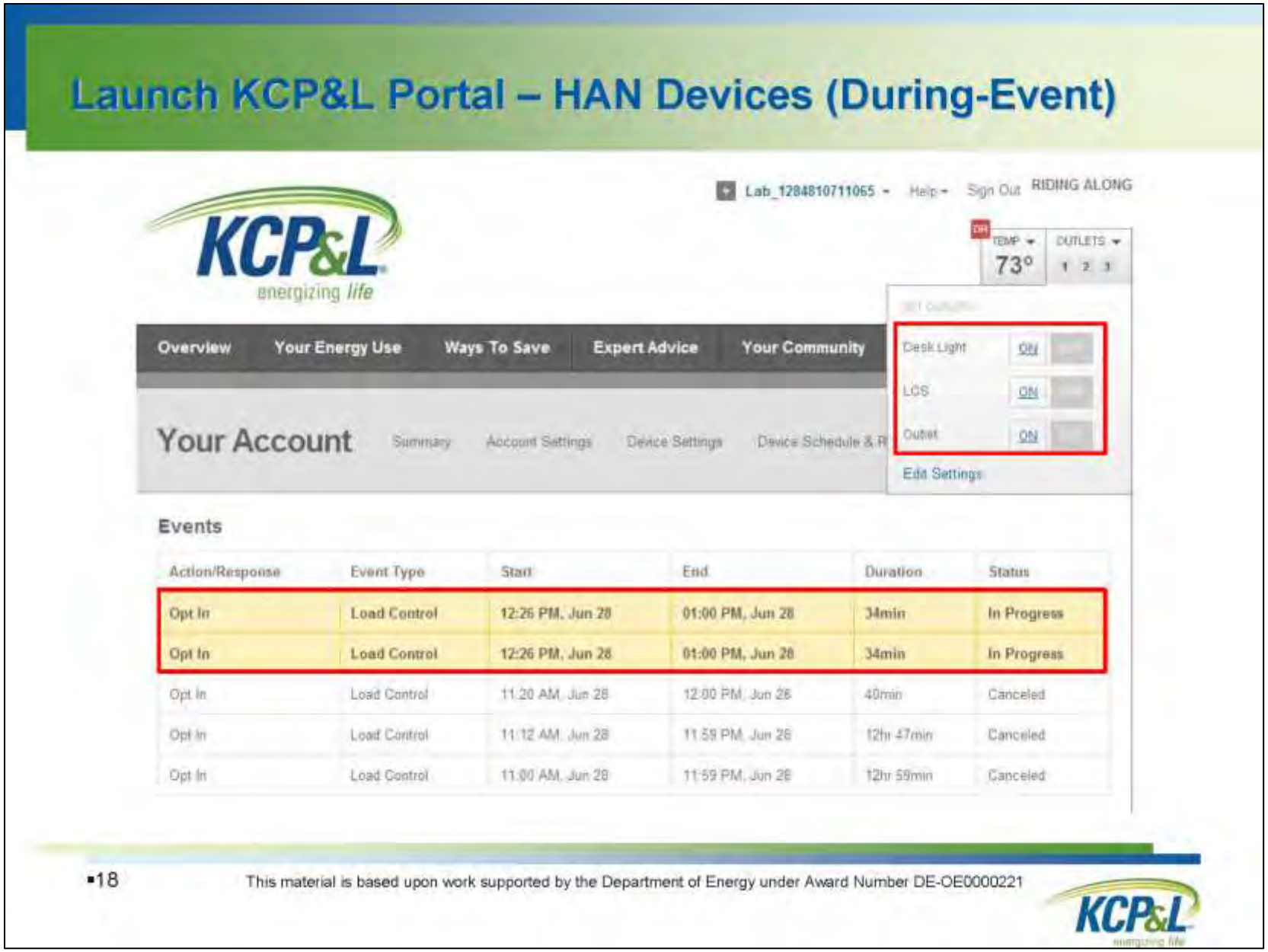


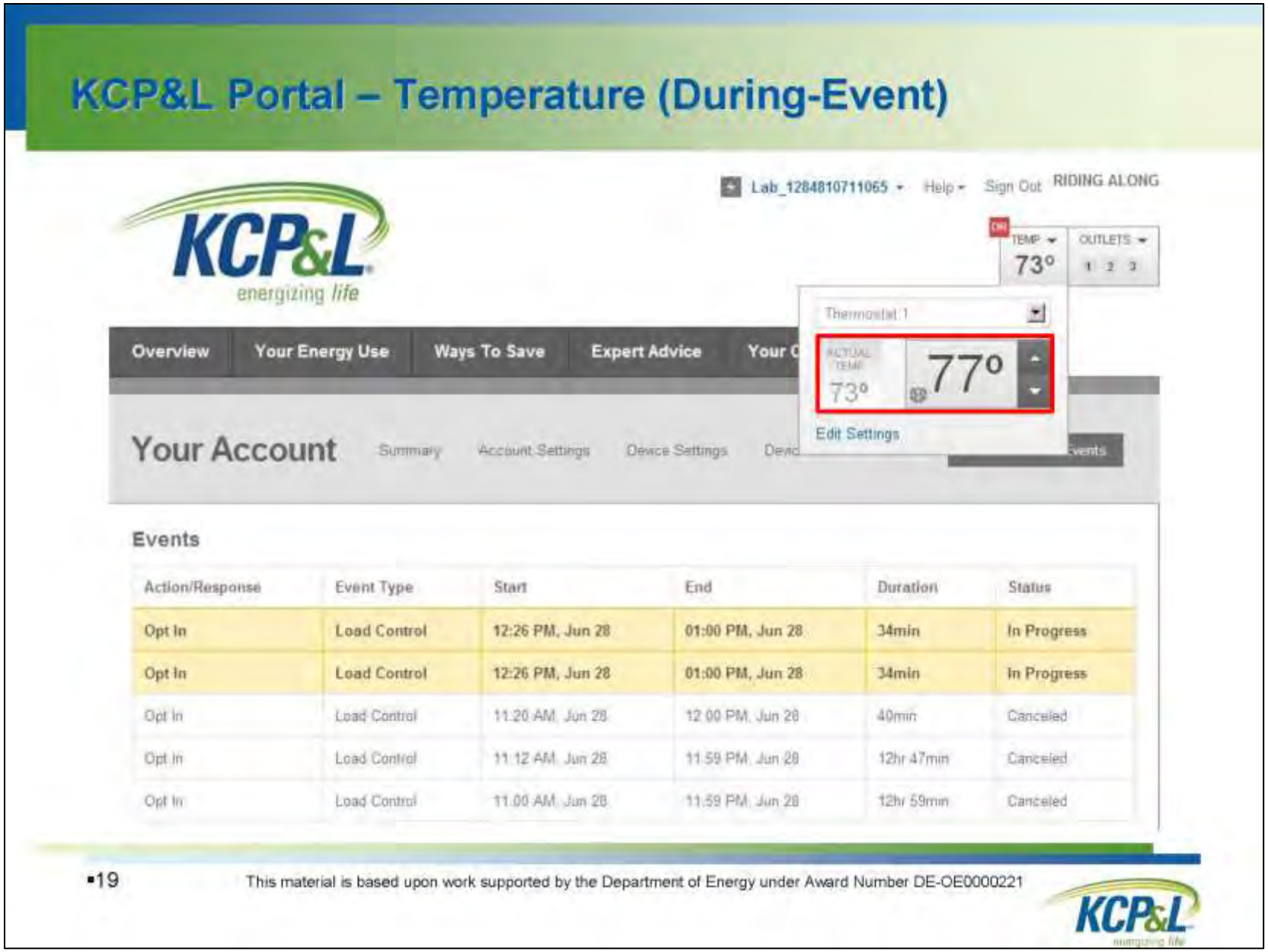
View Graph	Schedule Event	Program	Date	Status	Strategy	Firm	Notification Date	Start Hour	Start Min	End Hour	End Min	Ramping Begin	Ramping End	Time	Ramping
	GridViolation_RT_(06/28/2013)_3M_67	801 load control devices	06/28/2013	Aborted	LCS	Yes	06/28/2013 08:03	8	5	9	49	0	0	Yes	Yes
	GridViolation_RT_-_test1(06/28/2013)_68	801 thermostats	06/28/2013	Aborted	PCT	Yes	06/28/2013 08:57	8	59	8	59	0	0	Yes	Yes
	GridViolation_RT_-_test1(06/28/2013)_69	801 load control devices	06/28/2013	Aborted	LCS	Yes	06/28/2013 08:57	8	59	8	59	0	0	Yes	Yes
	GridViolation_RT_TEST1(06/28/2013)_70	801 thermostats	06/28/2013	Aborted	PCT	Yes	06/28/2013 09:13	9	15	9	17	0	0	Yes	Yes
	GridViolation_RT_TEST1(06/28/2013)_71	801 load control devices	06/28/2013	Aborted	LCS	Yes	06/28/2013 09:13	9	15	9	17	0	0	Yes	Yes
	GridViolation_RT_Test_1_(06/28/2013)_72	801 thermostats	06/28/2013	Aborted	PCT	Yes	06/28/2013 10:43	10	45	10	51	0	0	Yes	Yes
	GridViolation_RT_Test_1_(06/28/2013)_73	801 load control devices	06/28/2013	Aborted	LCS	Yes	06/28/2013 10:43	10	45	10	51	0	0	Yes	Yes
	801 LCS resource - notification test (06/28/2013)	801 load control devices	06/28/2013	Cancelled	LCS	Yes	06/28/2013 10:55	11	0	23	59			No	No
	801 tstat resource - cooling test (06/28/2013)	801 thermostats	06/28/2013	Cancelled	PCT	Yes	06/28/2013 11:07	11	12	23	59			No	No
	801 tstat resource - temp change(06/28/2013)	801 thermostats	06/28/2013	Aborted	PCT	Yes	06/28/2013 11:15	11	20	11	34			No	No
	GridViolation_RT_DOE_Test_1_(06/28/2013)_74	801 thermostats	06/28/2013	Active	PCT	Yes	06/28/2013 12:21	12	26	13	0	0	0	Yes	Yes
	GridViolation_RT_DOE_Test_1_(06/28/2013)_75	801 load control devices	06/28/2013	Active	LCS	Yes	06/28/2013 12:21	12	26	13	0	0	0	Yes	Yes

▪16 This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

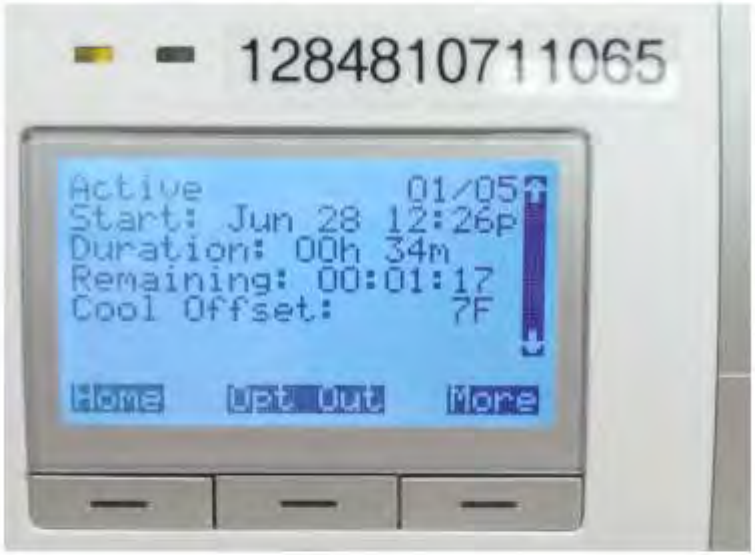
Thermostat Before the DR Event (Pre-Event)

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

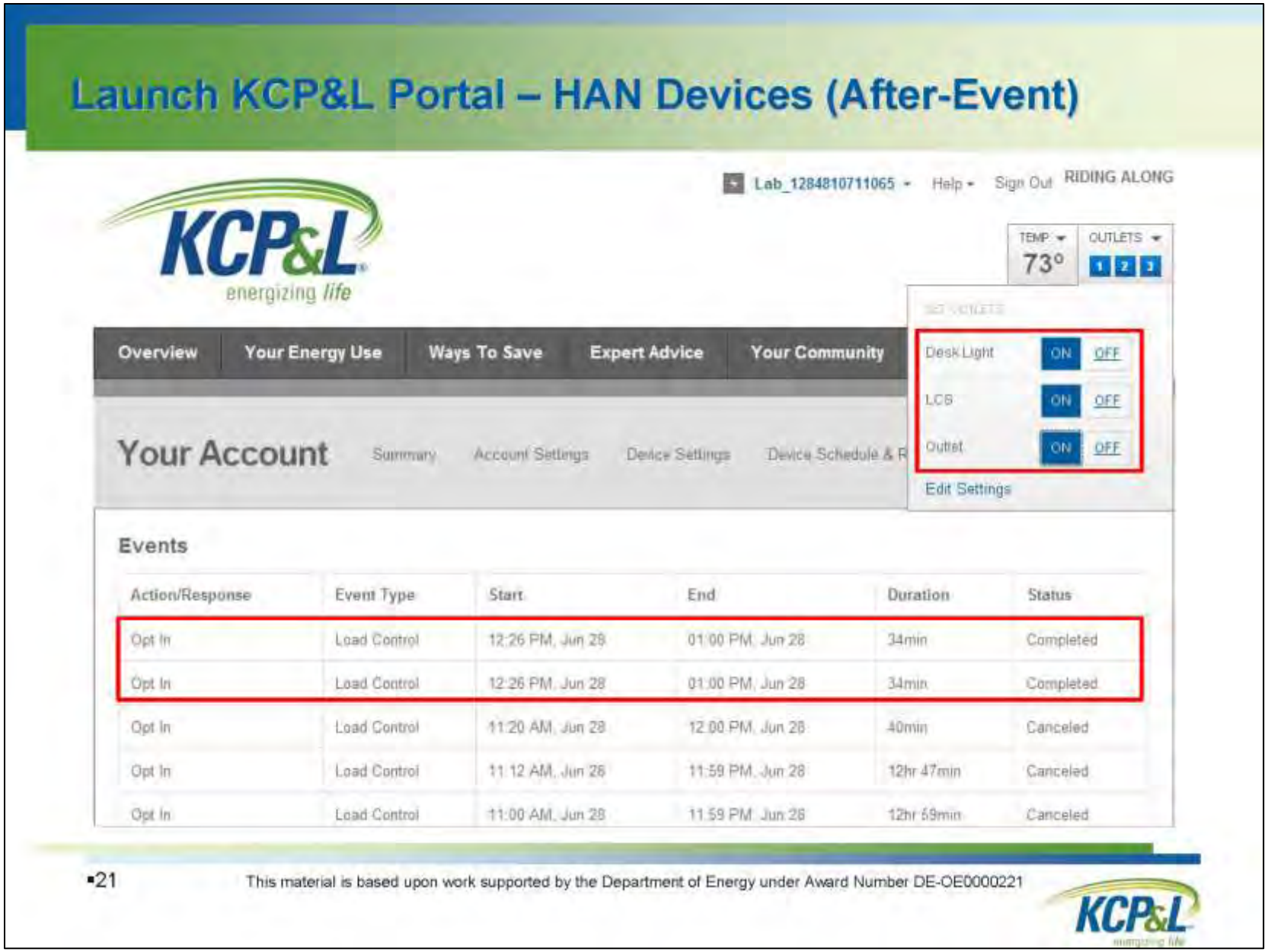

Launch KCP&L Portal – HAN Devices (During-Event)
KCP&L
energizing life
Lab_1284810711065
Help
Sign Out
RIDING ALONG
TEMP
73°
OUTLETS
1 2 3
Overview
Your Energy Use
Ways To Save
Expert Advice
Your Community
Desk Light
ON
LCS
ON
Outlet
ON
Edit Settings
Your Account
Summary
Account Settings
Device Settings
Events
Action/Response
Event Type
Start
End
Duration
Status
Opt In
Load Control
12:26 PM, Jun 28
01:00 PM, Jun 28
34min
In Progress
Opt In
Load Control
12:26 PM, Jun 28
01:00 PM, Jun 28
34min
In Progress
Opt In
Load Control
11:20 AM, Jun 28
12:00 PM, Jun 28
40min
Canceled
Opt In
Load Control
11:12 AM, Jun 28
11:59 PM, Jun 28
12hr 47min
Canceled
Opt In
Load Control
11:00 AM, Jun 28
11:59 PM, Jun 28
12hr 59min
Canceled
18
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

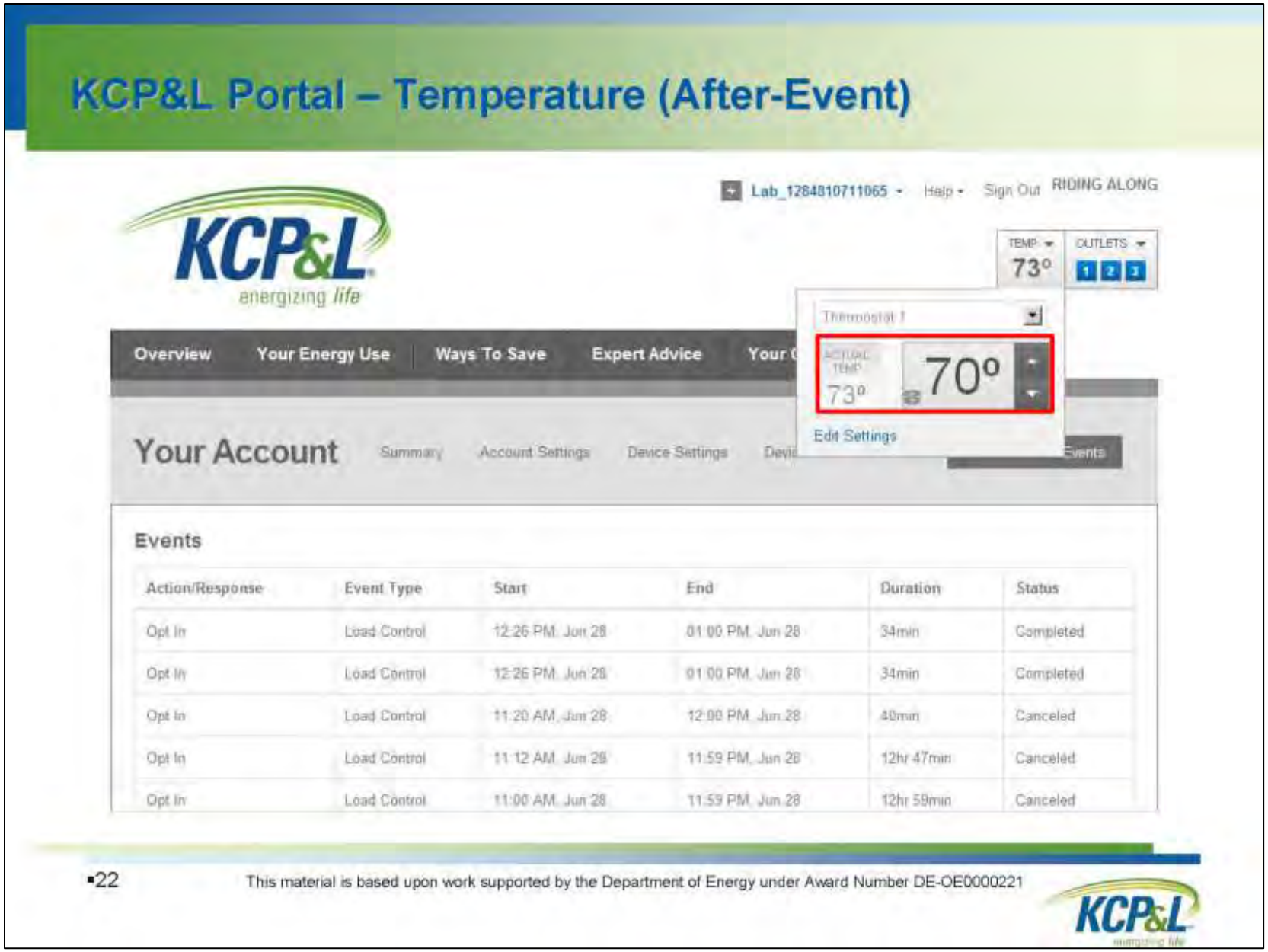

KCP&L Portal – Temperature (During-Event)
Lab_1284810711065
Help
Sign Out
RIDING ALONG
KCP&L
energizing life
TEMP
73°
OUTLETS
1 2 3
Thermostat 1
ACTUAL TEMP
73°
77°
Edit Settings
Overview
Your Energy Use
Ways To Save
Expert Advice
Your Account
Summary
Account Settings
Device Settings
Events
Action/Response
Event Type
Start
End
Duration
Status
Opt In
Load Control
12:26 PM, Jun 28
01:00 PM, Jun 28
34min
In Progress
Opt In
Load Control
12:26 PM, Jun 28
01:00 PM, Jun 28
34min
In Progress
Opt In
Load Control
11:20 AM, Jun 28
12:00 PM, Jun 28
40min
Canceled
Opt In
Load Control
11:12 AM, Jun 28
11:59 PM, Jun 28
12hr 47min
Canceled
Opt In
Load Control
11:00 AM, Jun 28
11:59 PM, Jun 28
12hr 59min
Canceled
19
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

Thermostat During the DR Event (During-Event)



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221


Launch KCP&L Portal – HAN Devices (After-Event)
Lab_1284810711065
Help
Sign Out
RIDING ALONG
KCP&L
energizing life
TEMP
73°
OUTLETS
1 2 3
Overview
Your Energy Use
Ways To Save
Expert Advice
Your Community
Desk Light ON OFF
LCS ON OFF
Outlet ON OFF
Edit Settings
Your Account
Summary
Account Settings
Device Settings
Events
Action/Response
Event Type
Start
End
Duration
Status
Opt In Load Control 12:26 PM, Jun 28 01:00 PM, Jun 28 34min Completed
Opt In Load Control 12:26 PM, Jun 28 01:00 PM, Jun 28 34min Completed
Opt In Load Control 11:20 AM, Jun 28 12:00 PM, Jun 28 40min Canceled
Opt In Load Control 11:12 AM, Jun 28 11:59 PM, Jun 28 12hr 47min Canceled
Opt In Load Control 11:00 AM, Jun 28 11:59 PM, Jun 28 12hr 59min Canceled
21
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

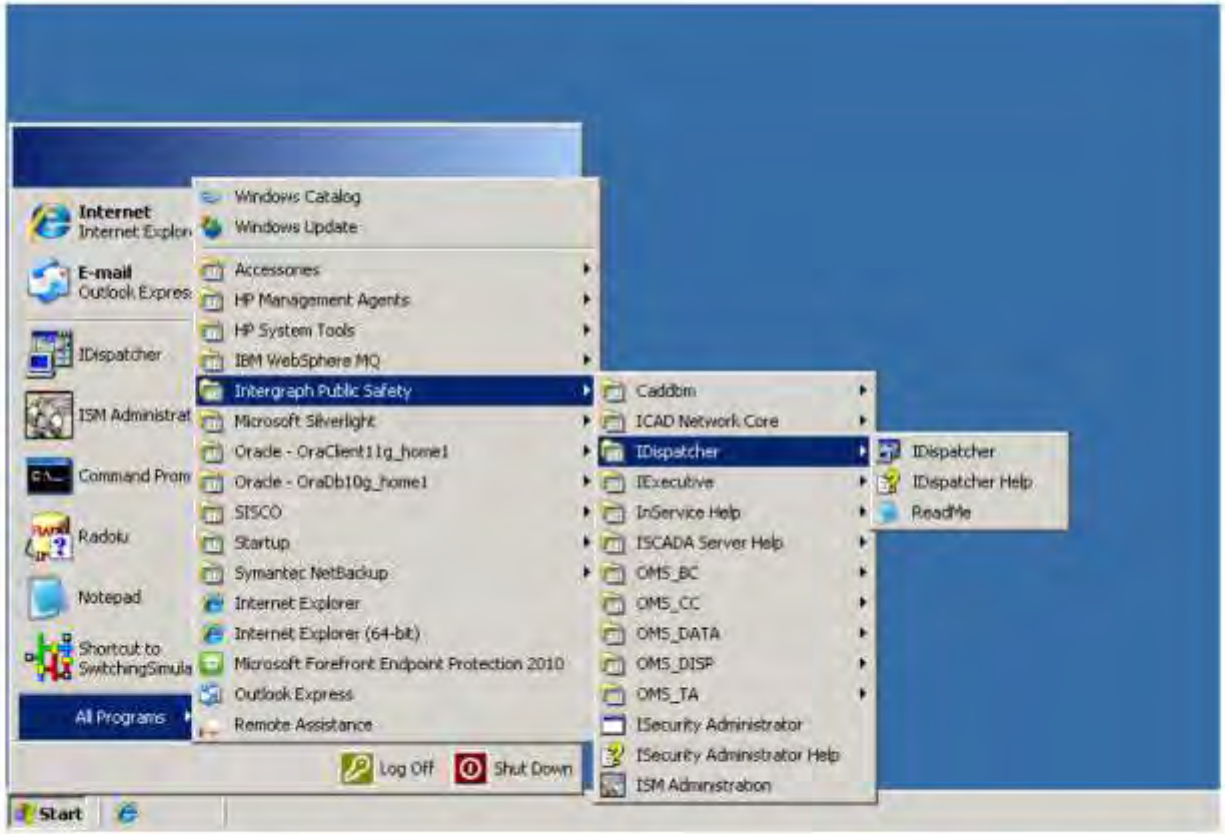

KCP&L Portal – Temperature (After-Event)
KCP&L
energizing life
Lab_1284810711065
Help
Sign Out
RIDING ALONG
TEMP
73°
OUTLETS
1 2 3
Thermostat 1
ACTUAL TEMP
73°
70°
Edit Settings
Overview
Your Energy Use
Ways To Save
Expert Advice
Your Account
Summary
Account Settings
Device Settings
Events
Events
Action/Response
Event Type
Start
End
Duration
Status
Opt In
Load Control
12:26 PM, Jun 28
01:00 PM, Jun 28
34min
Completed
Opt In
Load Control
12:26 PM, Jun 28
01:00 PM, Jun 28
34min
Completed
Opt In
Load Control
11:20 AM, Jun 28
12:00 PM, Jun 28
40min
Canceled
Opt In
Load Control
11:12 AM, Jun 28
11:59 PM, Jun 28
12hr 47min
Canceled
Opt In
Load Control
11:00 AM, Jun 28
11:59 PM, Jun 28
12hr 59min
Canceled
22
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

Thermostat After the DR Event (After-Event)

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221


Demand Response – Battery
- KC Green Impact Zone Initiative
- DOE Regional SmartGrid Demonstration Program
- EPRI SmartGrid Demonstration Program
KCP&L
SmartGrid
the future of energy

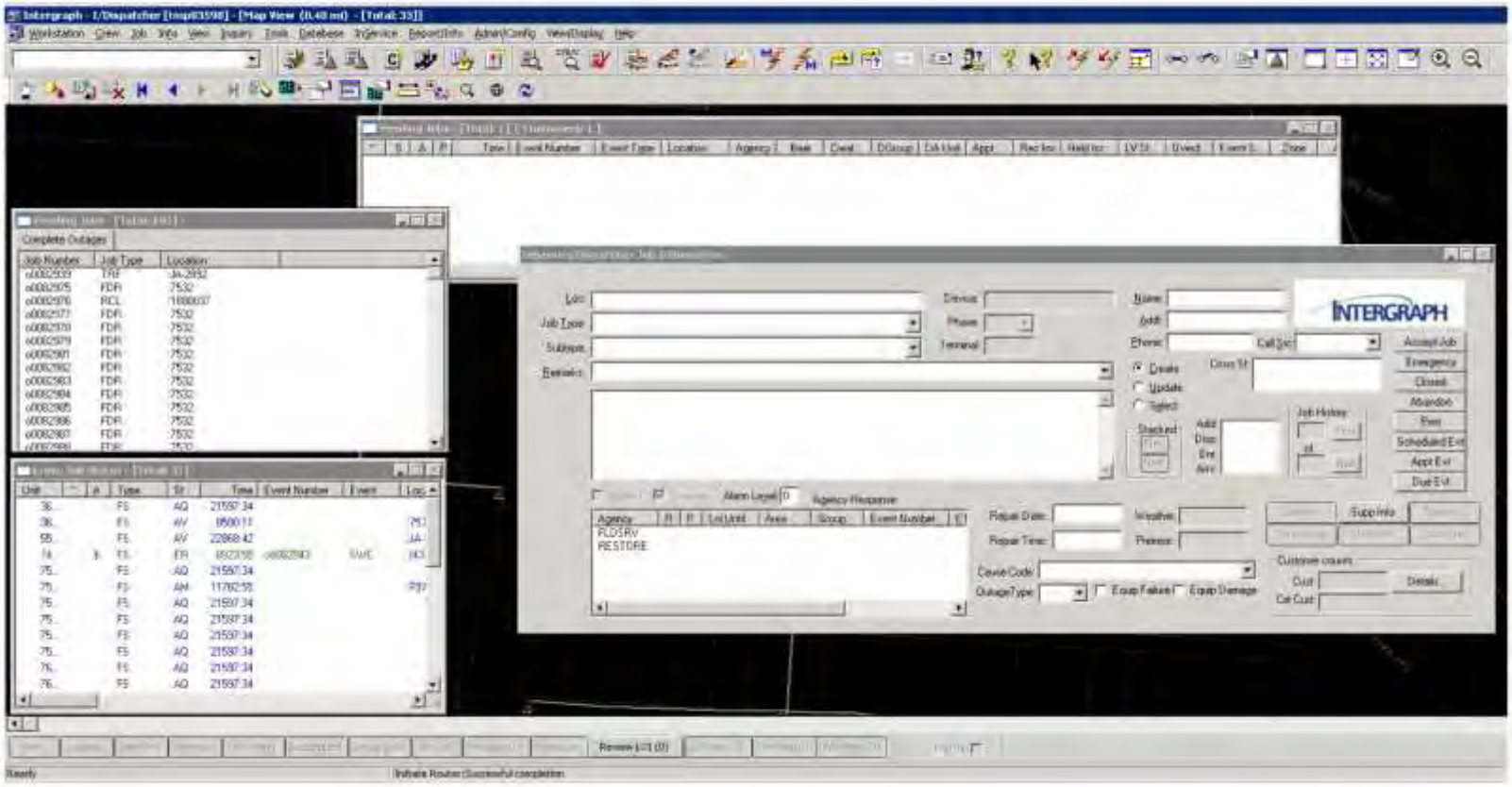
Launch InService I/Dispatcher



▪2

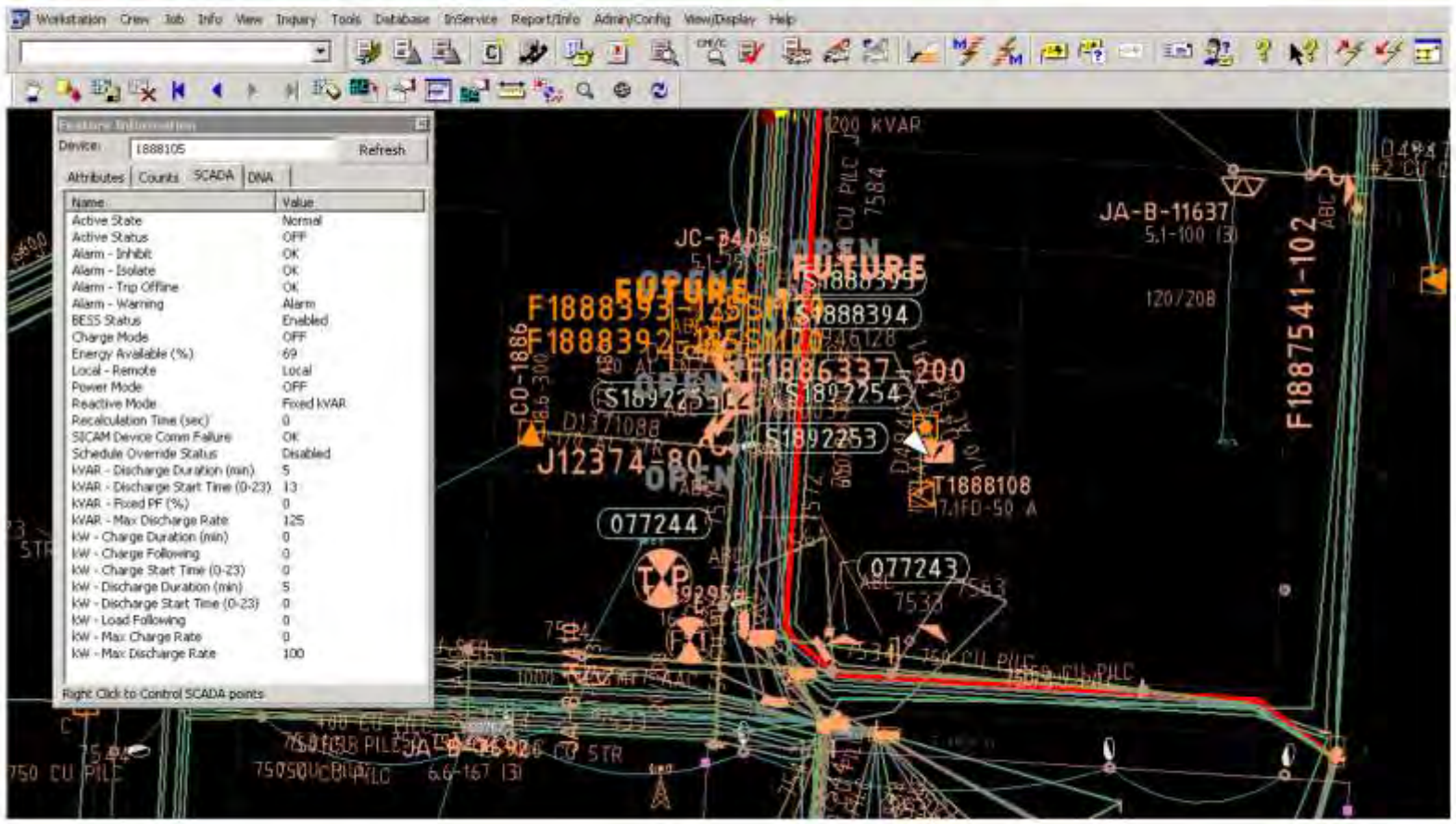
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

InService I/Dispatcher Main Screen

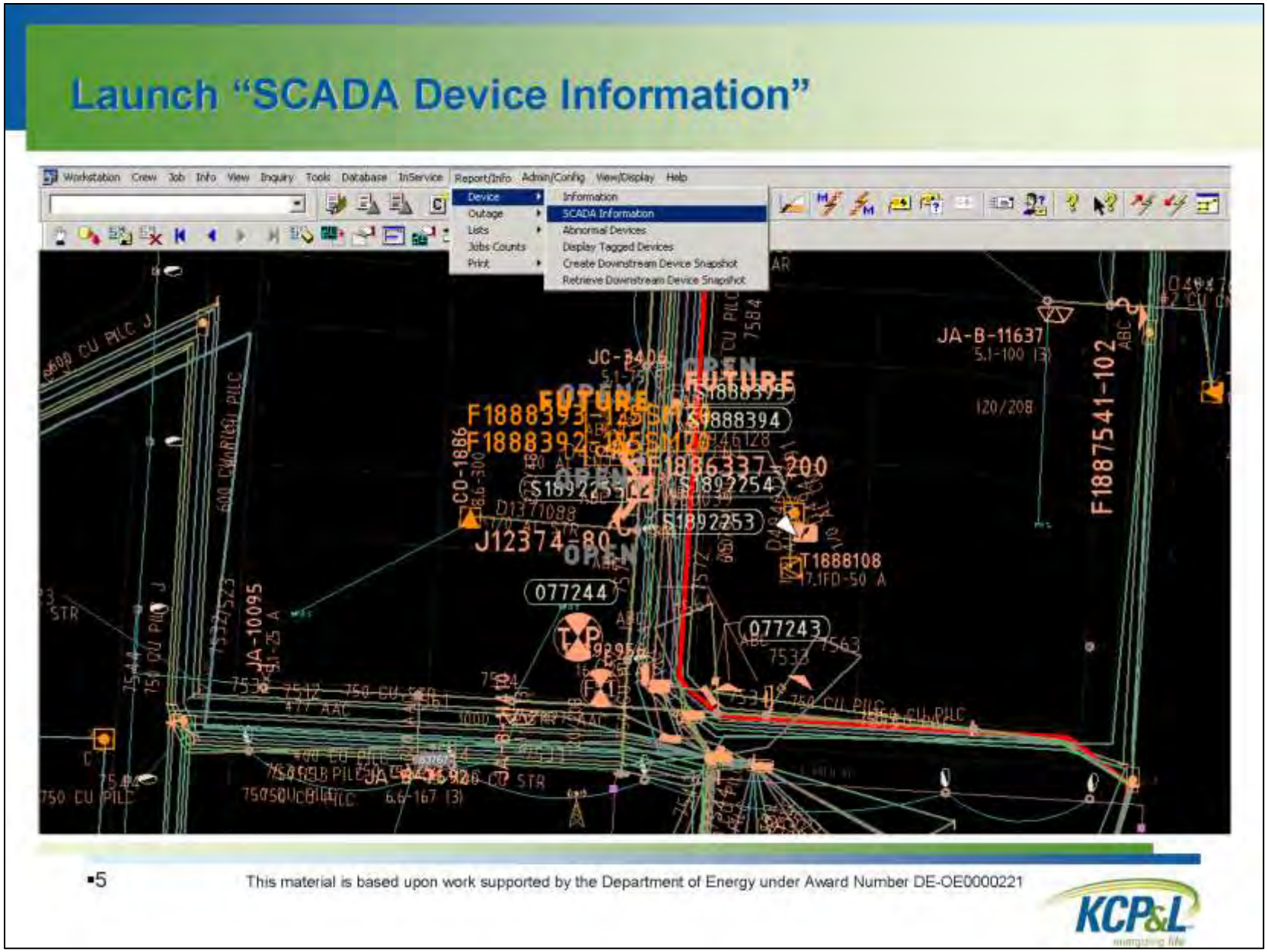


This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

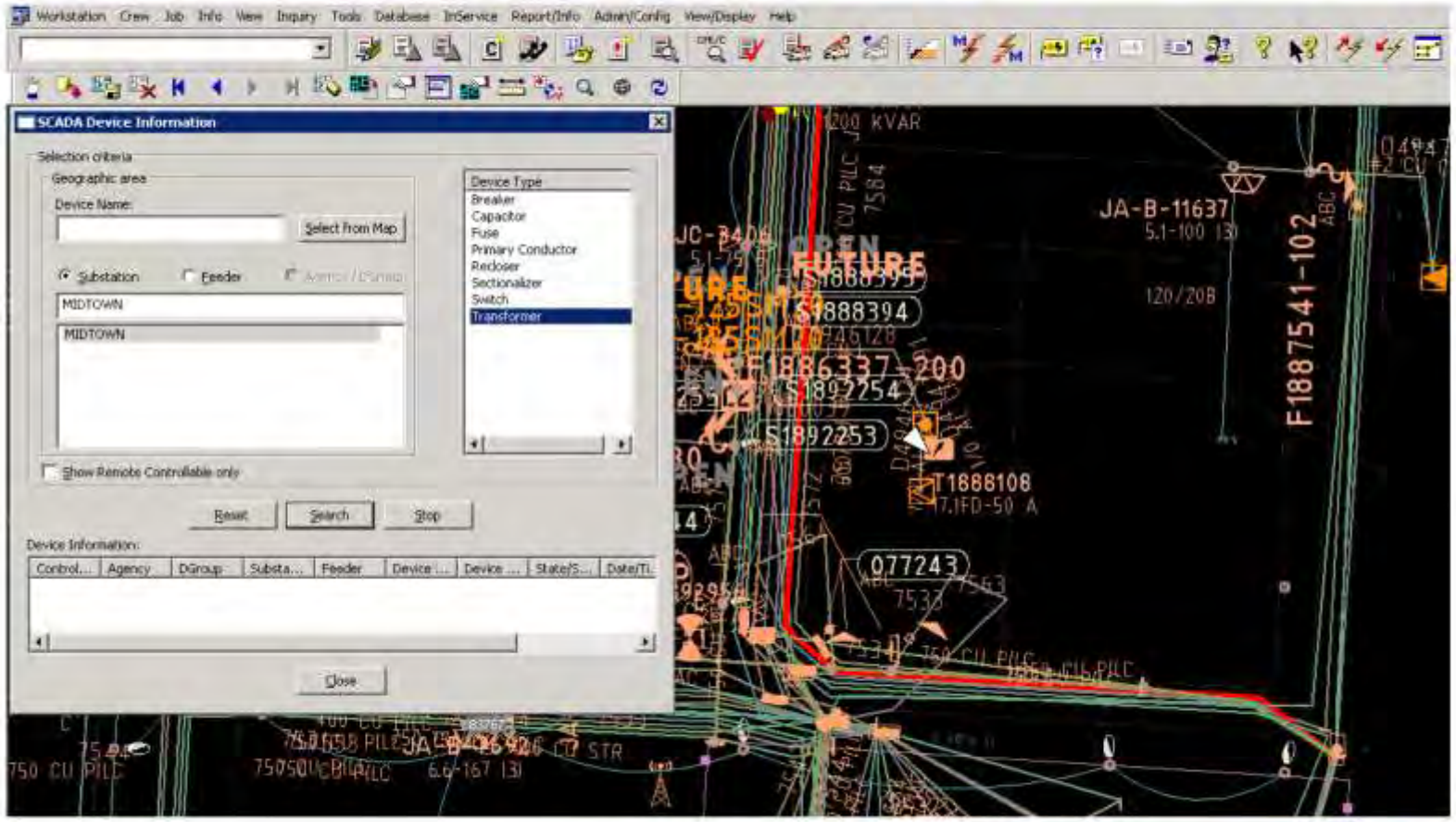
Feature Information: Battery



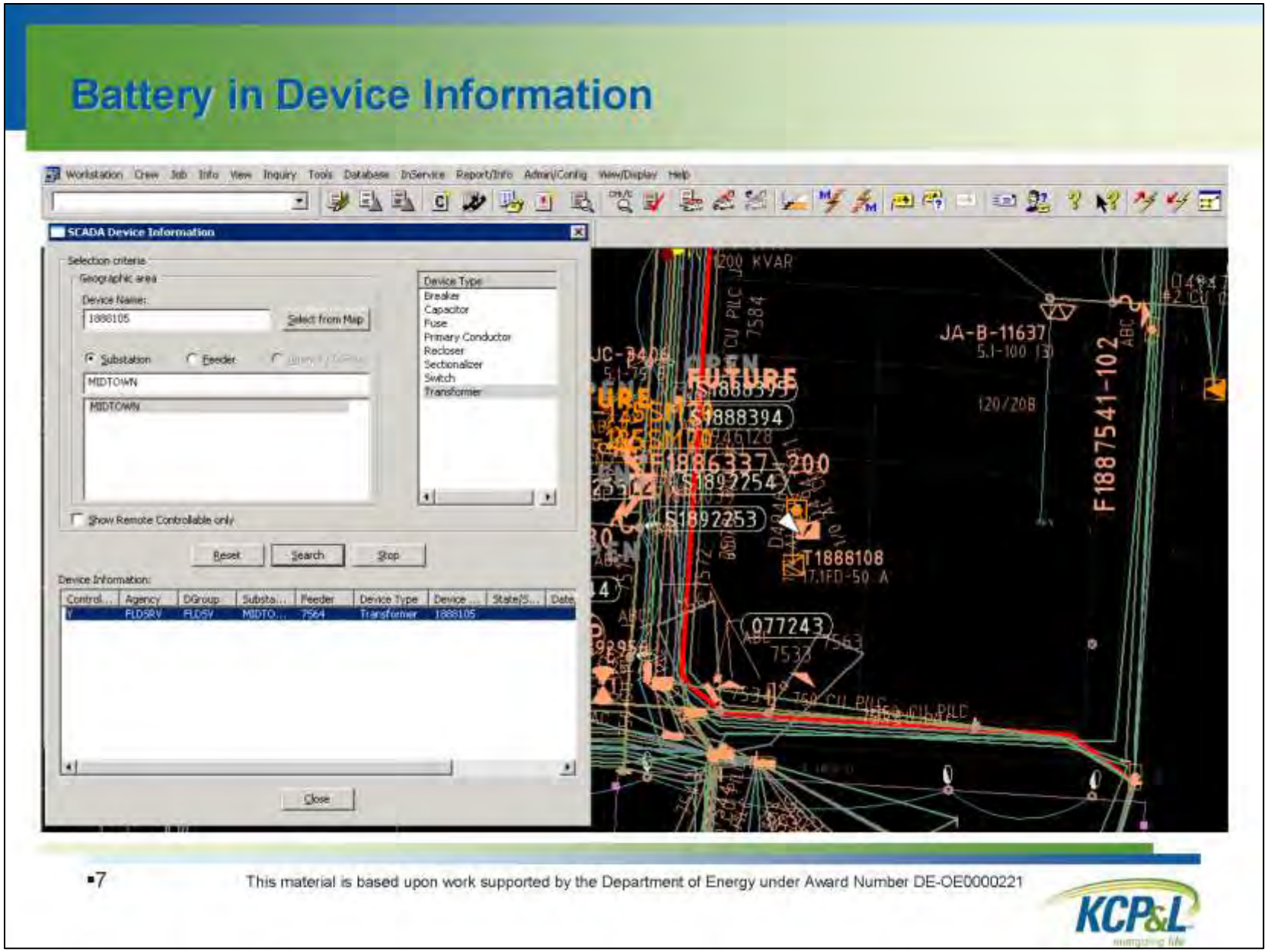
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

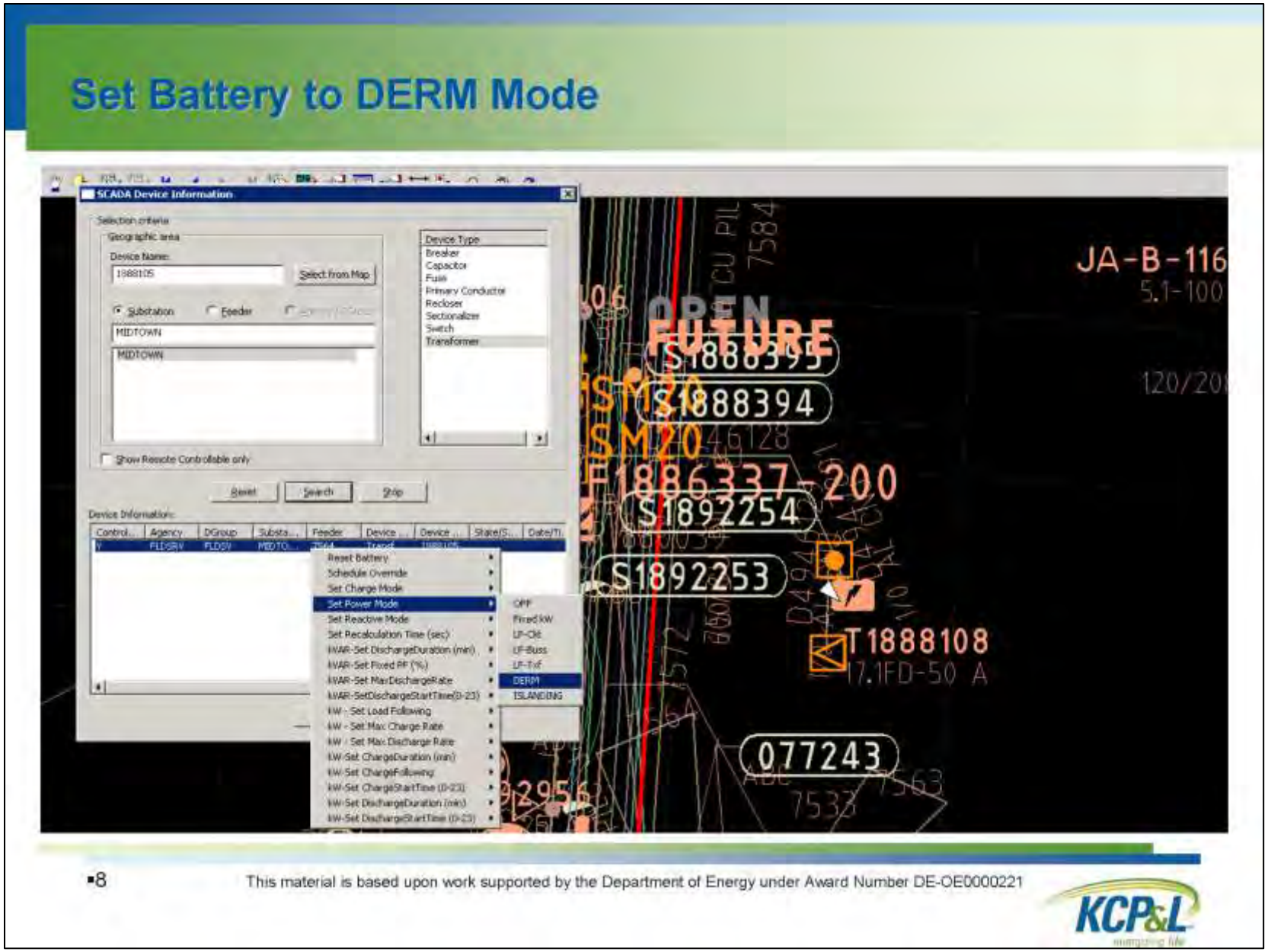

Launch "SCADA Device Information"
Workstation Crew Job Info View Inquiry Tools Database InService Report/Info Admin/Config View/Display Help
Device
Outage
Lists
Jobs Counts
Print
Information
SCADA Information
Abnormal Devices
Display Tagged Devices
Create Downstream Device Snapshot
Retrieve Downstream Device Snapshot
JA-B-11637
F1887541-102
FUTURE
OPEN
J12374-80
T1888108
077244
077243
JA-10095
▪5
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

SCADA Device Information Window

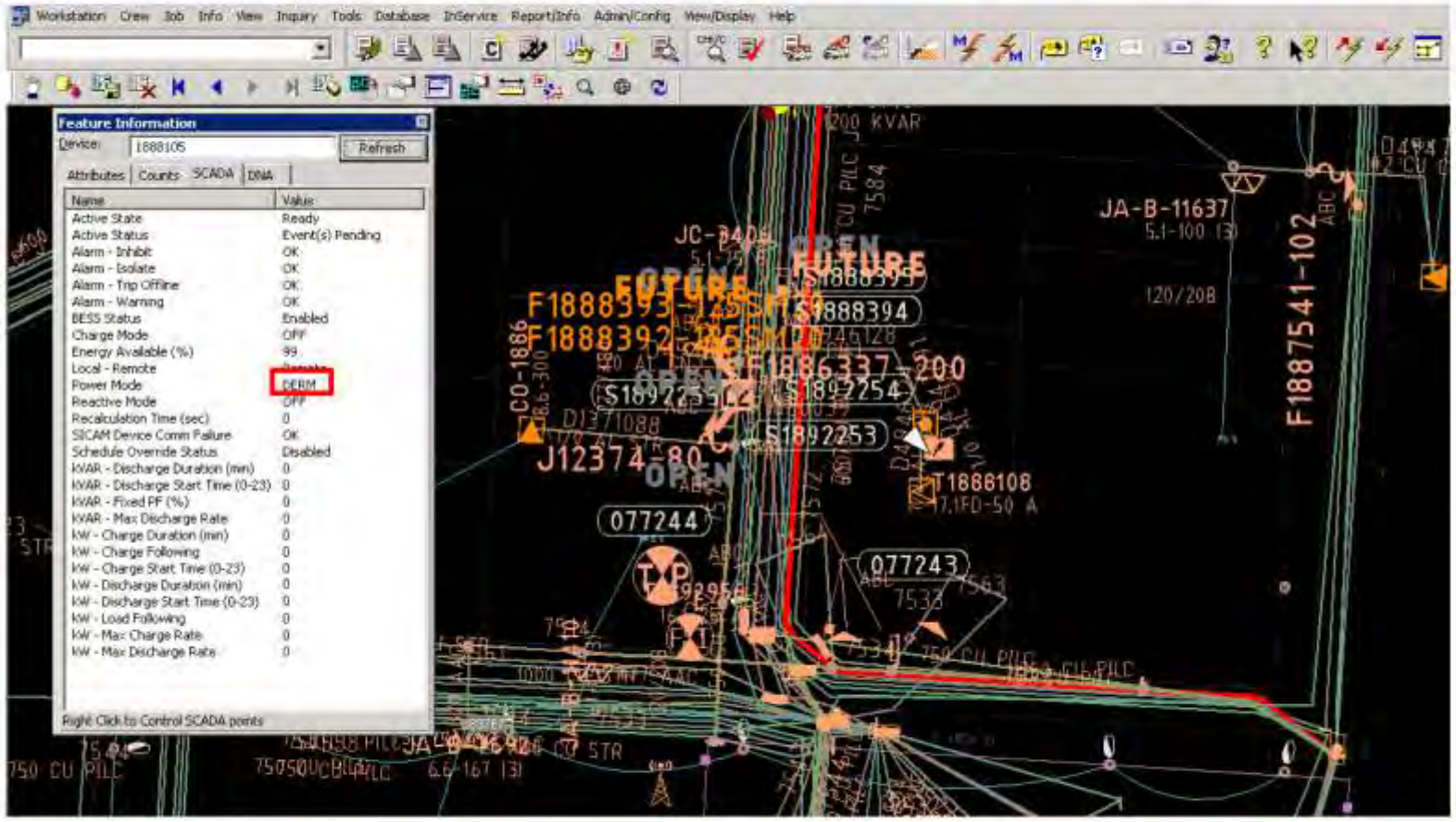


This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221


Battery in Device Information
SCADA Device Information
Selection criteria
Geographic area
Device Name:
1888105
Select from Map
Substation
Feeder
MIDTOWN
MIDTOWN
Device Type
Breaker
Capacitor
Fuse
Primary Conductor
Recloser
Sectionalizer
Switch
Transformer
Show Remote Controllable only
Reset
Search
Stop
Device Information:
Control...
Agency
DGroup
Substa...
Feeder
Device Type
Device ...
State/S...
Date
FLDSRV
FLDSV
MIDTO...
7564
Transformer
1888105
Close
JA-B-11637
F1887541-102
FUTURE
T1888108
077243
7564
7563
7534
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

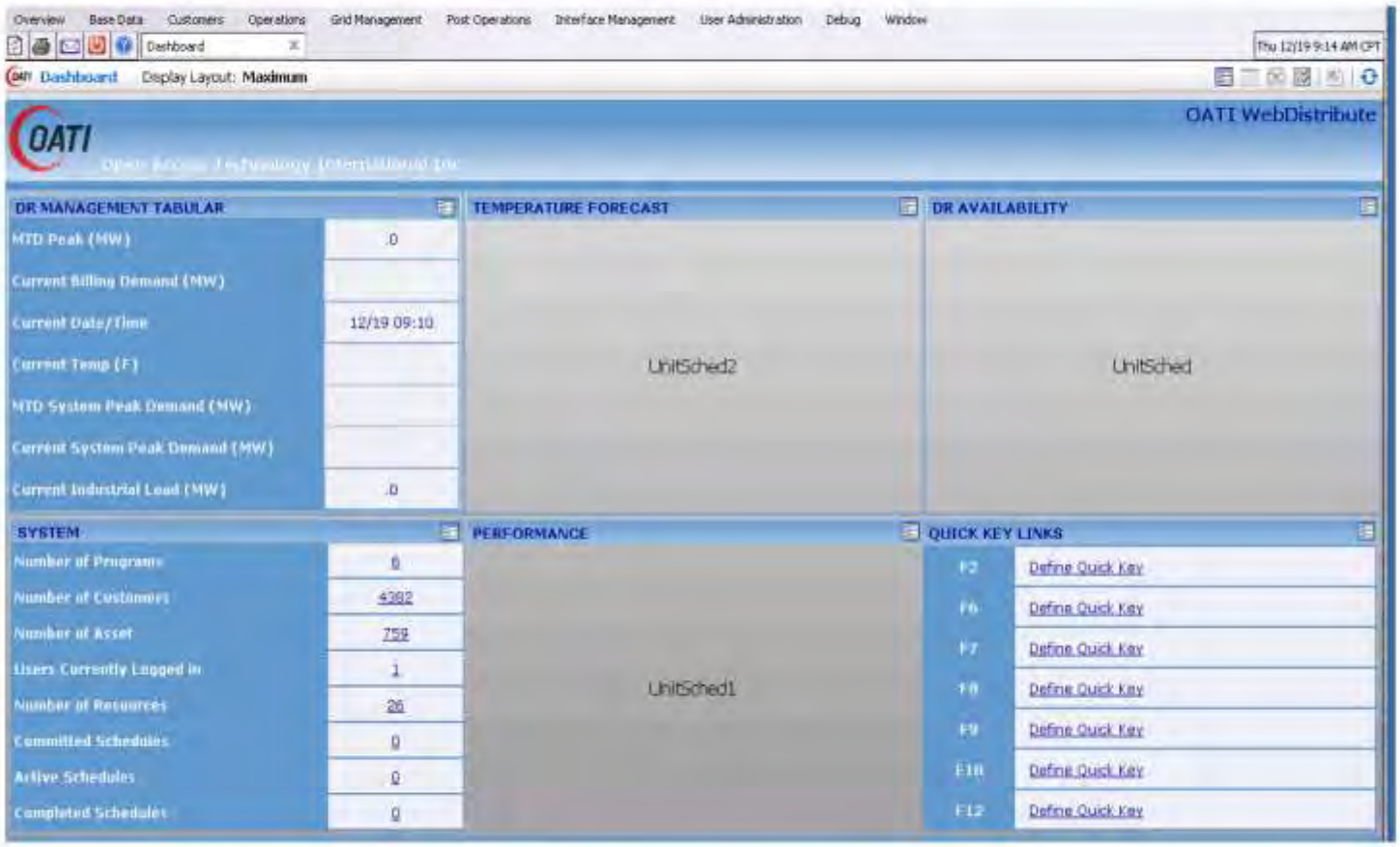

Set Battery to DERM Mode
SCADA Device Information
Selection criteria
Geographic area
Device Name:
1888105
Select from Map
Substation
Feeder
MIDTOWN
MIDTOWN
Show Remote Controllable only
Reset
Search
Stop
Device Information:
Control...
Agency
DGroup
Substa...
Feeder
Device ...
Device ...
State/S...
Date/Ti...
Device Type
Breaker
Capacitor
Fuse
Primary Conductor
Recloser
Sectionalizer
Switch
Transformer
Reset Battery
Schedule Override
Set Charge Mode
Set Power Mode
Set Reactive Mode
Set Recalculation Time (sec)
kWAR-Set DischargeDuration (min)
kWAR-Set Fixed PF (%)
kWAR-Set MaxDischargeRate
kWAR-SetDischargeStartTime(0-23)
kW - Set Load Following
kW - Set Max Charge Rate
kW - Set Max Discharge Rate
kW-Set ChargeDuration (min)
kW-Set ChargeFollowing
kW-Set ChargeStartTime (0-23)
kW-Set DischargeDuration (min)
kW-Set DischargeStartTime (0-23)
OFF
Fixed kW
LP-Old
LP-Buss
LP-Tot
DERM
ISLANDING
JA-B-116
5.1-100
FUTURE
S1888395
S1888394
F1886337-200
S1892254
S1892253
T1888108
077243
8
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

Battery set to DERM Power Mode



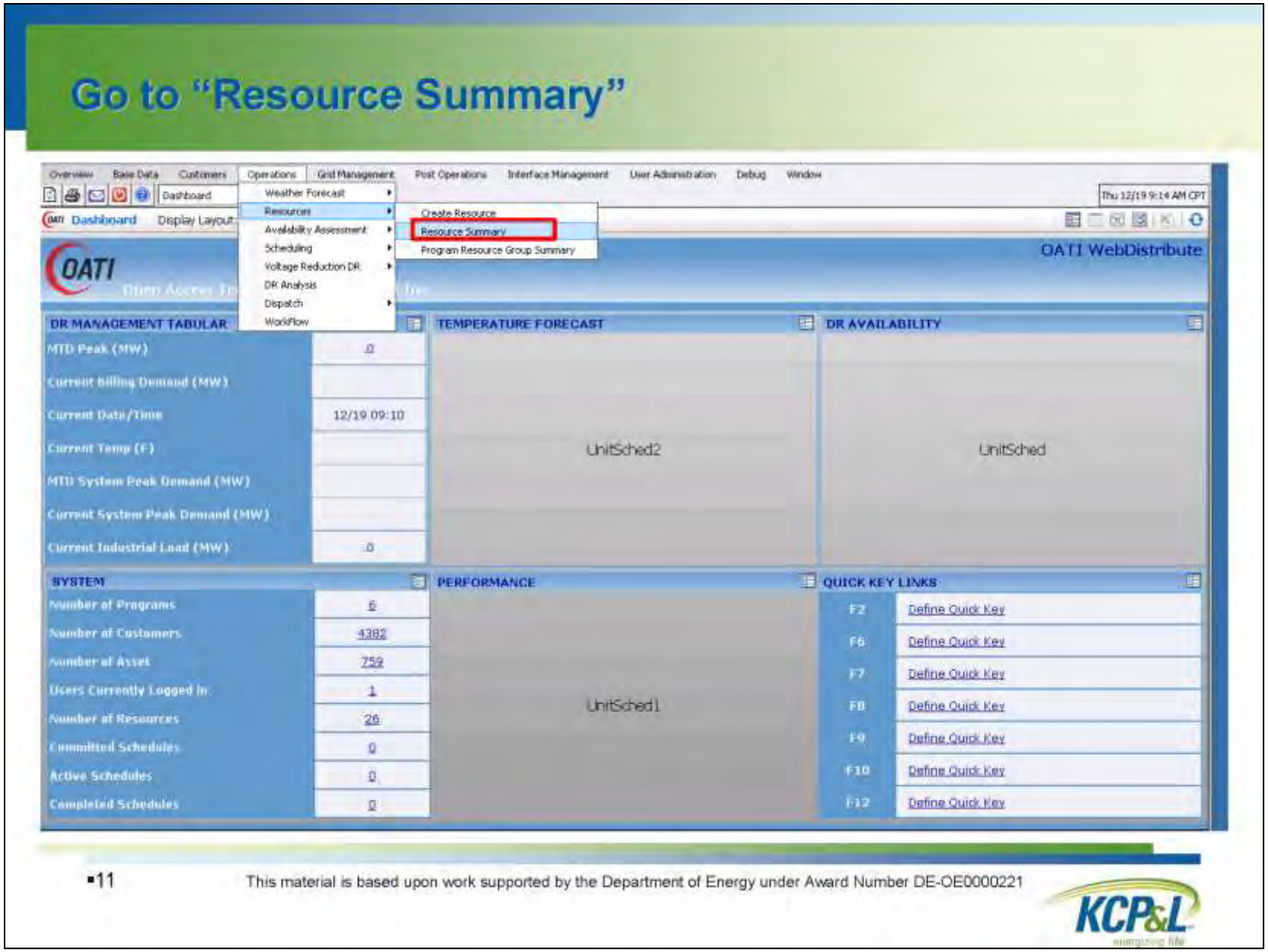
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Launch DERM WebUI

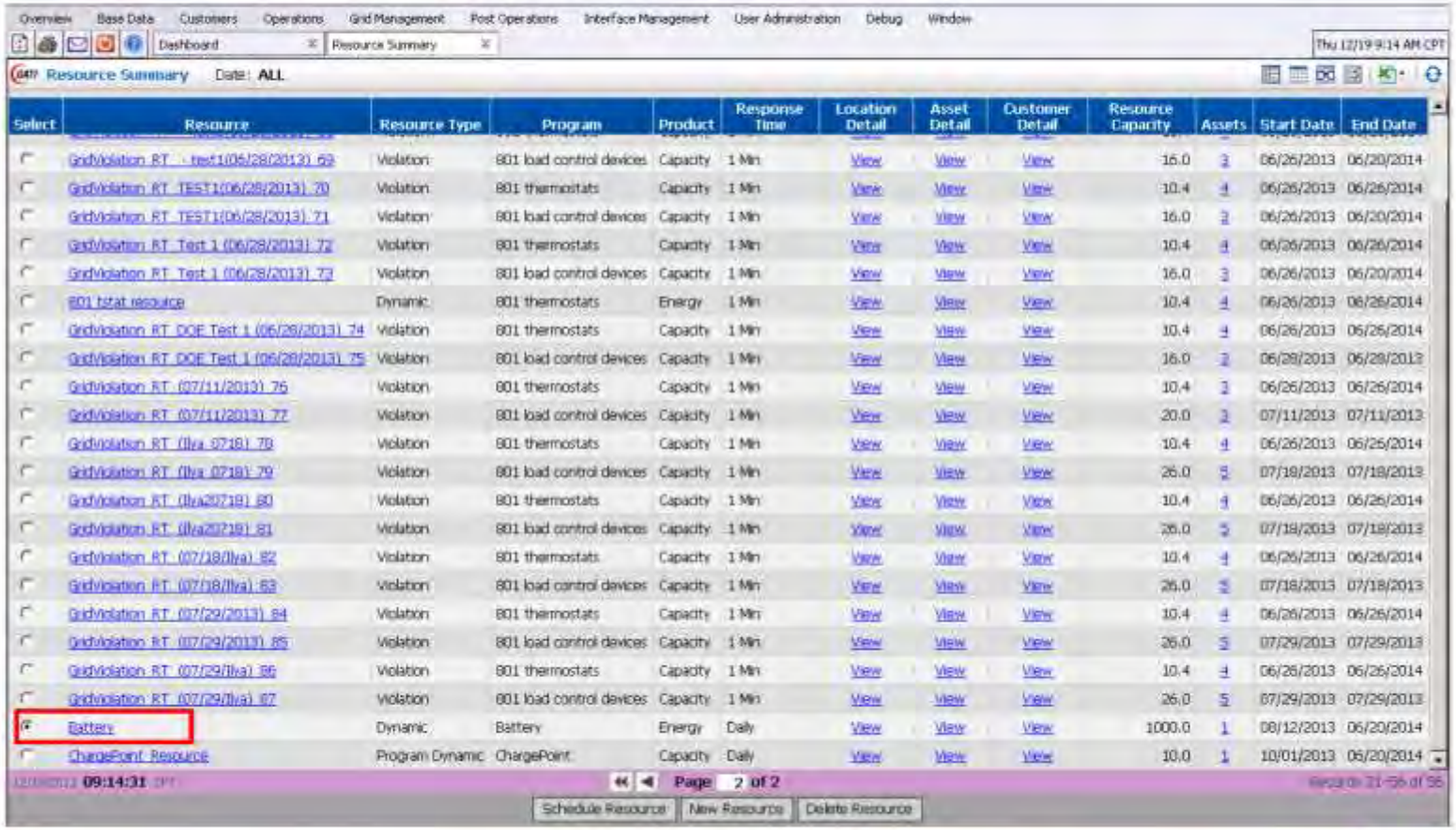


▪10

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

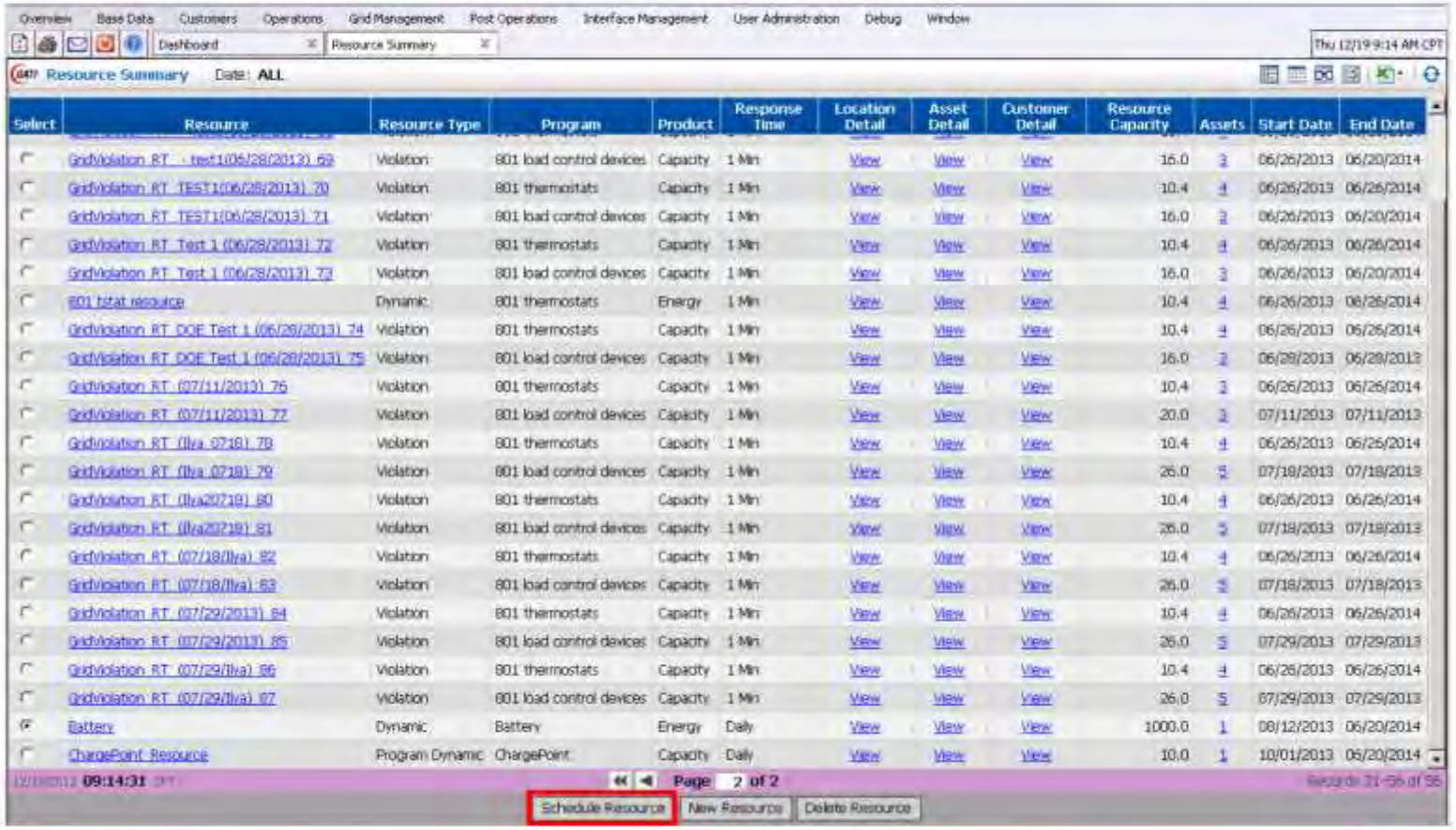

Go to "Resource Summary"
Overview
Base Data
Customers
Operations
Grid Management
Post Operations
Interface Management
User Administration
Debug
Window
Dashboard
Weather Forecast
Resources
Availability Assessment
Scheduling
Voltage Reduction DR
DR Analysis
Dispatch
Workflow
Create Resource
Resource Summary
Program Resource Group Summary
Thu 12/19 9:14 AM CPT
Dashboard
Display Layout
OATI
OATI WebDistribute
DR MANAGEMENT TABULAR
MTD Peak (MW) 0
Current Billing Demand (MW)
Current Date/Time 12/19 09:10
Current Temp (F)
MTD System Peak Demand (MW)
Current System Peak Demand (MW)
Current Industrial Load (MW) 0
TEMPERATURE FORECAST
UnitSched2
DR AVAILABILITY
UnitSched
SYSTEM
Number of Programs 6
Number of Customers 4382
Number of Asset 759
Users Currently Logged In 1
Number of Resources 26
Committed Schedules 0
Active Schedules 0
Completed Schedules 0
PERFORMANCE
UnitSched1
QUICK KEY LINKS
F2 Define Quick Key
F6 Define Quick Key
F7 Define Quick Key
F8 Define Quick Key
F9 Define Quick Key
F10 Define Quick Key
F12 Define Quick Key
11
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

List of Available Resources

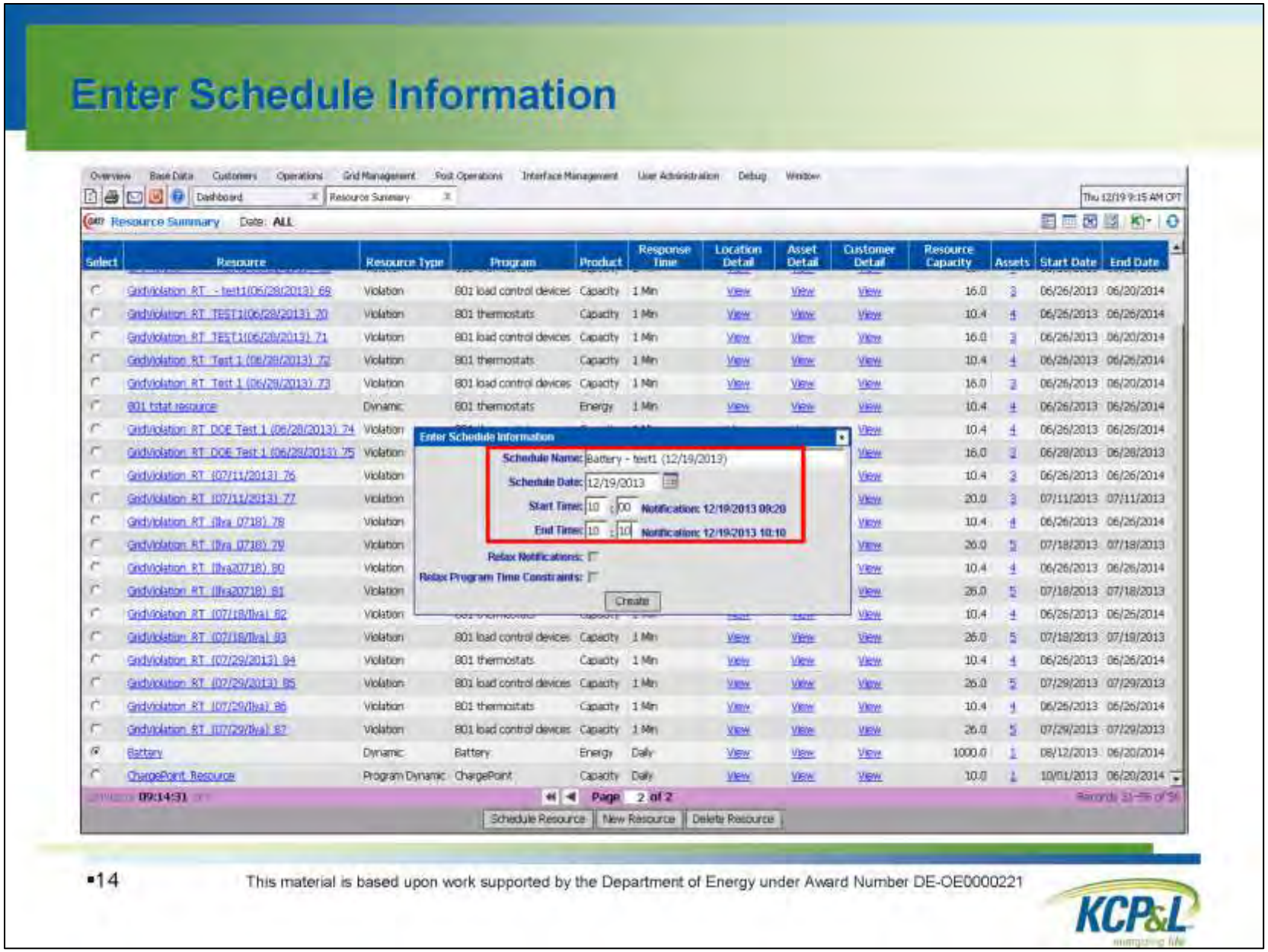


This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

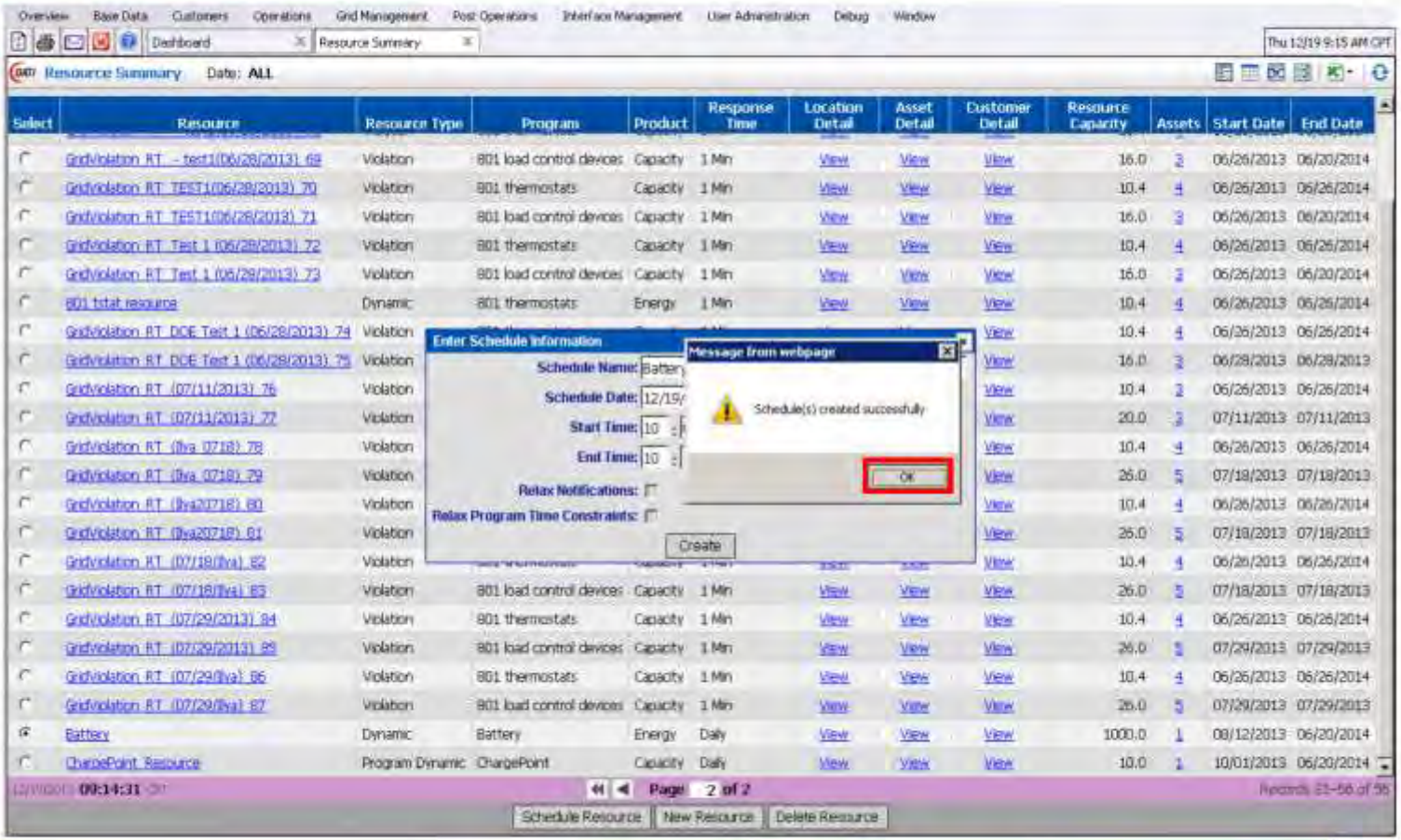
"Schedule Resource" to Schedule DR Event



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

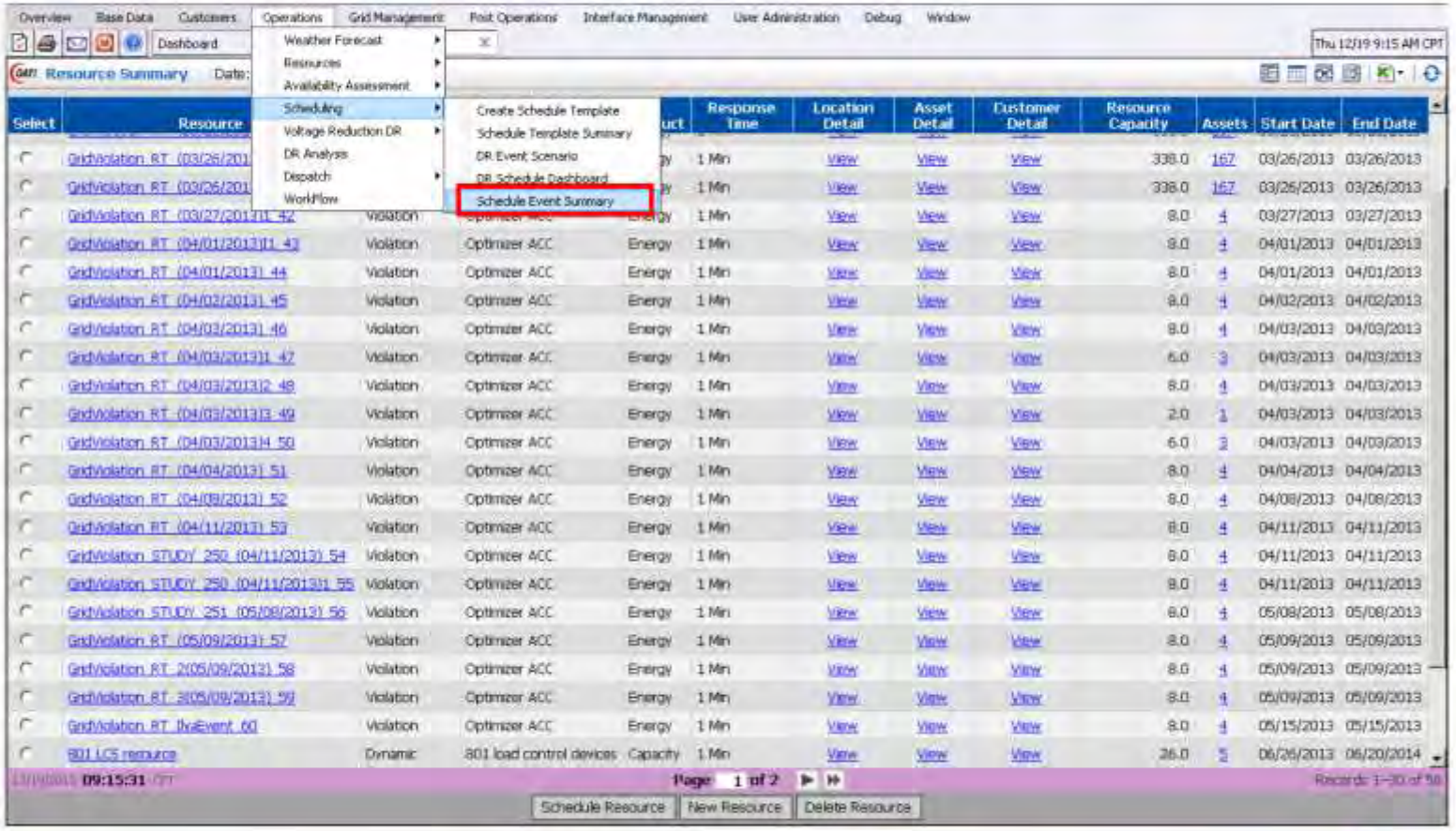

Enter Schedule Information
Overview Base Data Customers Operations Grid Management Post Operations Interface Management User Administration Debug Window
Dashboard
Resource Summary
Thu 12/19 9:15 AM CPT
Resource Summary Date: ALL
Select Resource Resource Type Program Product Response Time Location Detail Asset Detail Customer Detail Resource Capacity Assets Start Date End Date
GridViolation_RT_-test1(06/28/2013)_69 Violation 801 load control devices Capacity 1 Min View View View 16.0 3 06/26/2013 06/20/2014
GridViolation_RT_TEST1(06/28/2013)_70 Violation 801 thermostats Capacity 1 Min View View View 10.4 4 06/26/2013 06/26/2014
GridViolation_RT_TEST1(06/28/2013)_71 Violation 801 load control devices Capacity 1 Min View View View 16.0 3 06/26/2013 06/20/2014
GridViolation_RT_Test 1 (06/28/2013)_72 Violation 801 thermostats Capacity 1 Min View View View 10.4 4 06/26/2013 06/26/2014
GridViolation_RT_Test 1 (06/28/2013)_73 Violation 801 load control devices Capacity 1 Min View View View 16.0 3 06/26/2013 06/20/2014
801 total resource Dynamic 801 thermostats Energy 1 Min View View View 10.4 4 06/26/2013 06/26/2014
GridViolation_RT_DOE Test 1 (06/28/2013)_74 Violation View 10.4 4 06/26/2013 06/26/2014
GridViolation_RT_DOE Test 1 (06/28/2013)_75 Violation View 16.0 3 06/28/2013 06/28/2013
GridViolation_RT_(07/11/2013)_76 Violation View 10.4 2 06/26/2013 06/26/2014
GridViolation_RT_(07/11/2013)_77 Violation View 20.0 3 07/11/2013 07/11/2013
GridViolation_RT_(Ilva_0718)_78 Violation View 10.4 4 06/26/2013 06/26/2014
GridViolation_RT_(Ilva_0718)_79 Violation View 26.0 5 07/18/2013 07/18/2013
GridViolation_RT_(Ilva20718)_80 Violation View 10.4 4 06/26/2013 06/26/2014
GridViolation_RT_(Ilva20718)_81 Violation View 26.0 5 07/18/2013 07/18/2013
GridViolation_RT_(07/18/Ilva)_82 Violation View 10.4 4 06/26/2013 06/26/2014
GridViolation_RT_(07/18/Ilva)_83 Violation 801 load control devices Capacity 1 Min View View View 26.0 5 07/18/2013 07/18/2013
GridViolation_RT_(07/29/2013)_84 Violation 801 thermostats Capacity 1 Min View View View 10.4 4 06/26/2013 06/26/2014
GridViolation_RT_(07/29/2013)_85 Violation 801 load control devices Capacity 1 Min View View View 26.0 5 07/29/2013 07/29/2013
GridViolation_RT_(07/29/Ilva)_86 Violation 801 thermostats Capacity 1 Min View View View 10.4 4 06/26/2013 06/26/2014
GridViolation_RT_(07/29/Ilva)_87 Violation 801 load control devices Capacity 1 Min View View View 26.0 5 07/29/2013 07/29/2013
Battery Dynamic Battery Energy Daily View View View 1000.0 1 08/12/2013 06/20/2014
ChargePoint_Resource Program Dynamic ChargePoint Capacity Daily View View View 10.0 1 10/01/2013 06/20/2014
Enter Schedule Information
Schedule Name: Battery - test1 (12/19/2013)
Schedule Date: 12/19/2013
Start Time: 10 : 00 Notification: 12/19/2013 09:20
End Time: 10 : 10 Notification: 12/19/2013 10:10
Relax Notifications:
Relax Program Time Constraints:
Create
09:14:31
Page 2 of 2
Schedule Resource
New Resource
Delete Resource
14
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

Event Schedule Created



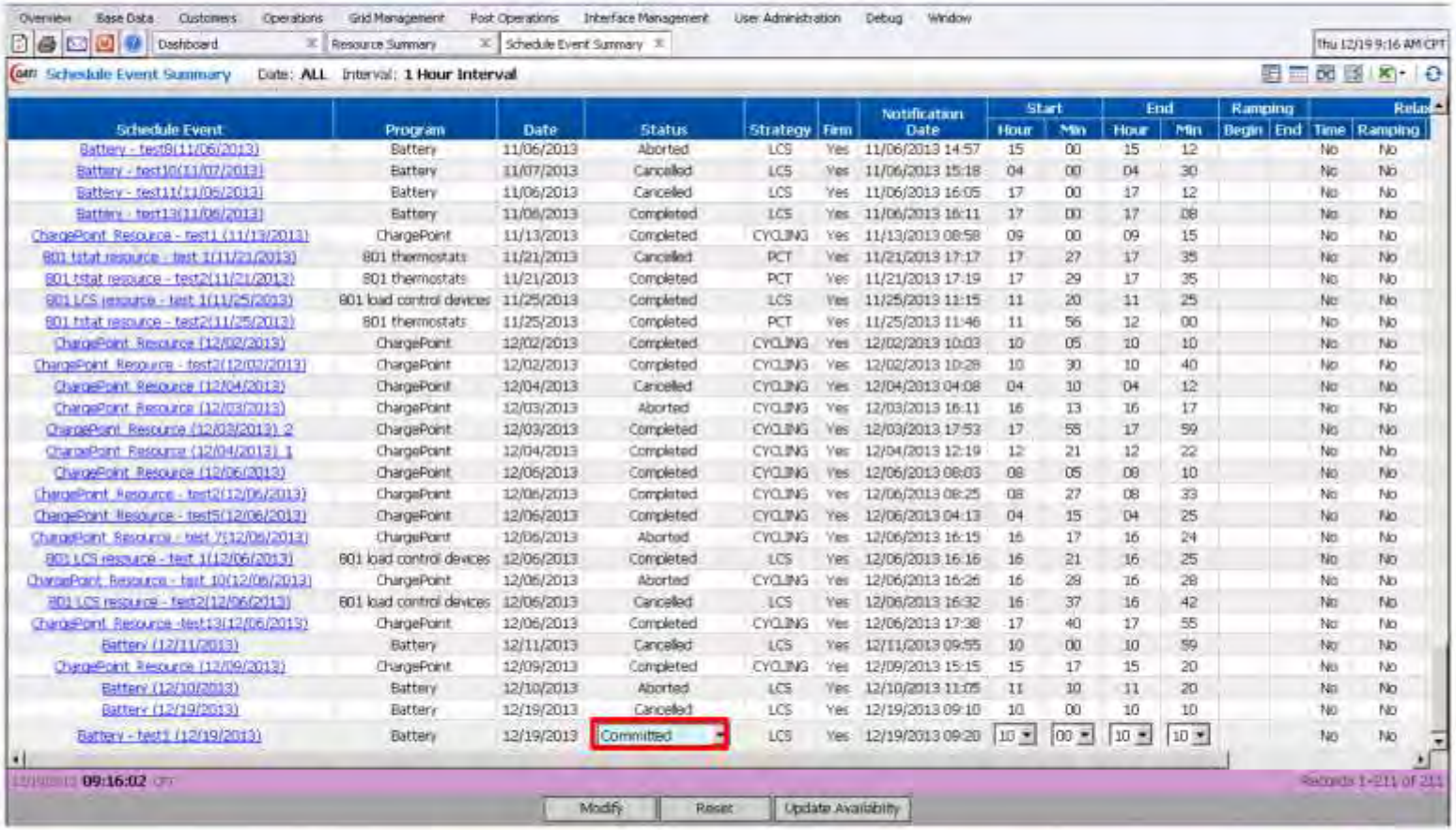
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Go to "Schedule Event Summary"



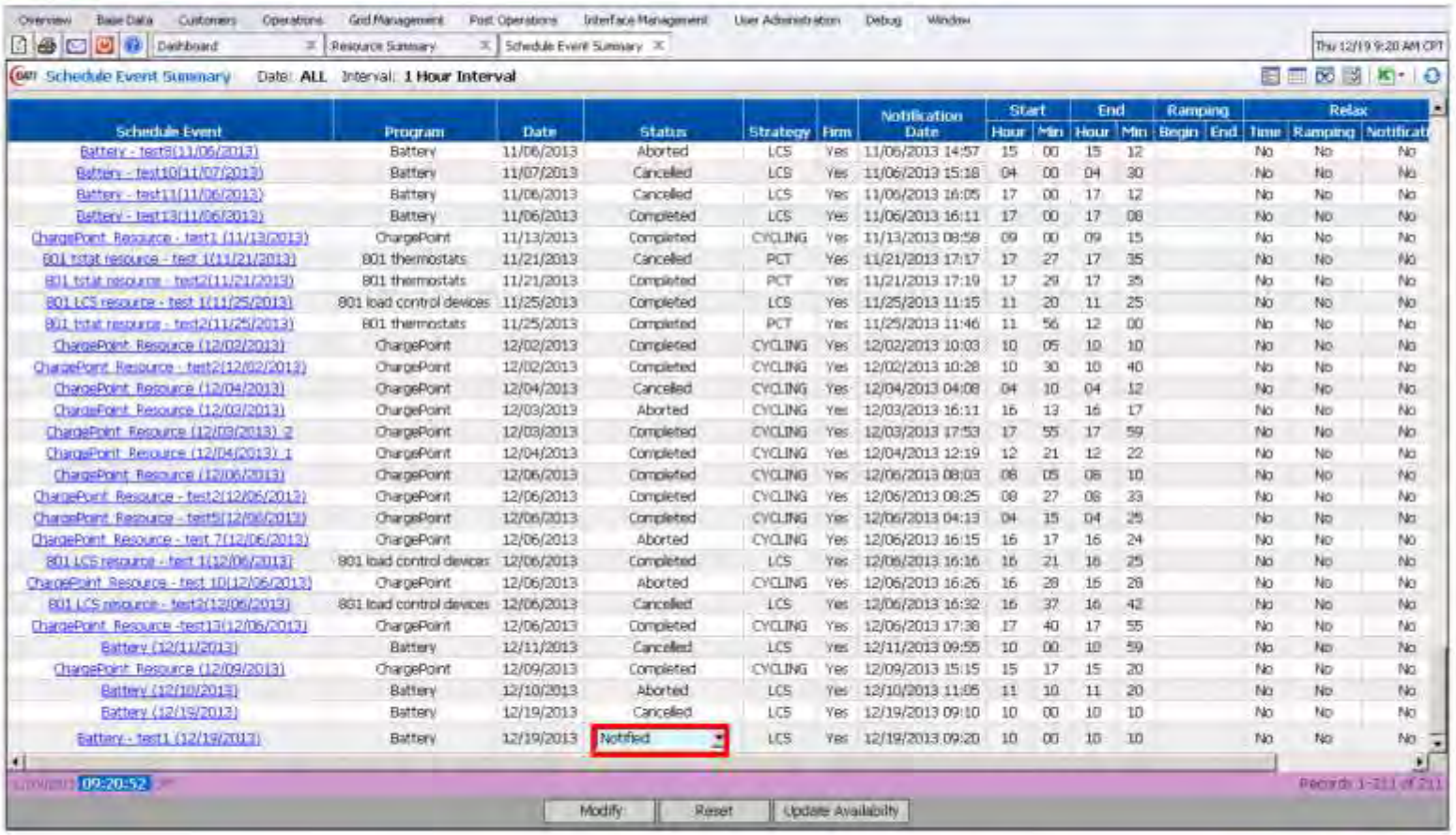
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

List of Scheduled Event Summaries

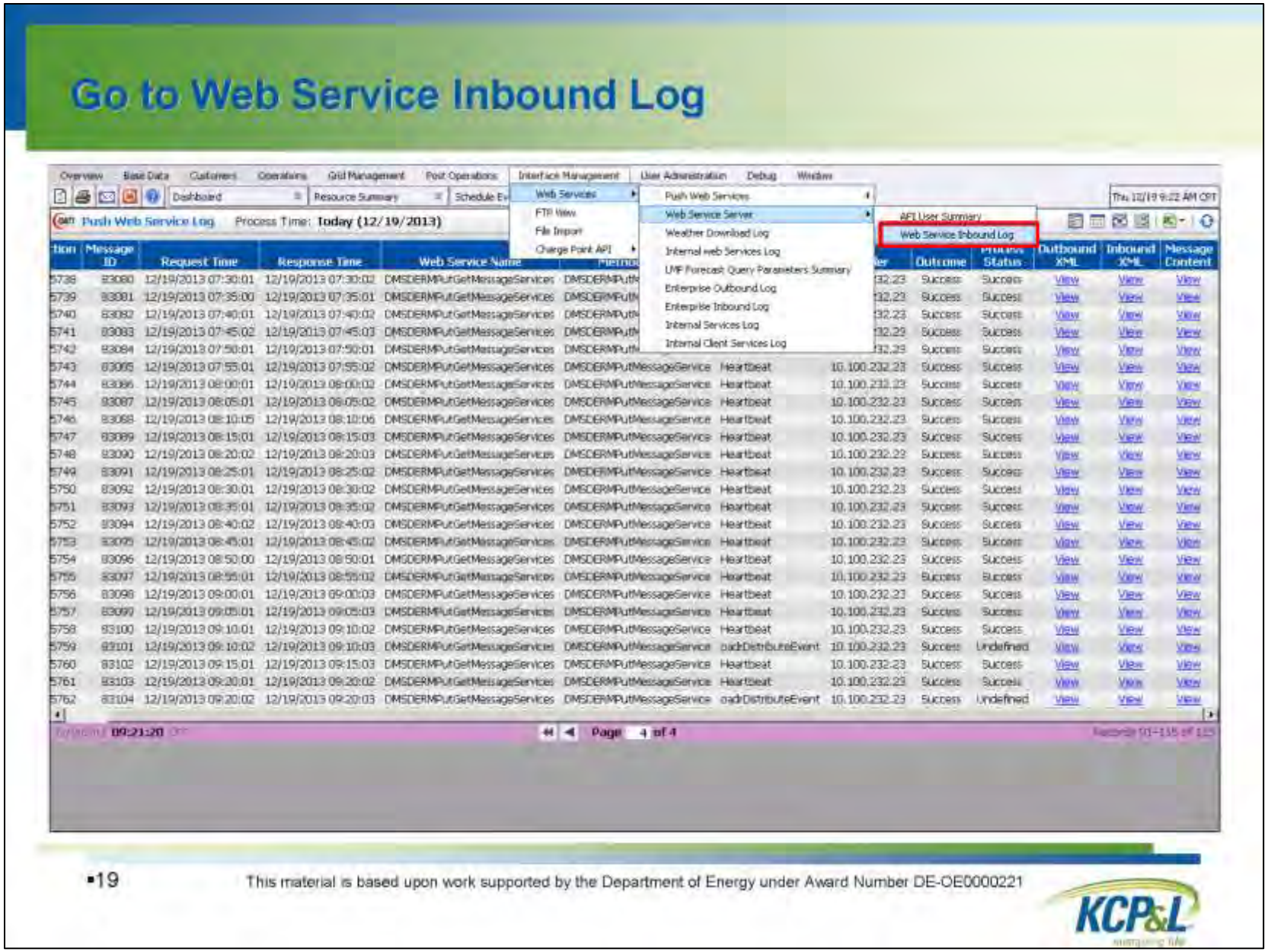


This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

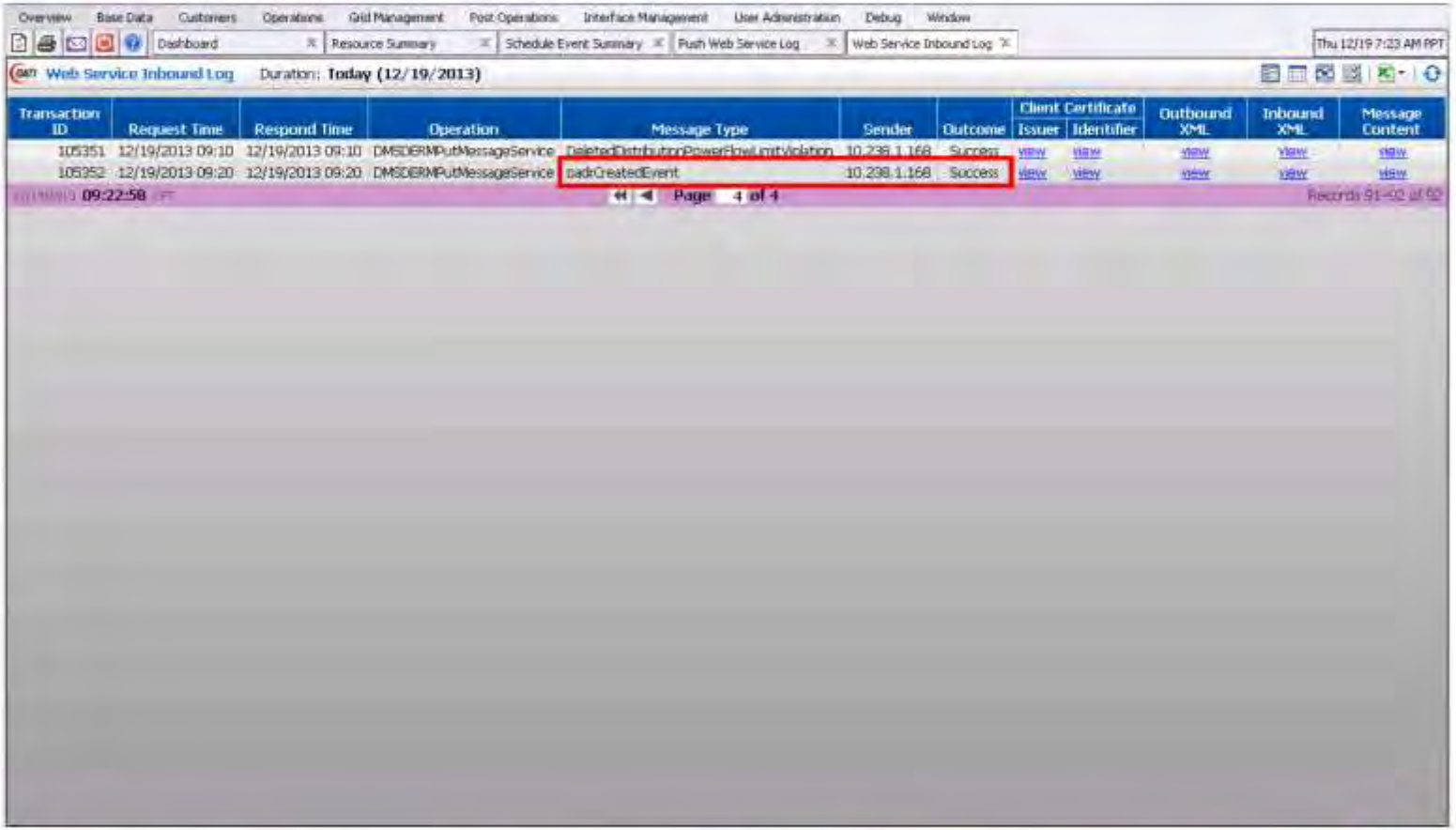
Status Change to "Notified" after Event Sent from DERM



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

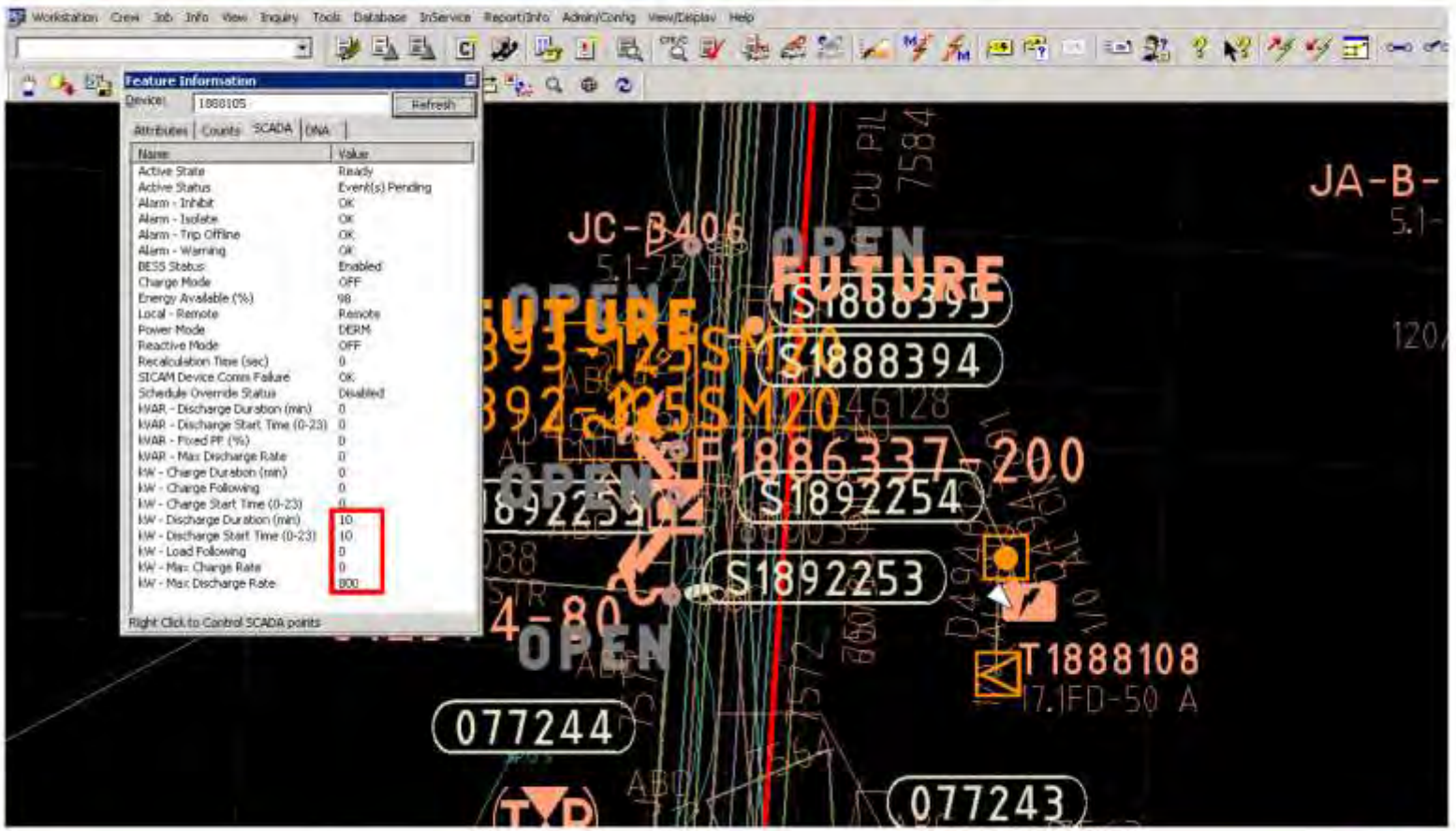

Go to Web Service Inbound Log
Overview
Base Data
Customers
Operations
Grid Management
Post Operations
Interface Management
User Administration
Debug
Window
Web Services
FTP View
File Import
Charge Point API
Push Web Services
Web Service Server
Weather Download Log
Internal web Services Log
UMF Forecast Query Parameters Summary
Enterprise Outbound Log
Enterprise Inbound Log
Internal Services Log
Internal Client Services Log
API User Summary
Web Service Inbound Log
Push Web Service Log
Process Time: Today (12/19/2013)
Message ID
Request Time
Response Time
Web Service Name
Outcome
Process Status
Outbound XML
Inbound XML
Message Content
Page 4 of 4
19
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Web Service Inbound Logs



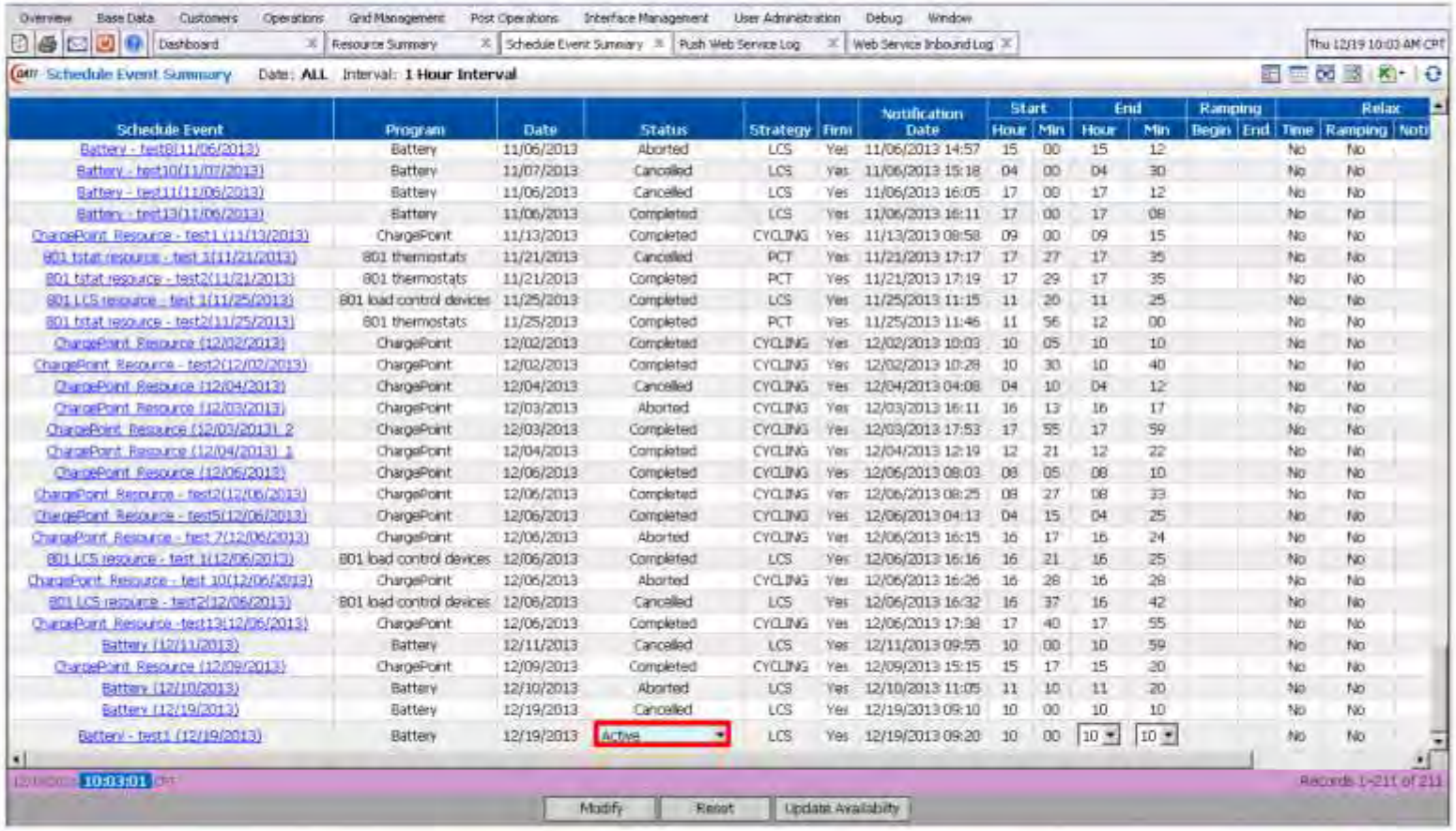
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

OMS: Battery Information Updated



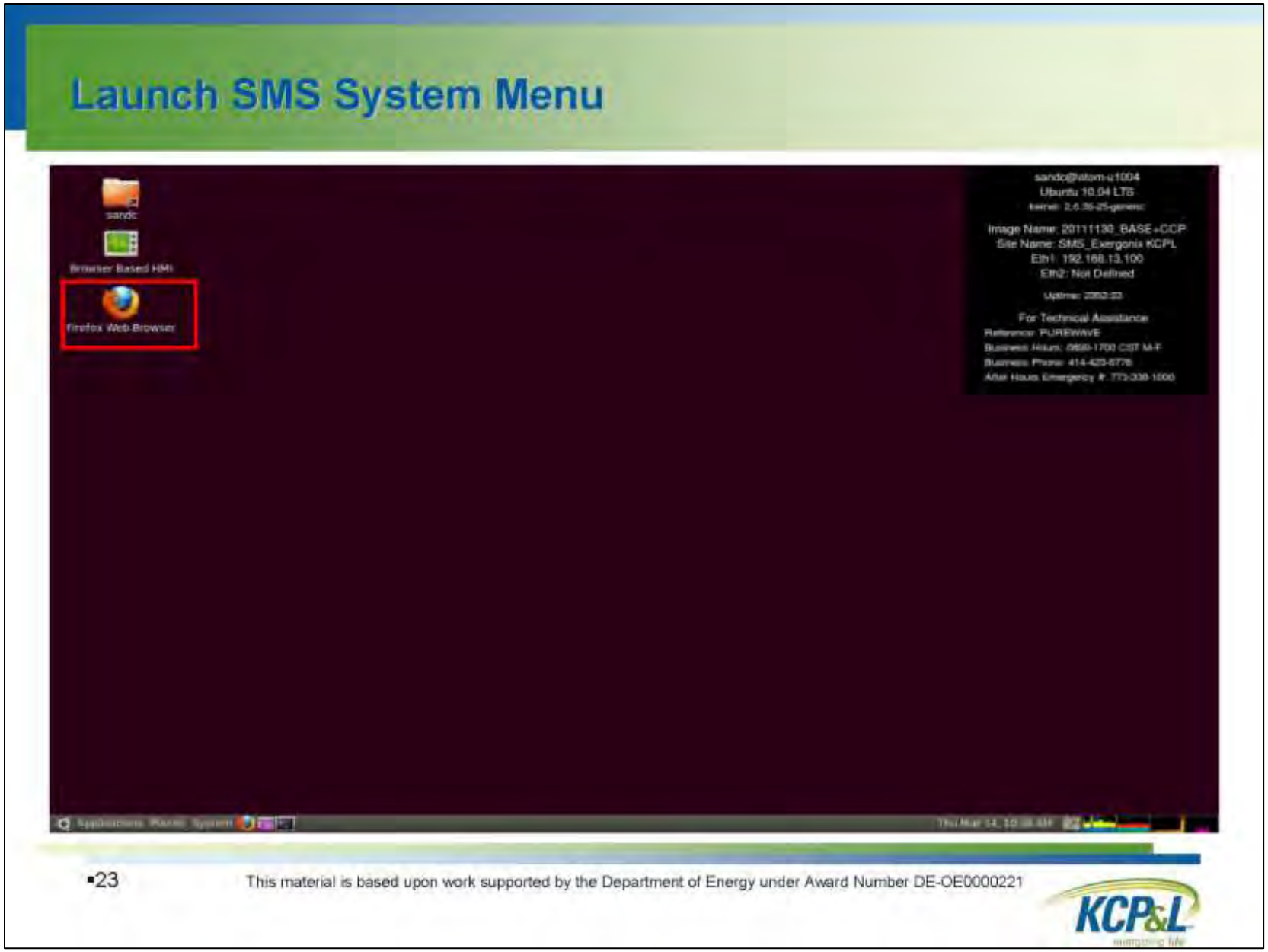
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

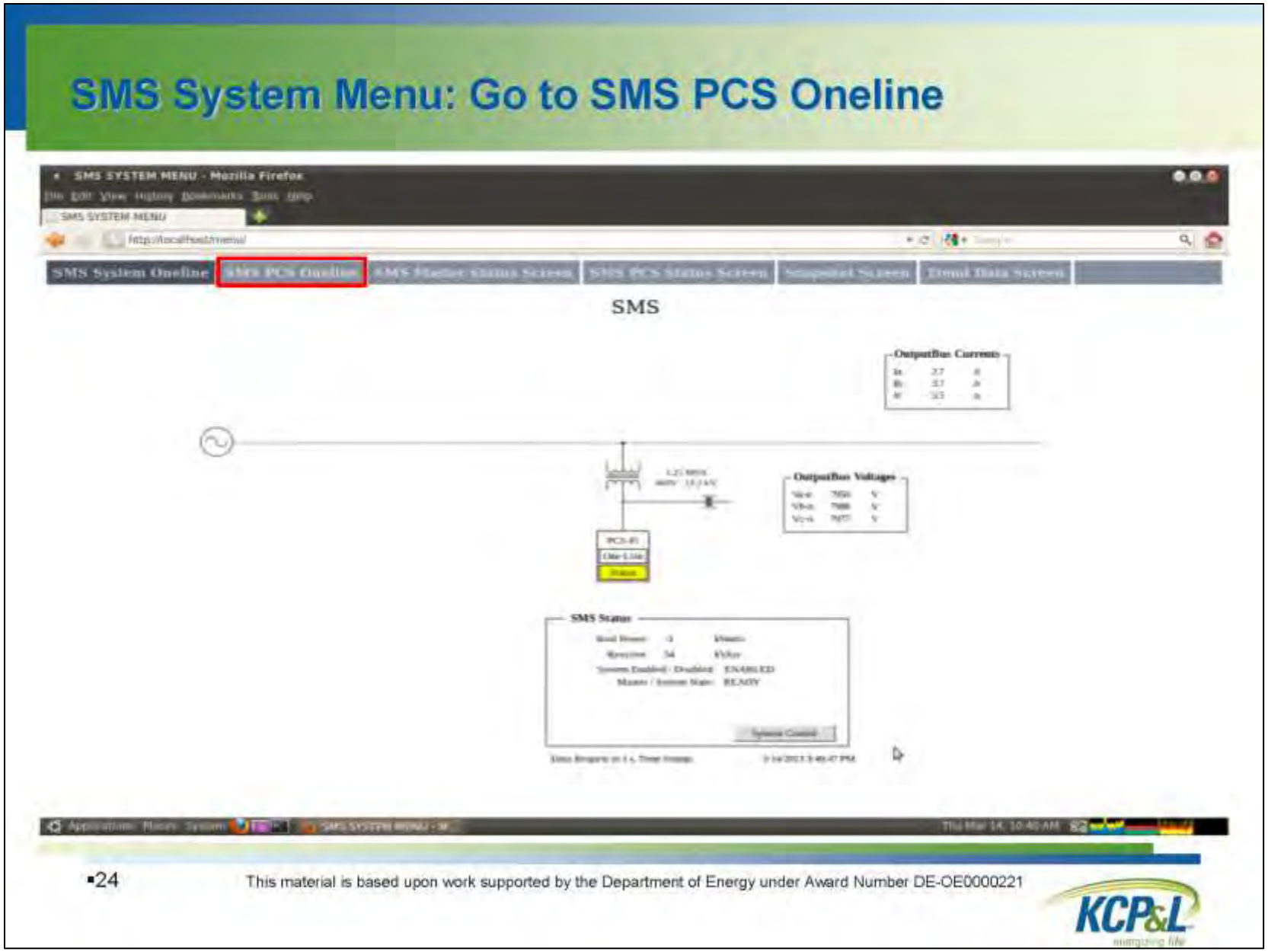
DERM: Status Updated to Active after Event Started



Schedule Event	Program	Date	Status	Strategy	Firm	Notification Date	Start Hour	Start Min	End Hour	End Min	Ramping Begin	Ramping End	Relax Time	Relax Ramping	Noti
Battery - test8(11/06/2013)	Battery	11/06/2013	Aborted	LCS	Yes	11/06/2013 14:57	15	00	15	12			No	No	
Battery - test10(11/07/2013)	Battery	11/07/2013	Cancelled	LCS	Yes	11/06/2013 15:18	04	00	04	30			No	No	
Battery - test11(11/06/2013)	Battery	11/06/2013	Cancelled	LCS	Yes	11/06/2013 16:05	17	00	17	12			No	No	
Battery - test13(11/06/2013)	Battery	11/06/2013	Completed	LCS	Yes	11/06/2013 16:11	17	00	17	08			No	No	
ChargePoint Resource - test1 (11/13/2013)	ChargePoint	11/13/2013	Completed	CYCLING	Yes	11/13/2013 08:58	09	00	09	15			No	No	
801 tstat resource - test 1(11/21/2013)	801 thermostats	11/21/2013	Cancelled	PCT	Yes	11/21/2013 17:17	17	27	17	35			No	No	
801 tstat resource - test2(11/21/2013)	801 thermostats	11/21/2013	Completed	PCT	Yes	11/21/2013 17:19	17	29	17	35			No	No	
801 LCS resource - test 1(11/25/2013)	801 load control devices	11/25/2013	Completed	LCS	Yes	11/25/2013 11:15	11	20	11	25			No	No	
801 tstat resource - test2(11/25/2013)	801 thermostats	11/25/2013	Completed	PCT	Yes	11/25/2013 11:46	11	56	12	00			No	No	
ChargePoint Resource (12/02/2013)	ChargePoint	12/02/2013	Completed	CYCLING	Yes	12/02/2013 10:03	10	05	10	10			No	No	
ChargePoint Resource - test2(12/02/2013)	ChargePoint	12/02/2013	Completed	CYCLING	Yes	12/02/2013 10:28	10	30	10	40			No	No	
ChargePoint Resource (12/04/2013)	ChargePoint	12/04/2013	Cancelled	CYCLING	Yes	12/04/2013 04:08	04	10	04	12			No	No	
ChargePoint Resource (12/03/2013)	ChargePoint	12/03/2013	Aborted	CYCLING	Yes	12/03/2013 16:11	16	13	16	17			No	No	
ChargePoint Resource (12/03/2013) 2	ChargePoint	12/03/2013	Completed	CYCLING	Yes	12/03/2013 17:53	17	55	17	59			No	No	
ChargePoint Resource (12/04/2013) 1	ChargePoint	12/04/2013	Completed	CYCLING	Yes	12/04/2013 12:19	12	21	12	22			No	No	
ChargePoint Resource (12/06/2013)	ChargePoint	12/06/2013	Completed	CYCLING	Yes	12/06/2013 08:03	08	05	08	10			No	No	
ChargePoint Resource - test2(12/06/2013)	ChargePoint	12/06/2013	Completed	CYCLING	Yes	12/06/2013 08:25	08	27	08	33			No	No	
ChargePoint Resource - test5(12/06/2013)	ChargePoint	12/06/2013	Completed	CYCLING	Yes	12/06/2013 04:13	04	15	04	25			No	No	
ChargePoint Resource - test 7(12/06/2013)	ChargePoint	12/06/2013	Aborted	CYCLING	Yes	12/06/2013 16:15	16	17	16	24			No	No	
801 LCS resource - test 1(12/06/2013)	801 load control devices	12/06/2013	Completed	LCS	Yes	12/06/2013 16:16	16	21	16	25			No	No	
ChargePoint Resource - test 10(12/06/2013)	ChargePoint	12/06/2013	Aborted	CYCLING	Yes	12/06/2013 16:26	16	28	16	28			No	No	
801 LCS resource - test2(12/06/2013)	801 load control devices	12/06/2013	Cancelled	LCS	Yes	12/06/2013 16:32	16	37	16	42			No	No	
ChargePoint Resource -test13(12/06/2013)	ChargePoint	12/06/2013	Completed	CYCLING	Yes	12/06/2013 17:38	17	40	17	55			No	No	
Battery (12/11/2013)	Battery	12/11/2013	Cancelled	LCS	Yes	12/11/2013 09:55	10	00	10	59			No	No	
ChargePoint Resource (12/09/2013)	ChargePoint	12/09/2013	Completed	CYCLING	Yes	12/09/2013 15:15	15	17	15	30			No	No	
Battery (12/10/2013)	Battery	12/10/2013	Aborted	LCS	Yes	12/10/2013 11:05	11	10	11	20			No	No	
Battery (12/19/2013)	Battery	12/19/2013	Cancelled	LCS	Yes	12/19/2013 09:10	10	00	10	10			No	No	
Battery - test1 (12/19/2013)	Battery	12/19/2013	Active	LCS	Yes	12/19/2013 09:20	10	00	10	10			No	No	

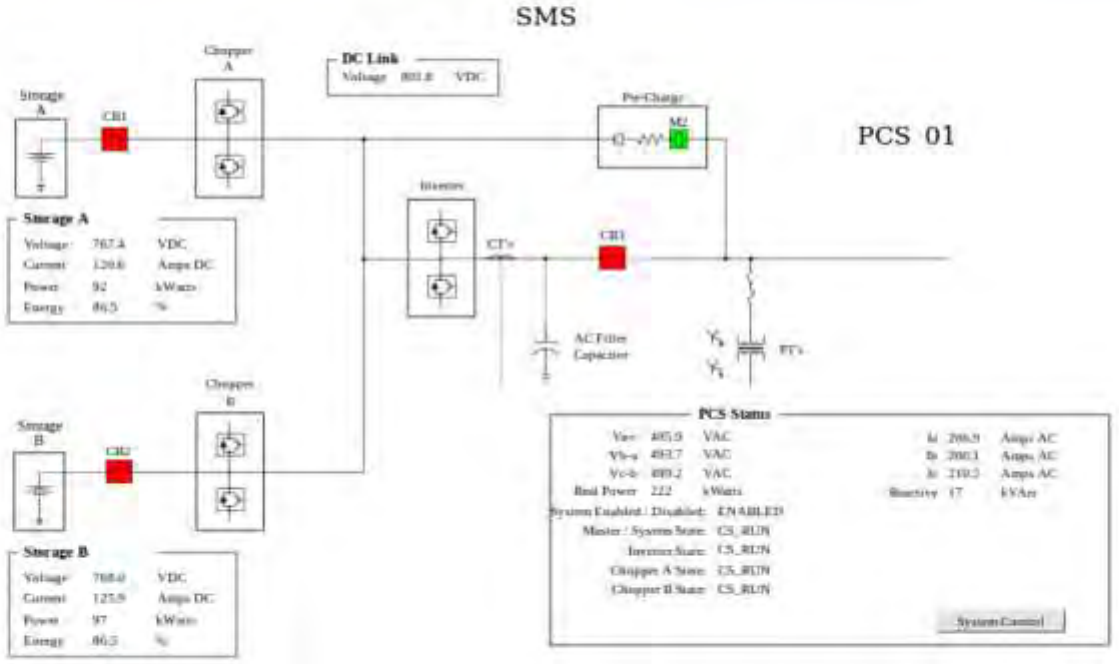
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221


Launch SMS System Menu
sandc
Browser Based HMI
Firefox Web Browser
Image Name: 20111130_BASE+CCP
Site Name: SMS_Exergonix KCPL
Eth1: 192.168.13.100
Eth2: Not Defined
For Technical Assistance
23
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L


SMS System Menu: Go to SMS PCS Oneline
SMS SYSTEM MENU - Mozilla Firefox
SMS System Oneline
SMS PCS Oneline
SMS
OutputBus Currents
OutputBus Voltages
SMS Status
24
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L
energizing life

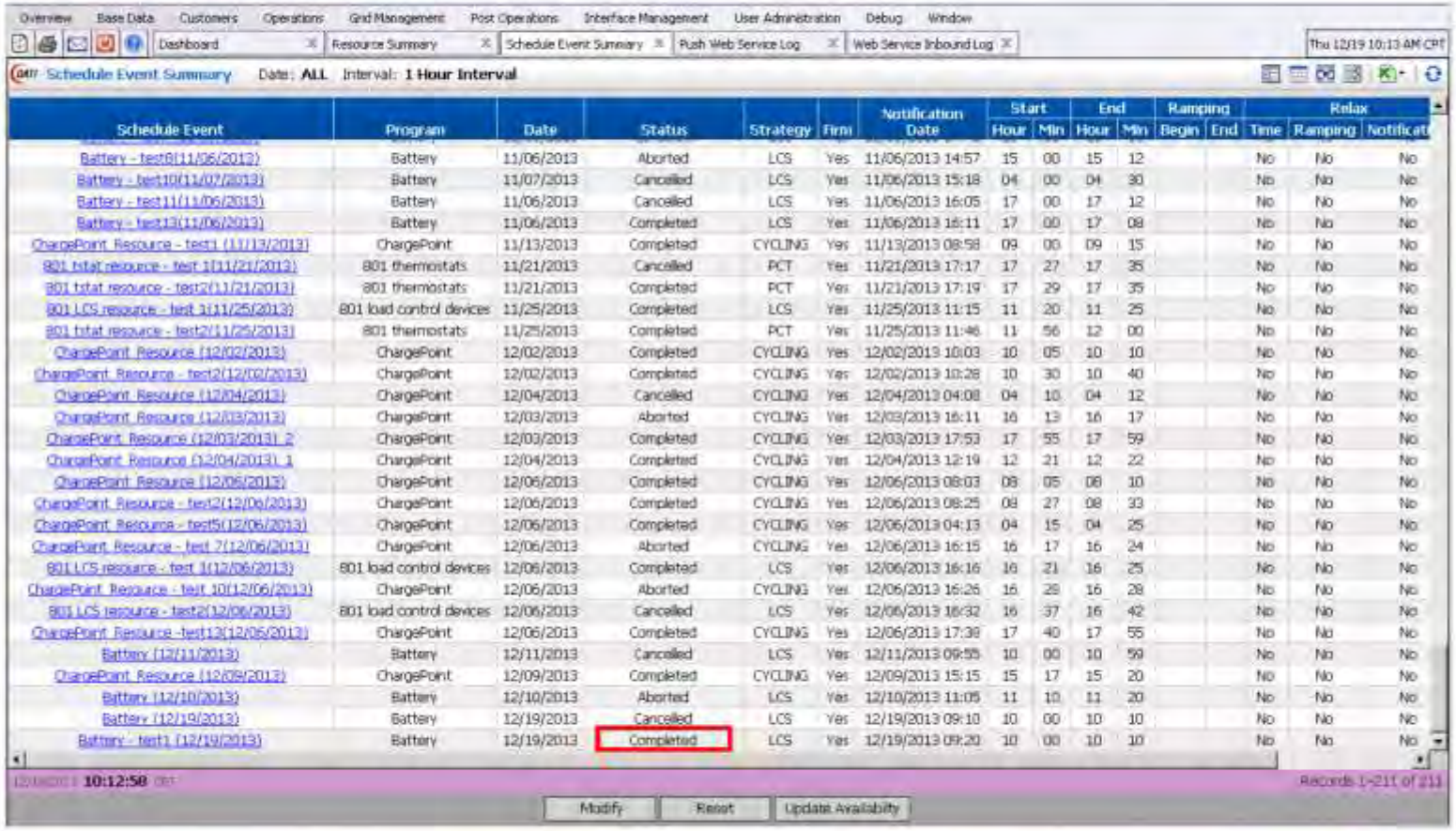
SMS PCS Oneline: Battery is Discharging

SMS System Oneline | SMS PCS Oneline | SMS Master Status Screen | SMS PCS Status Screen | Snapshot Screen
Trend Data Screen



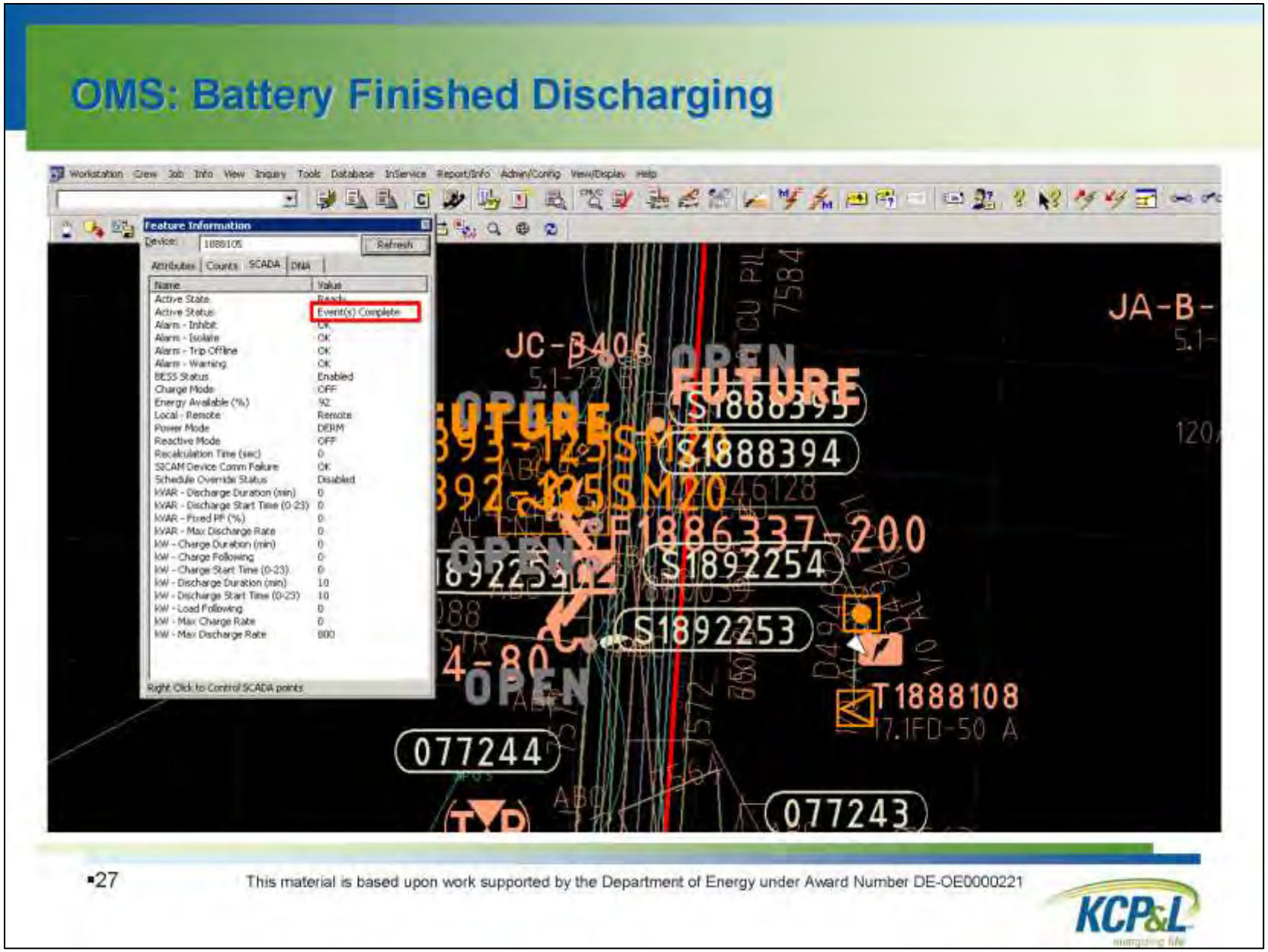
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

DERM: Event Complete



Schedule Event	Program	Date	Status	Strategy	Firm	Notification Date	Start Hour	Start Min	End Hour	End Min	Ramping Begin	Ramping End	Relax Time	Relax Ramping	Relax Notificati
Battery - test9(11/06/2013)	Battery	11/06/2013	Aborted	LCS	Yes	11/06/2013 14:57	15	00	15	12			No	No	No
Battery - test10(11/07/2013)	Battery	11/07/2013	Cancelled	LCS	Yes	11/06/2013 15:18	04	00	04	30			No	No	No
Battery - test11(11/06/2013)	Battery	11/06/2013	Cancelled	LCS	Yes	11/06/2013 16:05	17	00	17	12			No	No	No
Battery - test13(11/06/2013)	Battery	11/06/2013	Completed	LCS	Yes	11/06/2013 16:11	17	00	17	08			No	No	No
ChargePoint Resource - test1 (11/13/2013)	ChargePoint	11/13/2013	Completed	CYCLING	Yes	11/13/2013 08:58	09	00	09	15			No	No	No
801 tstat resource - test 1(11/21/2013)	801 thermostats	11/21/2013	Cancelled	PCT	Yes	11/21/2013 17:17	17	27	17	35			No	No	No
801 tstat resource - test2(11/21/2013)	801 thermostats	11/21/2013	Completed	PCT	Yes	11/21/2013 17:19	17	29	17	35			No	No	No
801 LCS resource - test 1(11/25/2013)	801 load control devices	11/25/2013	Completed	LCS	Yes	11/25/2013 11:15	11	20	11	25			No	No	No
801 tstat resource - test2(11/25/2013)	801 thermostats	11/25/2013	Completed	PCT	Yes	11/25/2013 11:46	11	56	12	00			No	No	No
ChargePoint Resource (12/02/2013)	ChargePoint	12/02/2013	Completed	CYCLING	Yes	12/02/2013 10:03	10	05	10	10			No	No	No
ChargePoint Resource - test2(12/02/2013)	ChargePoint	12/02/2013	Completed	CYCLING	Yes	12/02/2013 10:28	10	30	10	40			No	No	No
ChargePoint Resource (12/04/2013)	ChargePoint	12/04/2013	Cancelled	CYCLING	Yes	12/04/2013 04:08	04	10	04	12			No	No	No
ChargePoint Resource (12/03/2013)	ChargePoint	12/03/2013	Aborted	CYCLING	Yes	12/03/2013 16:11	16	13	16	17			No	No	No
ChargePoint Resource (12/03/2013) 2	ChargePoint	12/03/2013	Completed	CYCLING	Yes	12/03/2013 17:53	17	55	17	59			No	No	No
ChargePoint Resource (12/04/2013) 1	ChargePoint	12/04/2013	Completed	CYCLING	Yes	12/04/2013 12:19	12	21	12	22			No	No	No
ChargePoint Resource (12/06/2013)	ChargePoint	12/06/2013	Completed	CYCLING	Yes	12/06/2013 08:03	08	05	08	10			No	No	No
ChargePoint Resource - test2(12/06/2013)	ChargePoint	12/06/2013	Completed	CYCLING	Yes	12/06/2013 08:25	08	27	08	33			No	No	No
ChargePoint Resource - test5(12/06/2013)	ChargePoint	12/06/2013	Completed	CYCLING	Yes	12/06/2013 04:13	04	15	04	25			No	No	No
ChargePoint Resource - test 7(12/06/2013)	ChargePoint	12/06/2013	Aborted	CYCLING	Yes	12/06/2013 16:15	16	17	16	24			No	No	No
801 LCS resource - test 1(12/06/2013)	801 load control devices	12/06/2013	Completed	LCS	Yes	12/06/2013 16:16	16	21	16	25			No	No	No
ChargePoint Resource - test 10(12/06/2013)	ChargePoint	12/06/2013	Aborted	CYCLING	Yes	12/06/2013 16:26	16	28	16	28			No	No	No
801 LCS resource - test2(12/06/2013)	801 load control devices	12/06/2013	Cancelled	LCS	Yes	12/06/2013 16:32	16	37	16	42			No	No	No
ChargePoint Resource -test13(12/06/2013)	ChargePoint	12/06/2013	Completed	CYCLING	Yes	12/06/2013 17:39	17	40	17	55			No	No	No
Battery (12/11/2013)	Battery	12/11/2013	Cancelled	LCS	Yes	12/11/2013 09:55	10	00	10	59			No	No	No
ChargePoint Resource (12/09/2013)	ChargePoint	12/09/2013	Completed	CYCLING	Yes	12/09/2013 15:15	15	17	15	20			No	No	No
Battery (12/10/2013)	Battery	12/10/2013	Aborted	LCS	Yes	12/10/2013 11:05	11	10	11	20			No	No	No
Battery (12/19/2013)	Battery	12/19/2013	Cancelled	LCS	Yes	12/19/2013 09:10	10	00	10	10			No	No	No
Battery - test1 (12/19/2013)	Battery	12/19/2013	Completed	LCS	Yes	12/19/2013 09:20	10	00	10	10			No	No	No

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221


OMS: Battery Finished Discharging
Feature Information
Device: 1888105
Refresh
Attributes
Counts
SCADA
DNA
Name
Value
Active State
Active Status
Event(s) Complete
Alarm - Inhibit
Alarm - Isolate
Alarm - Trip Offline
Alarm - Warning
BESS Status
Enabled
Charge Mode
OFF
Energy Available (%)
92
Local - Remote
Remote
Power Mode
DERM
Reactive Mode
OFF
Recalculation Time (sec)
SCADA Device Comm Failure
Schedule Override Status
Disabled
kVAR - Discharge Duration (min)
kVAR - Discharge Start Time (0-23)
kVAR - Fixed PF (%)
kVAR - Max Discharge Rate
kW - Charge Duration (min)
kW - Charge Following
kW - Charge Start Time (0-23)
kW - Discharge Duration (min)
10
kW - Discharge Start Time (0-23)
10
kW - Load Following
kW - Max Charge Rate
kW - Max Discharge Rate
800
Right Click to Control SCADA points
JC-B406
OPEN
FUTURE
S1888395
S1888394
F1886337-200
S1892254
S1892253
T1888108
077244
077243
JA-B-
27
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L


Demand Response – EVCS
- KC Green Impact Zone Initiative
- DOE Regional SmartGrid Demonstration Program
- EPRI SmartGrid Demonstration Program
KCP&L
SmartGrid
the future of energy

EV Dashboard Prior to EV Charging Session

▪2

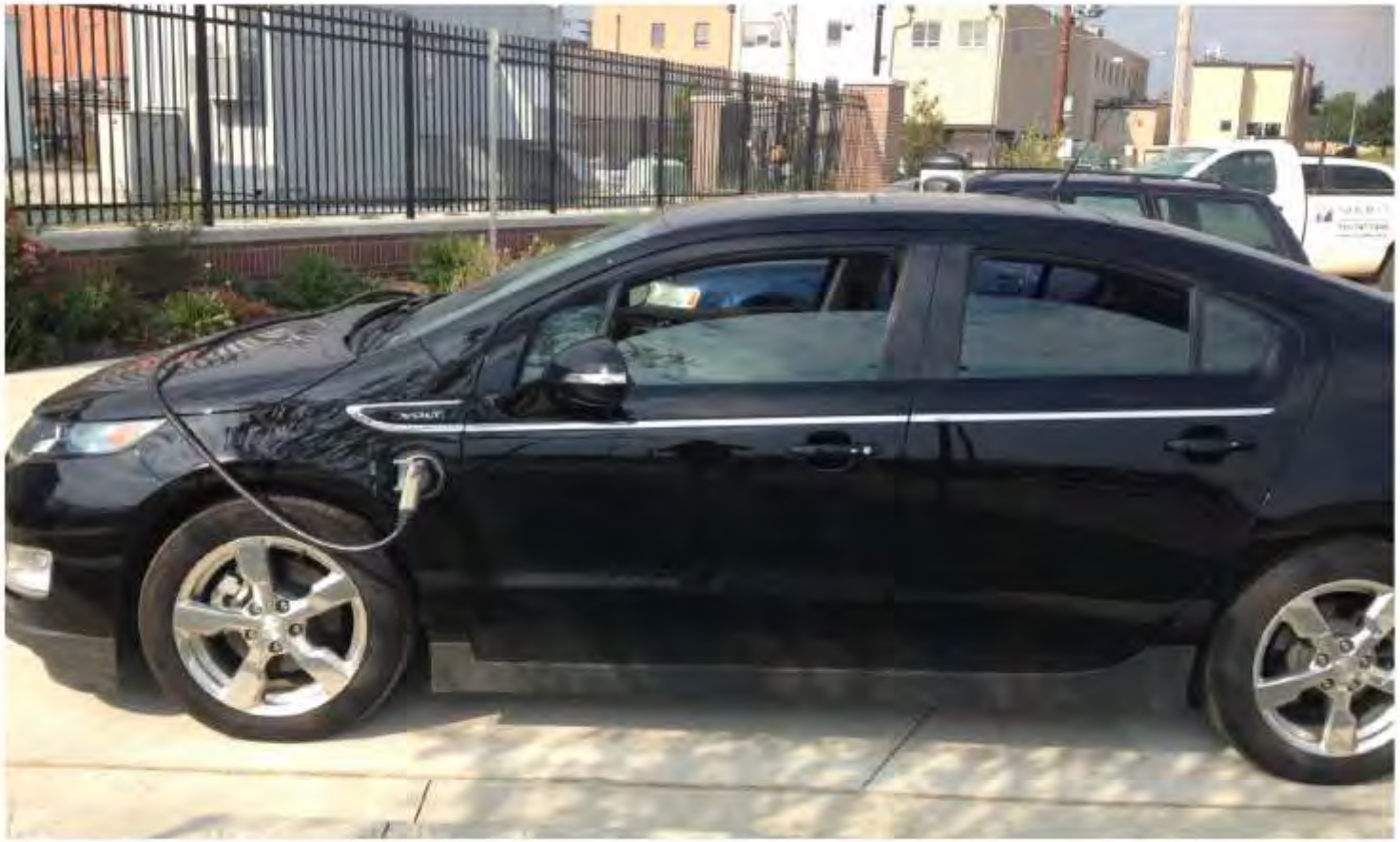
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

KCP&L energizing life

Cell Phone App Prior to EV Charging Session

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

EV Plugged into Charging Station



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

KCP&L energizing life

EV Dashboard: Vehicle Plugged into Station

▪5

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

KCP&L energizing life

EV Dashboard: Vehicle Charging

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

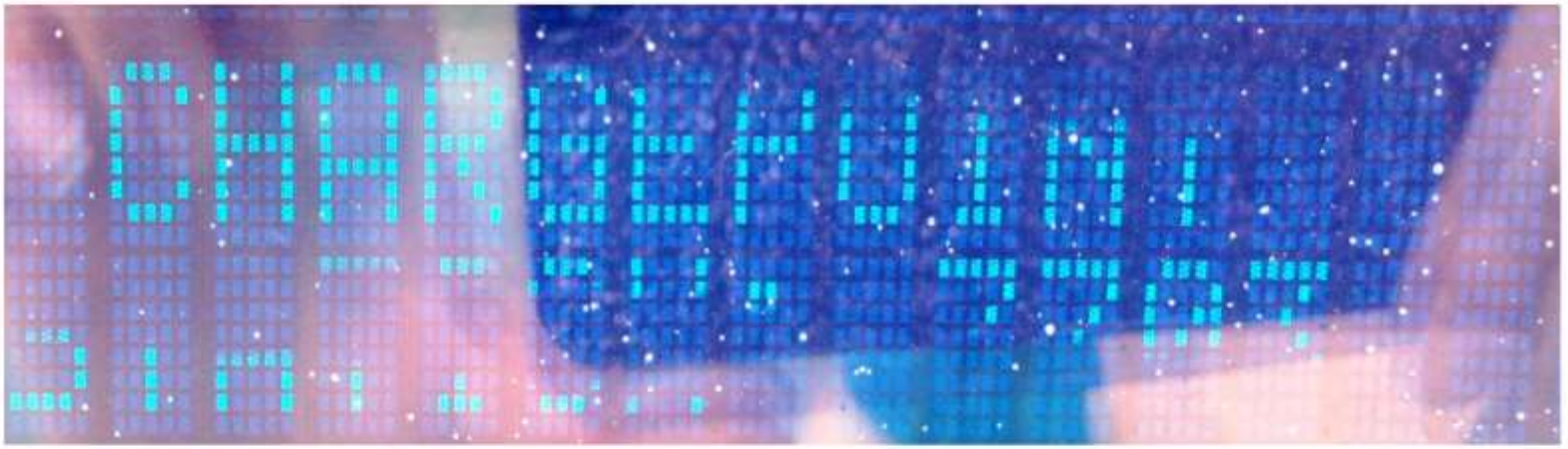
Cell Phone App: Vehicle Charging

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

EVCS Display: EV Plugged in but Prior to DR Event

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

EVCS Display: EV Plugged in but Prior to DR Event



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

EVCS Display: EV Plugged in but Prior to DR Event

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

EVCS Display: EV Plugged in but Prior to DR Event

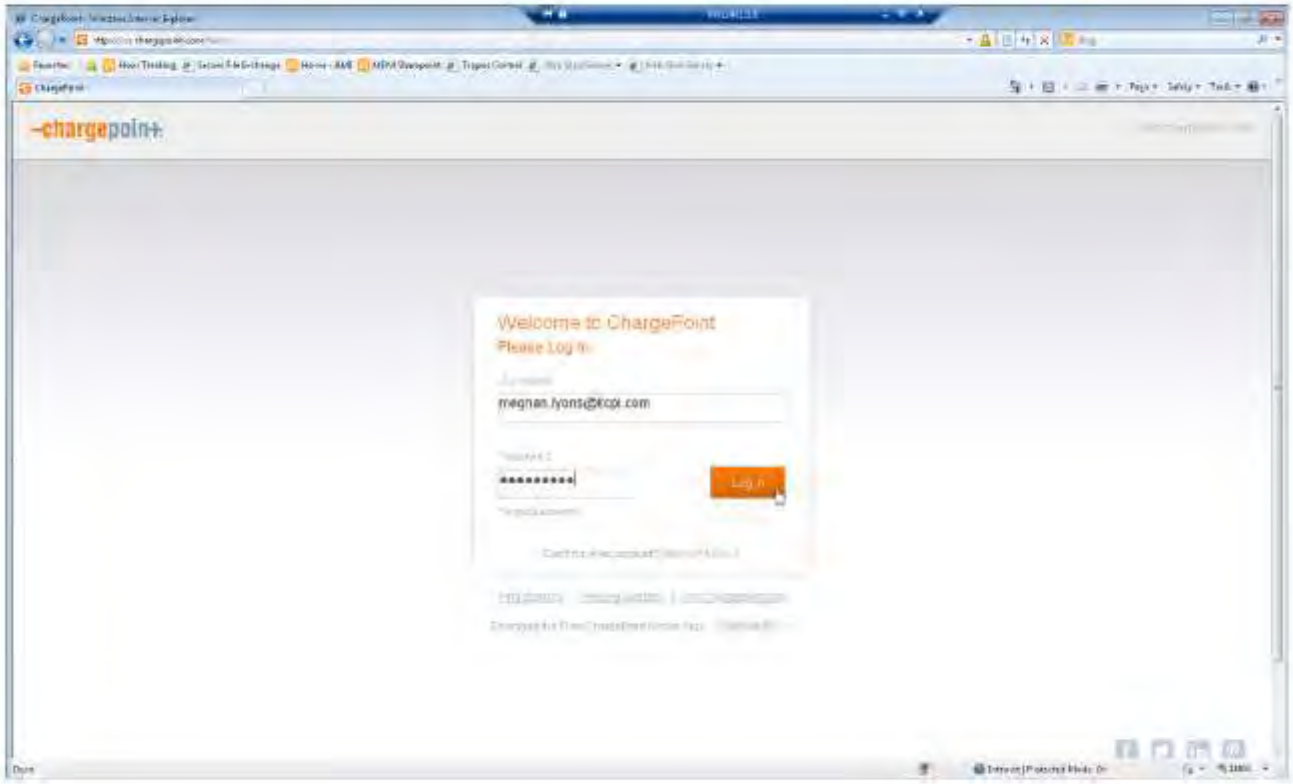
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

KCP&L energizing life

EVCS Display: EV Plugged in but Prior to DR Event

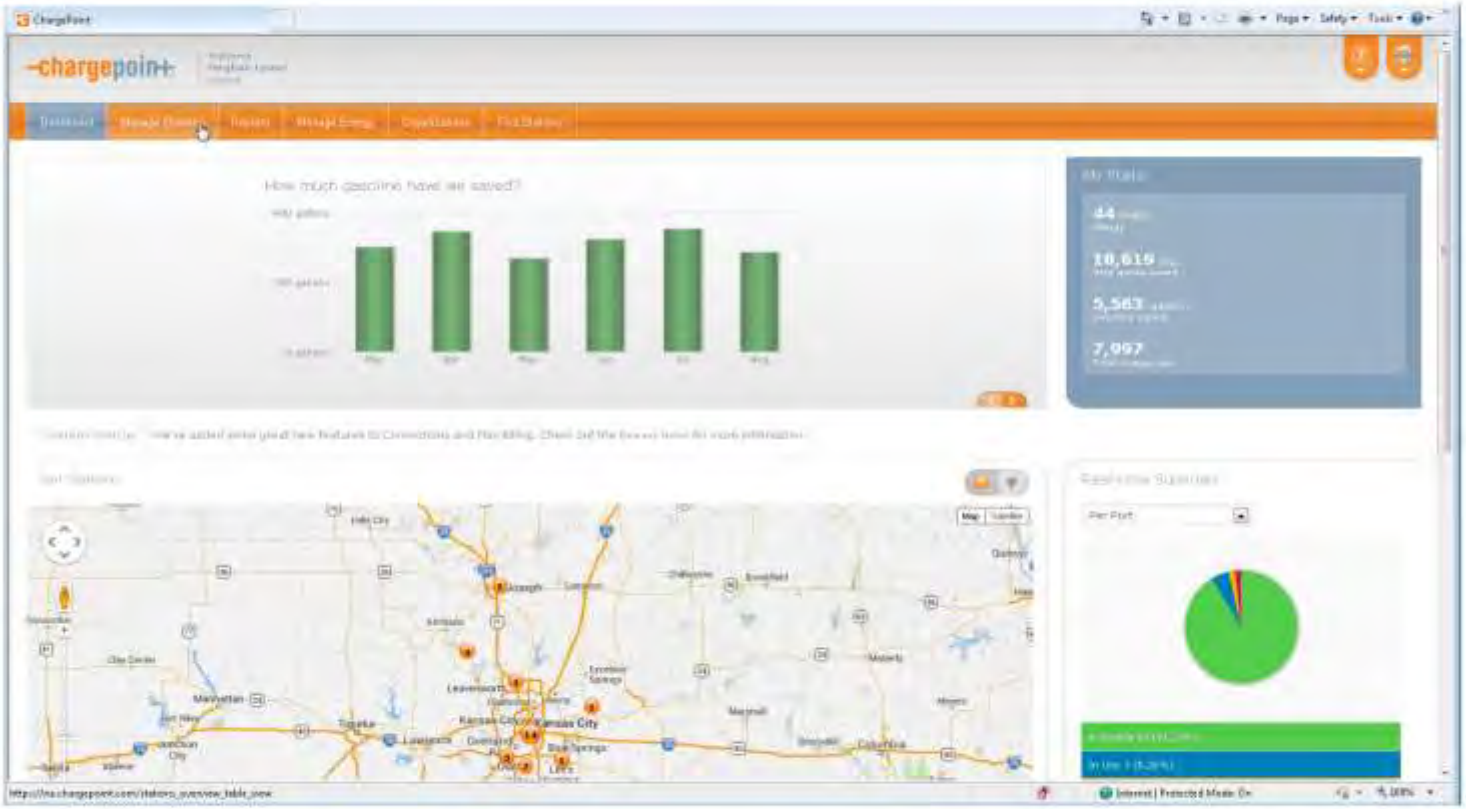
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Launch ChargePoint



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

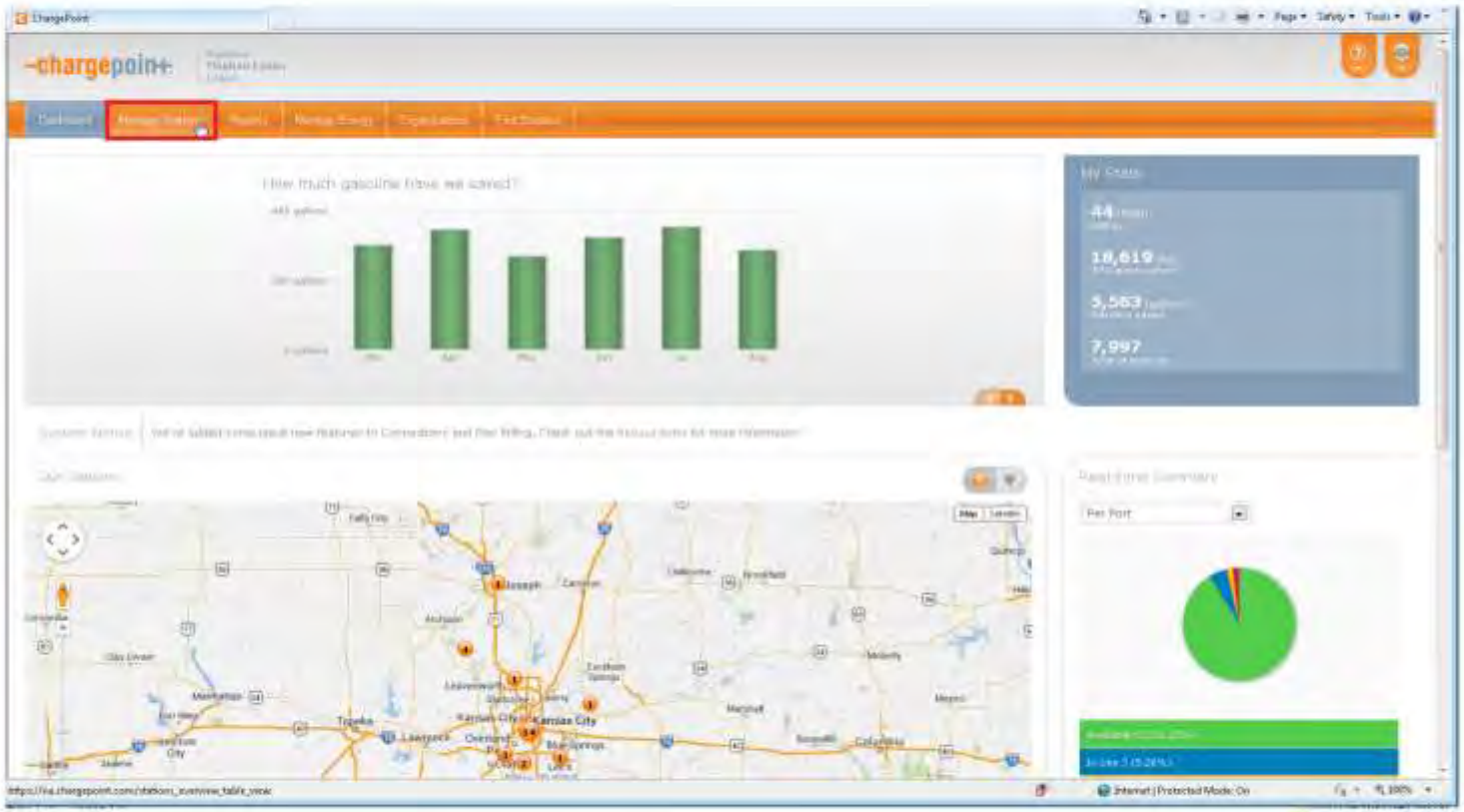
ChargePoint Dashboard



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

KCP&L energizing life

Go to "Manage Stations"



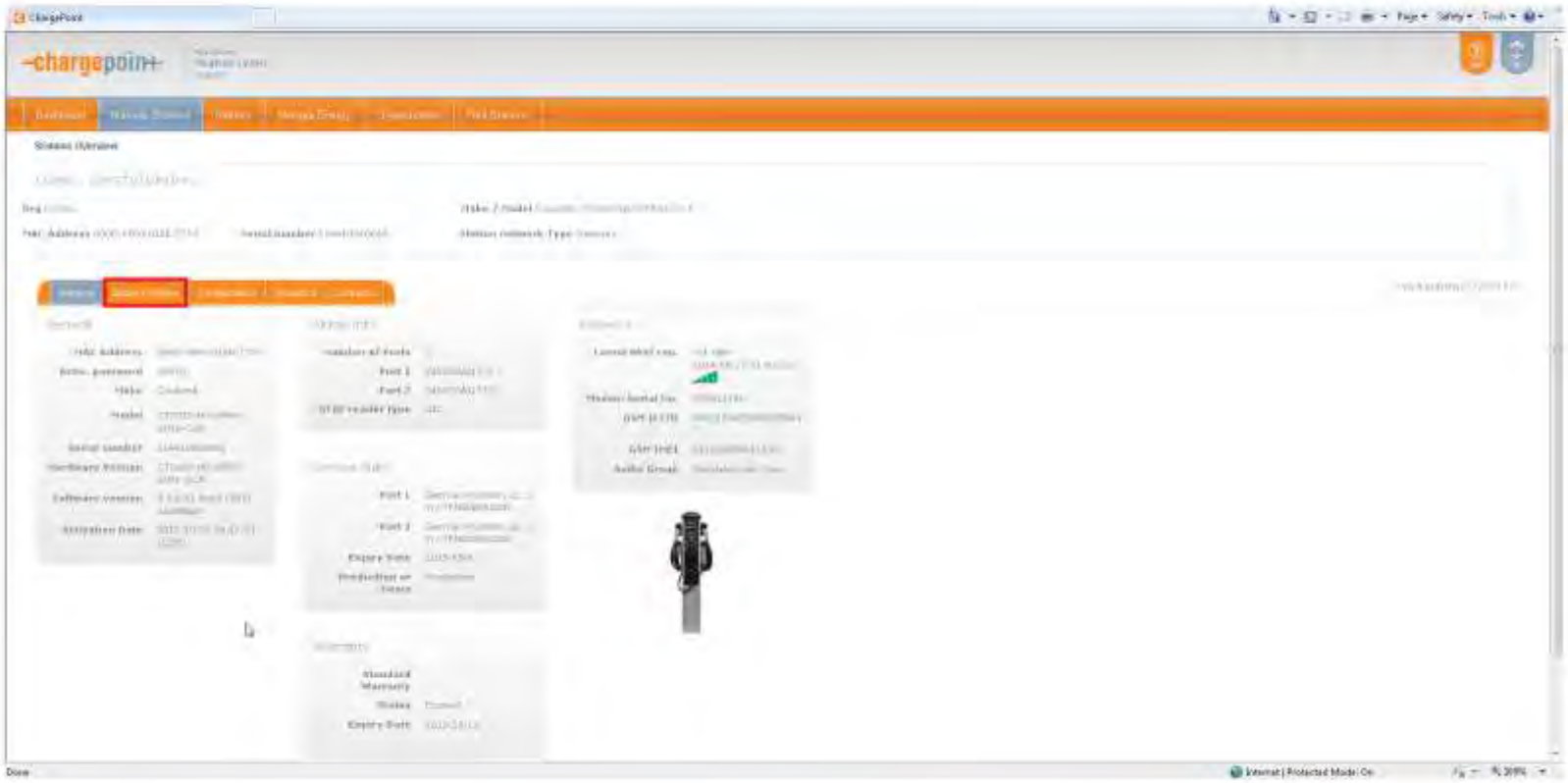
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Select the Midtown Substation Charge Station

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

KCP&L energizing life

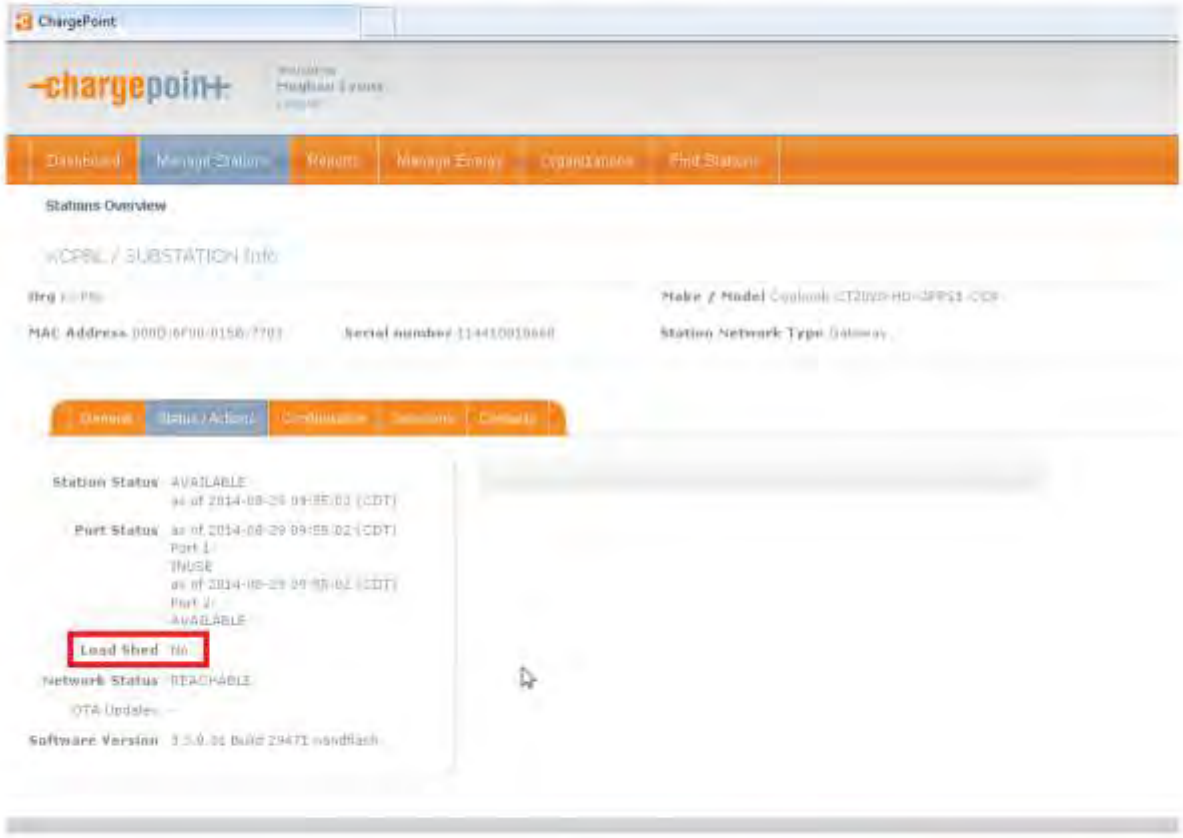
Go to the "Status/Action" Tab



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

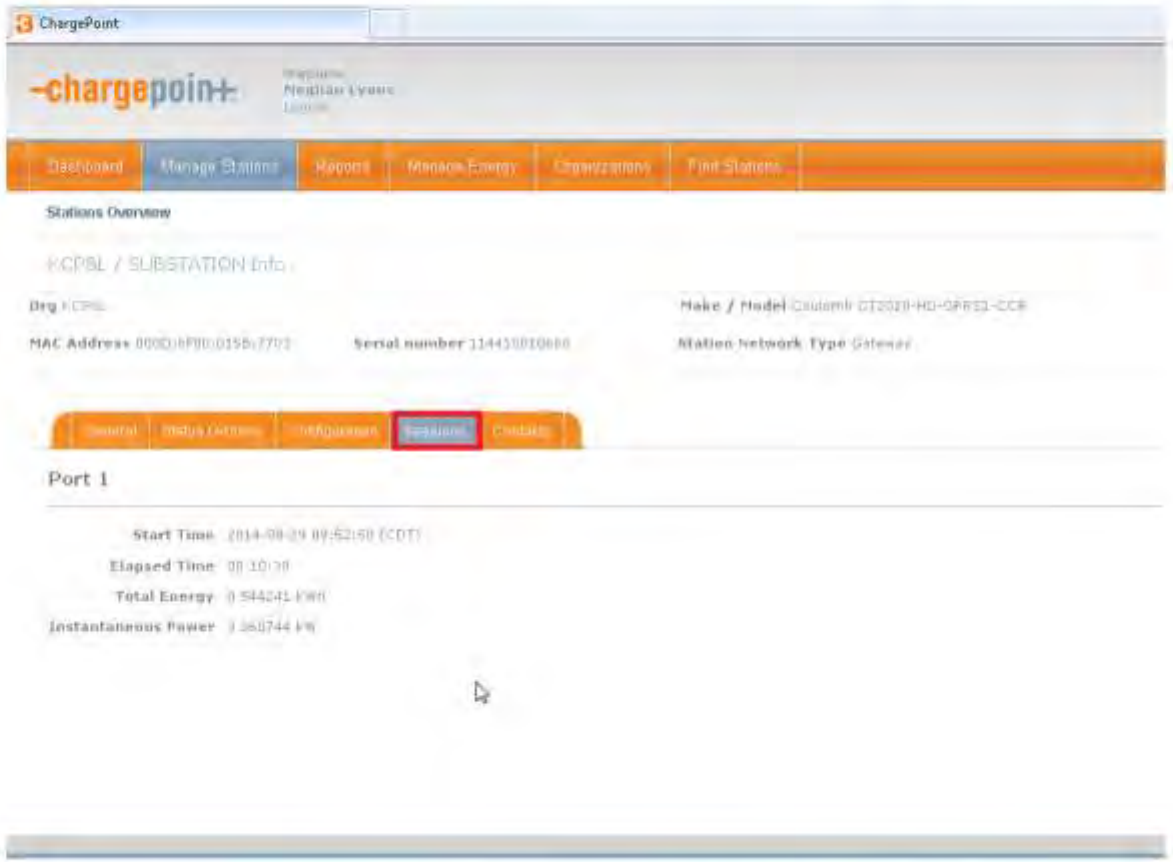
KCP&L energizing life

Load Shed = "No" Prior to DR Event



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

ChargeStation Port 1 in Use Prior to DR Event

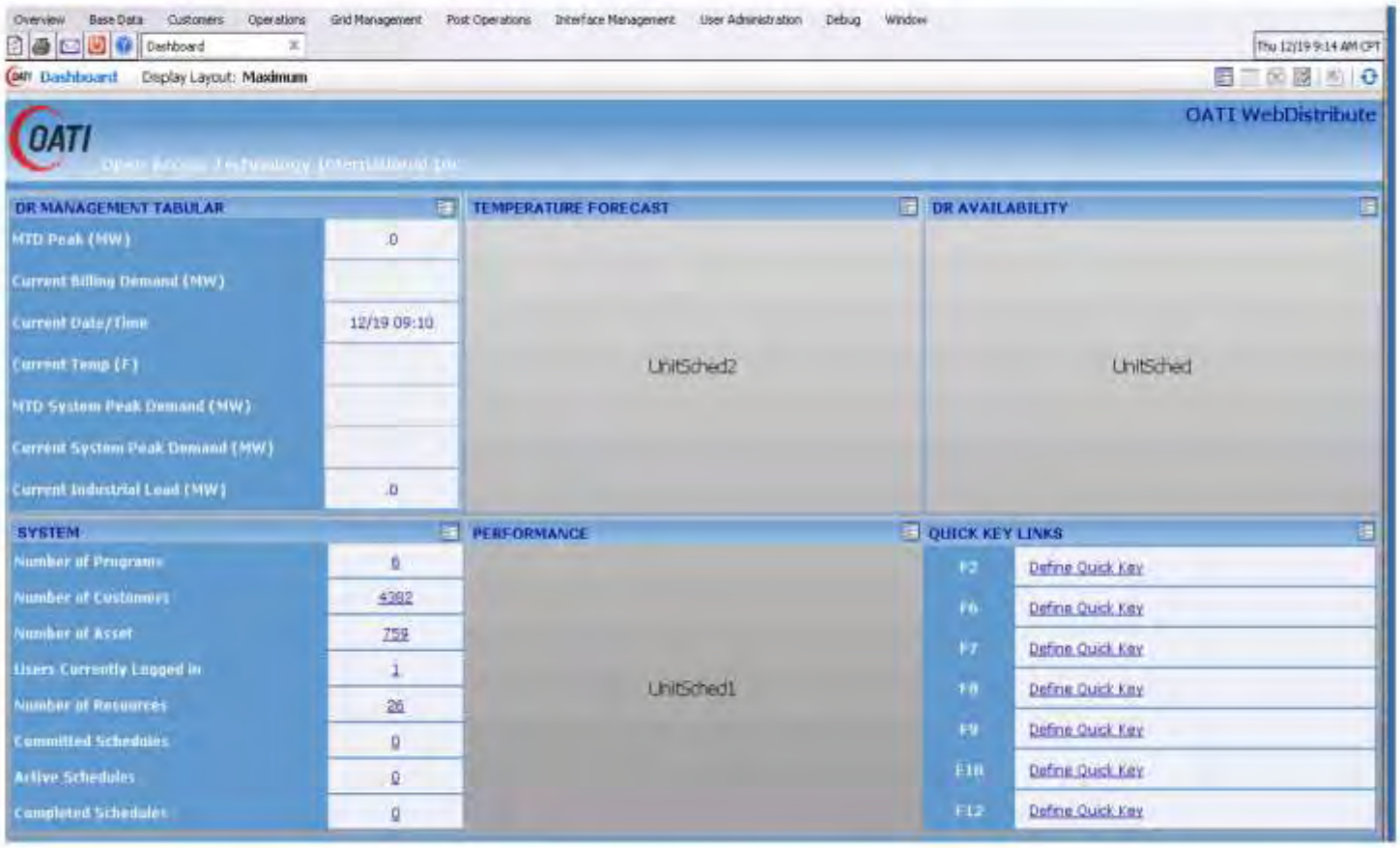


This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Launch DERM WebUI

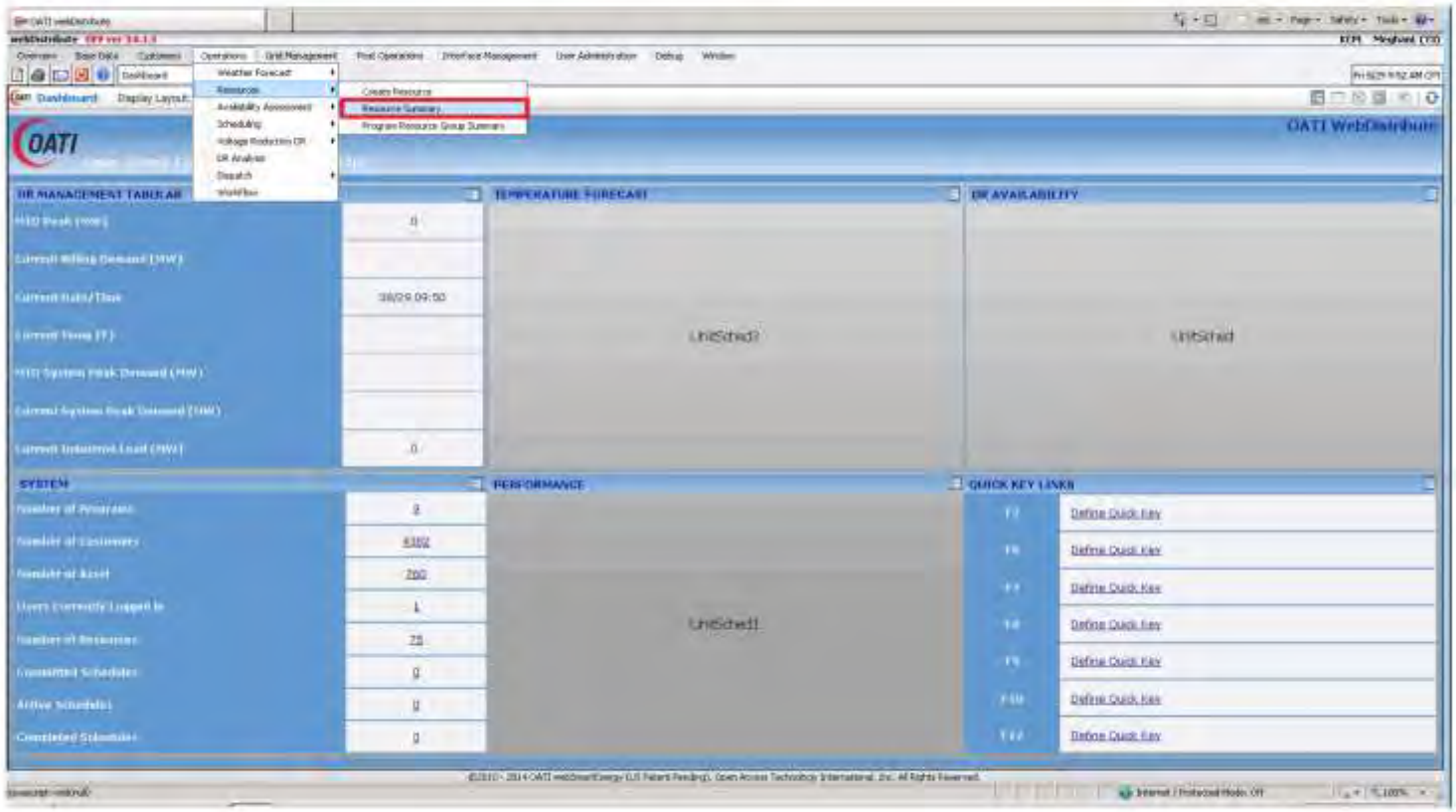
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Launch DERM WebUI



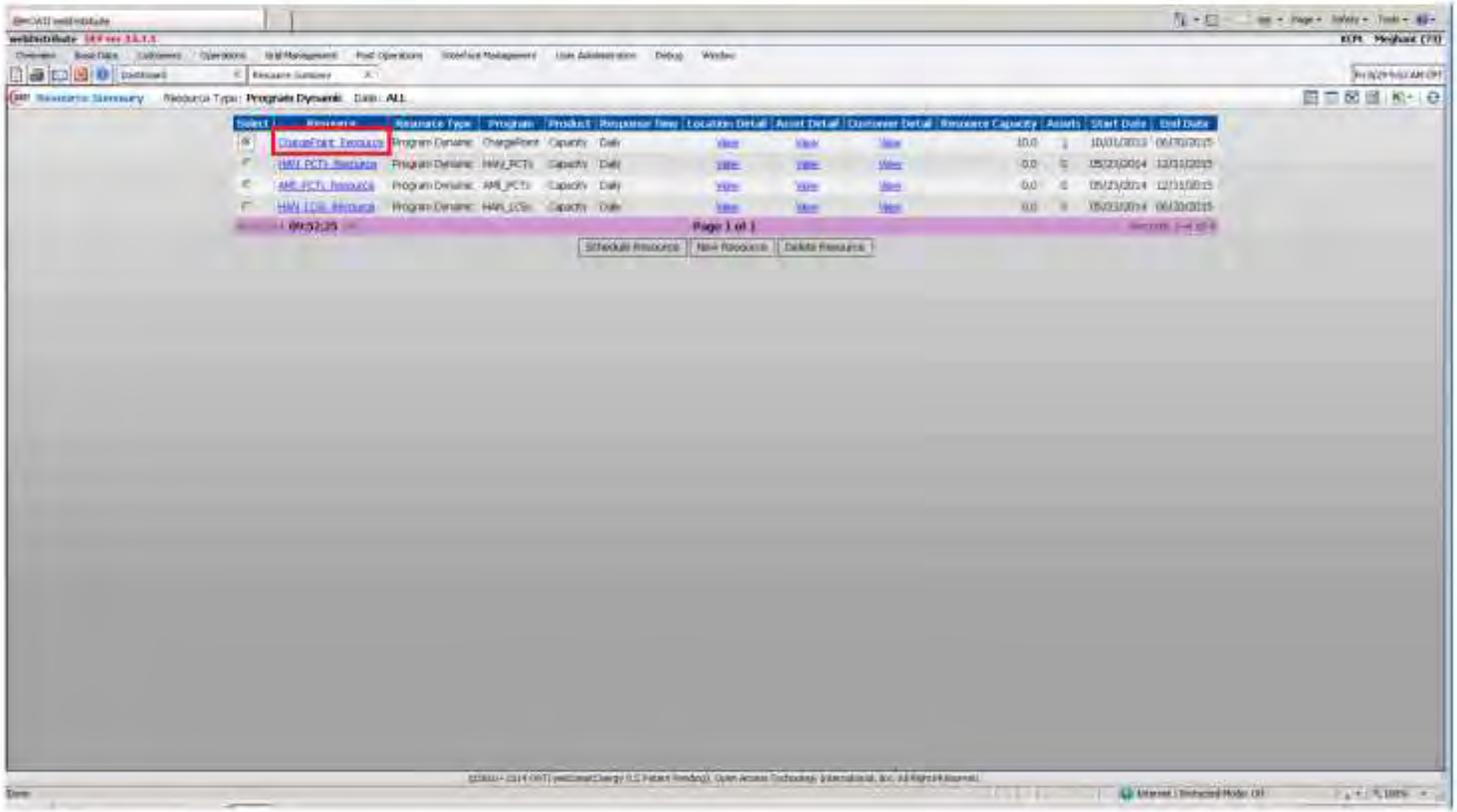
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Go to "Resource Summary"



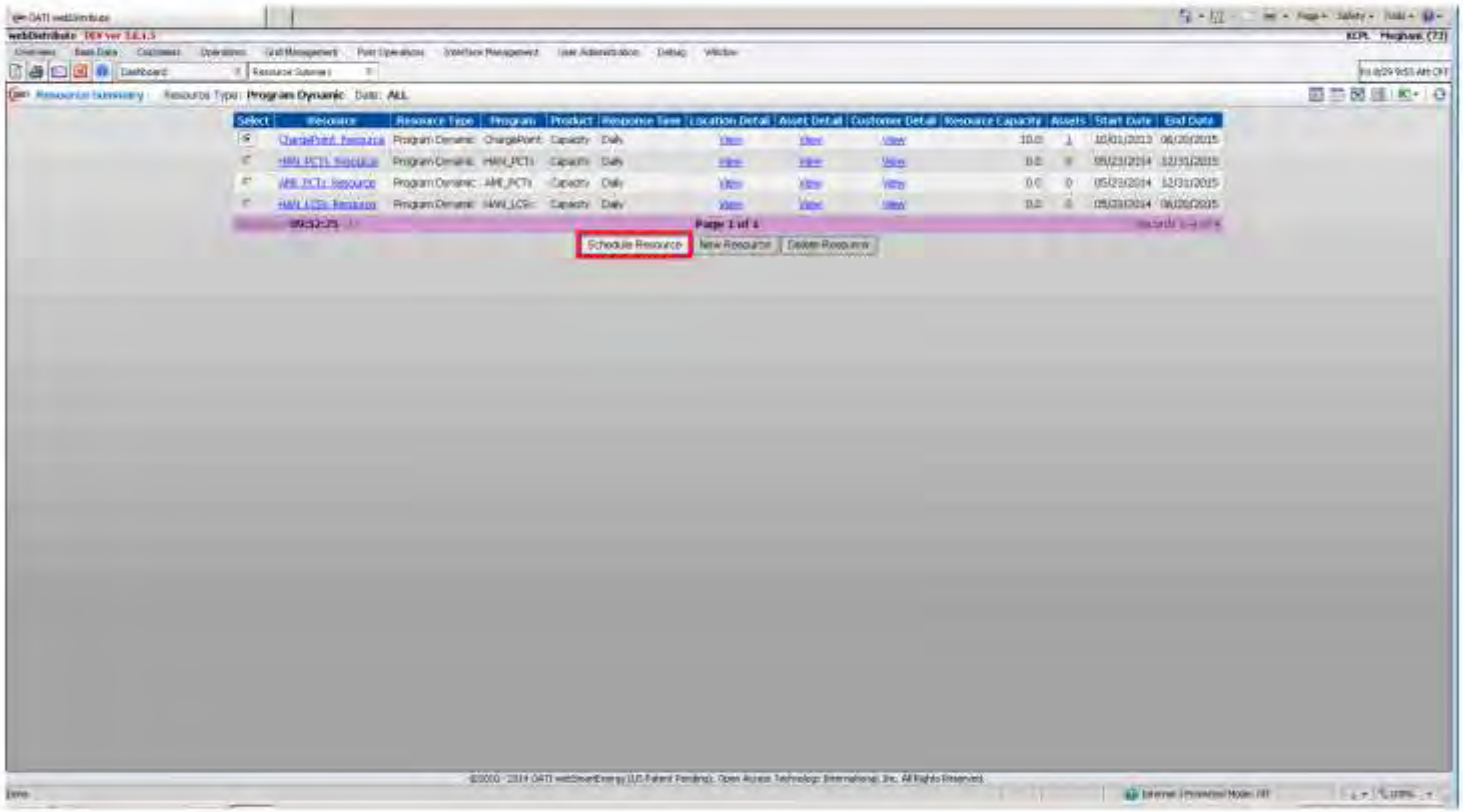
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

List of Available Resources



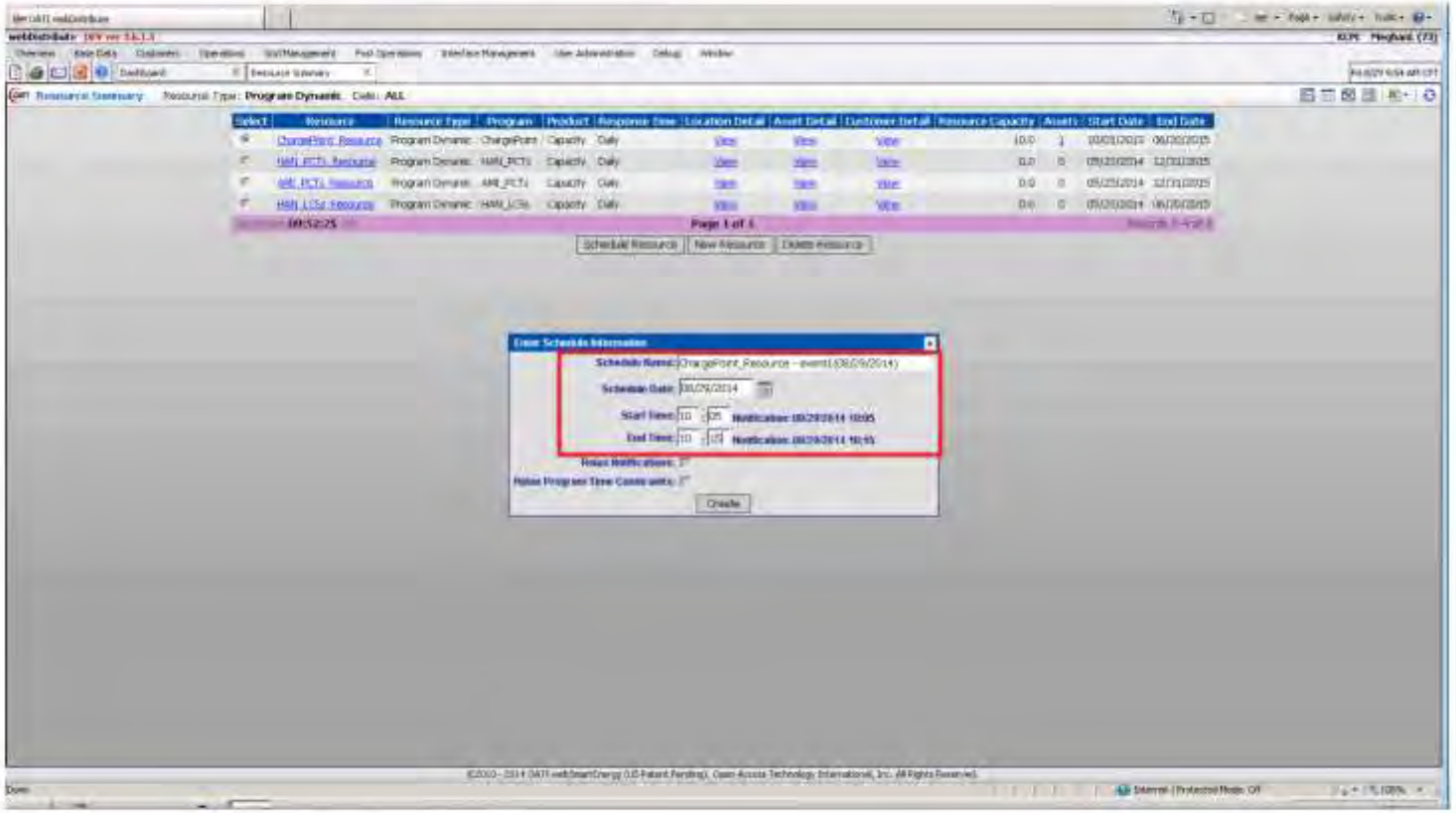
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

"Schedule Resource" to Schedule DR Event



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Enter Schedule Information

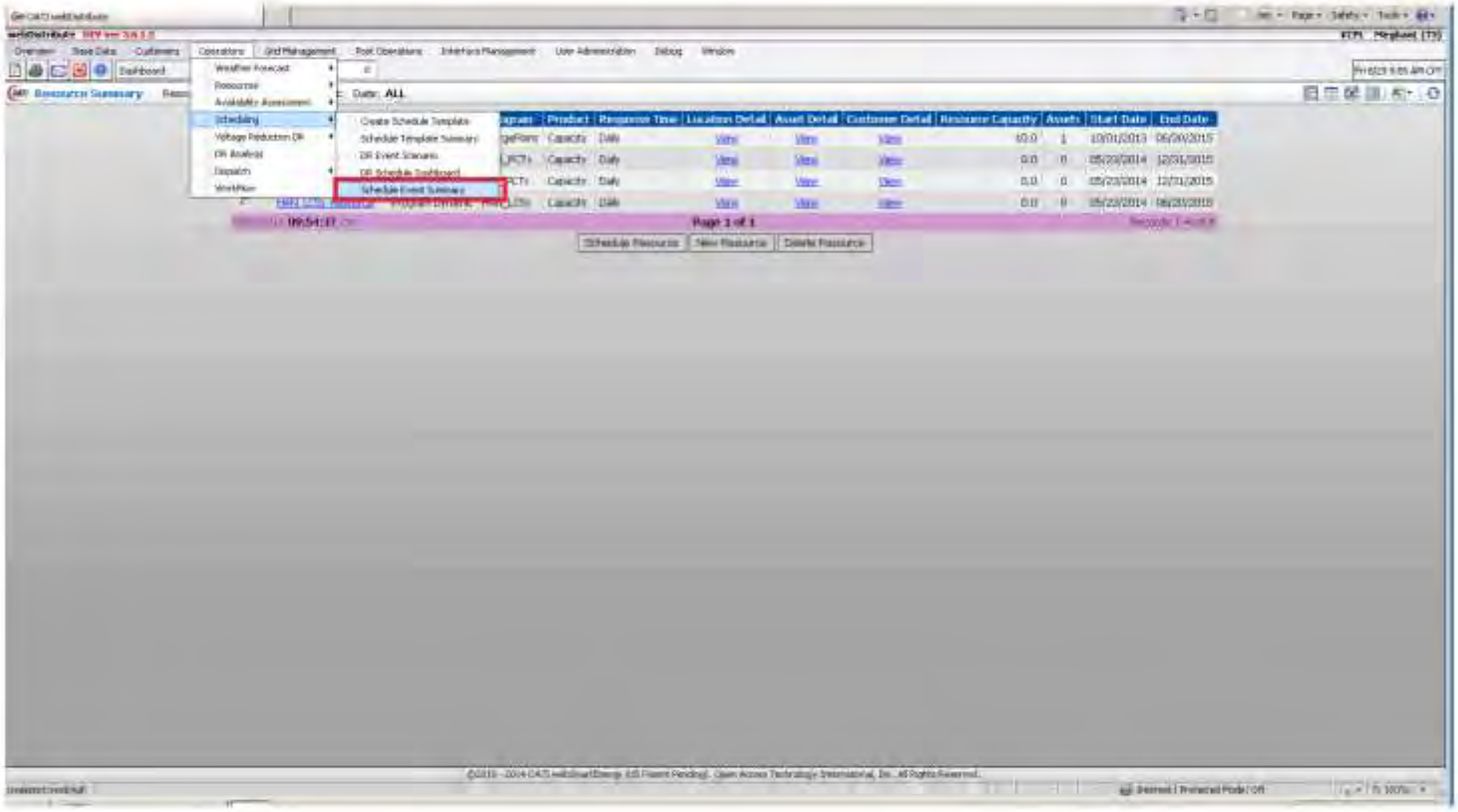


This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Event Schedule Created

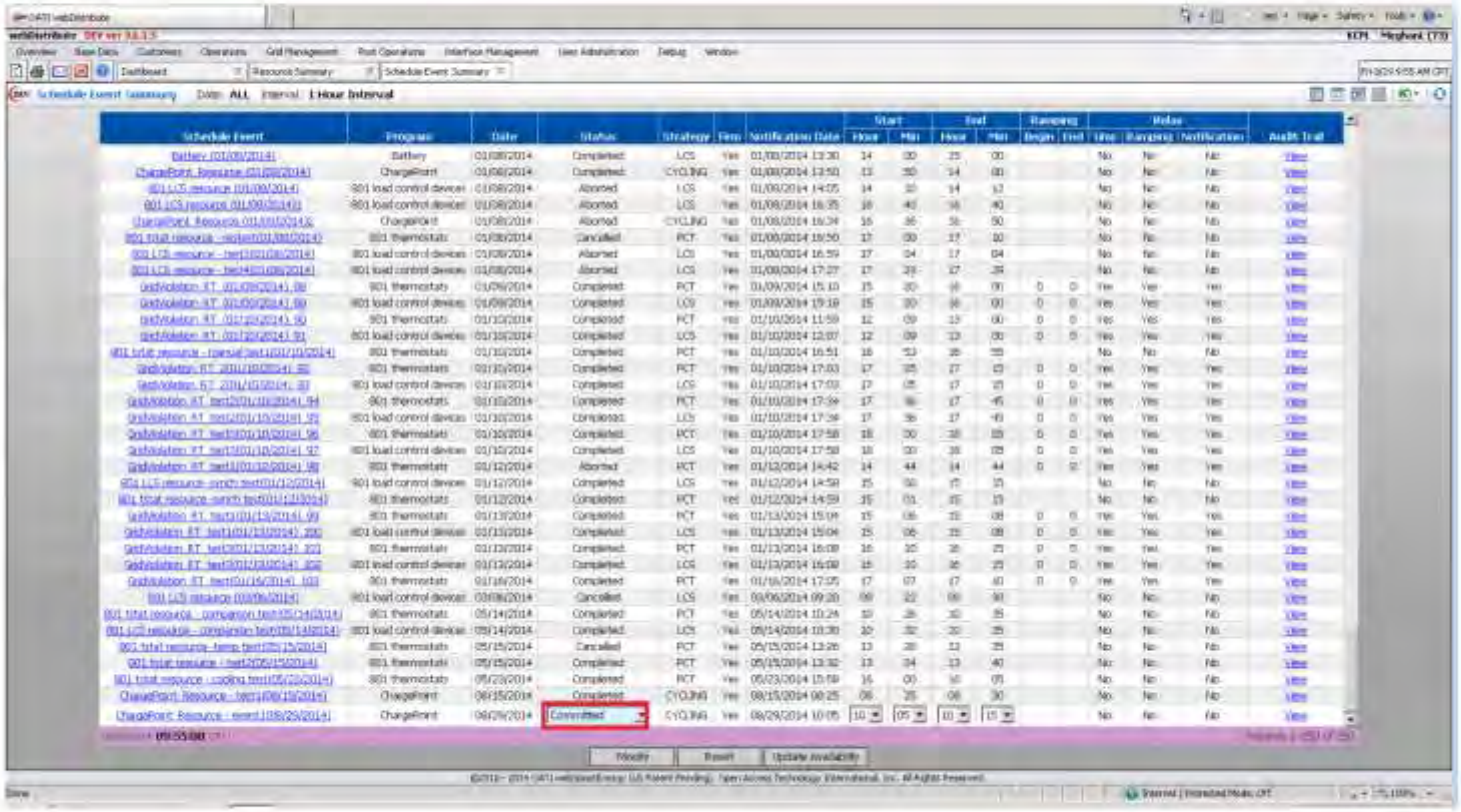
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Go to "Schedule Event Summary"



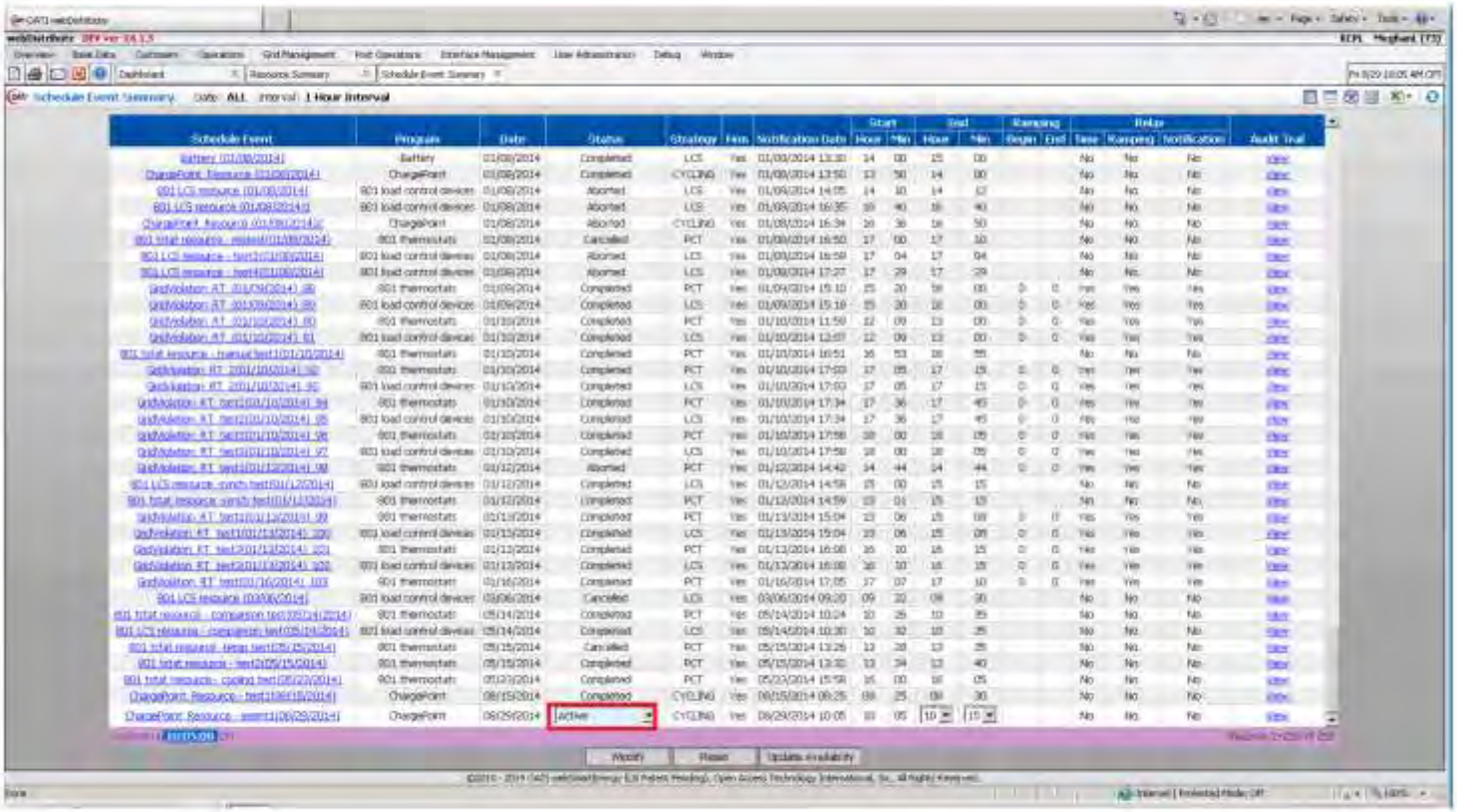
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

List of Scheduled Event Summaries

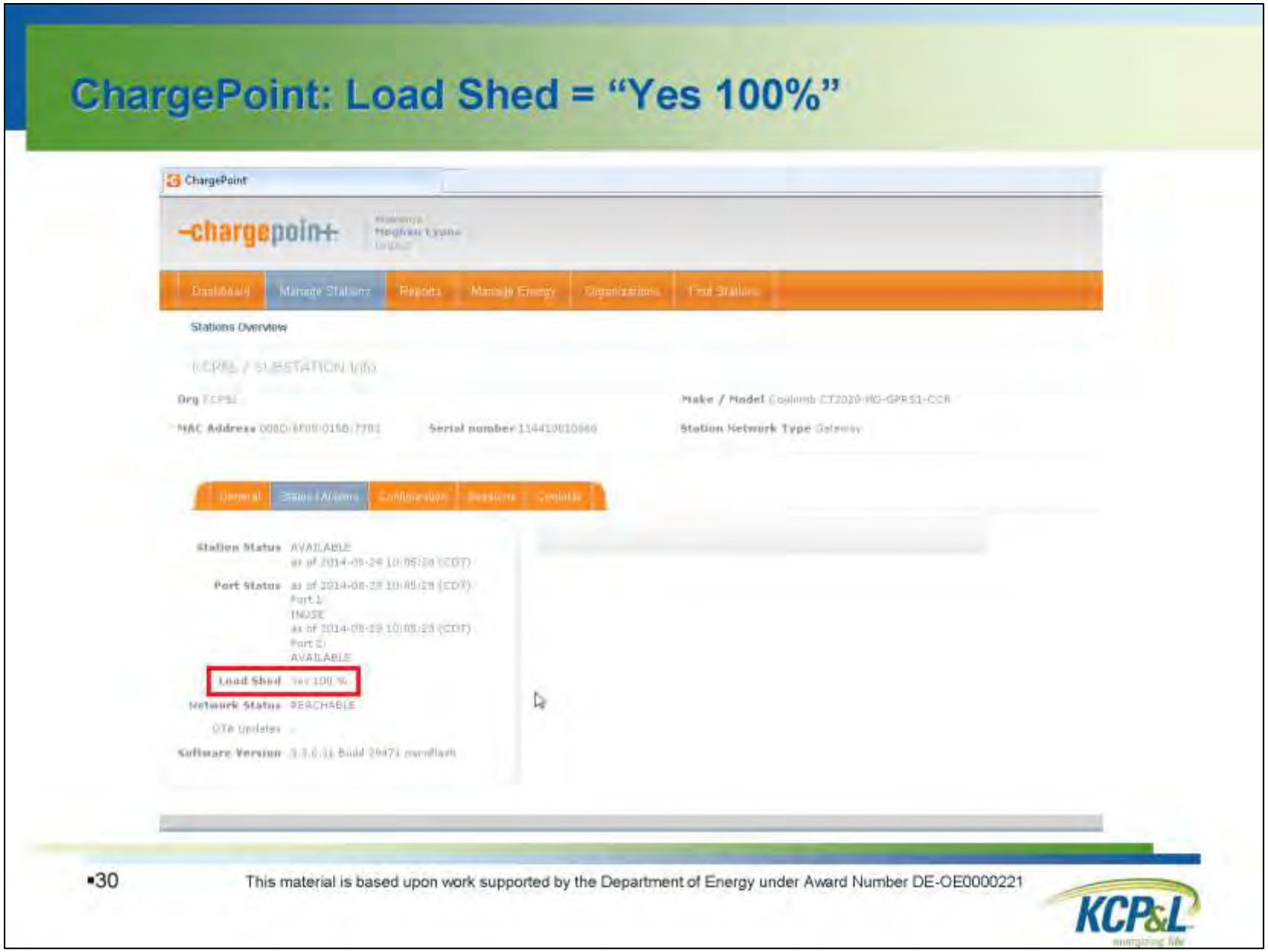


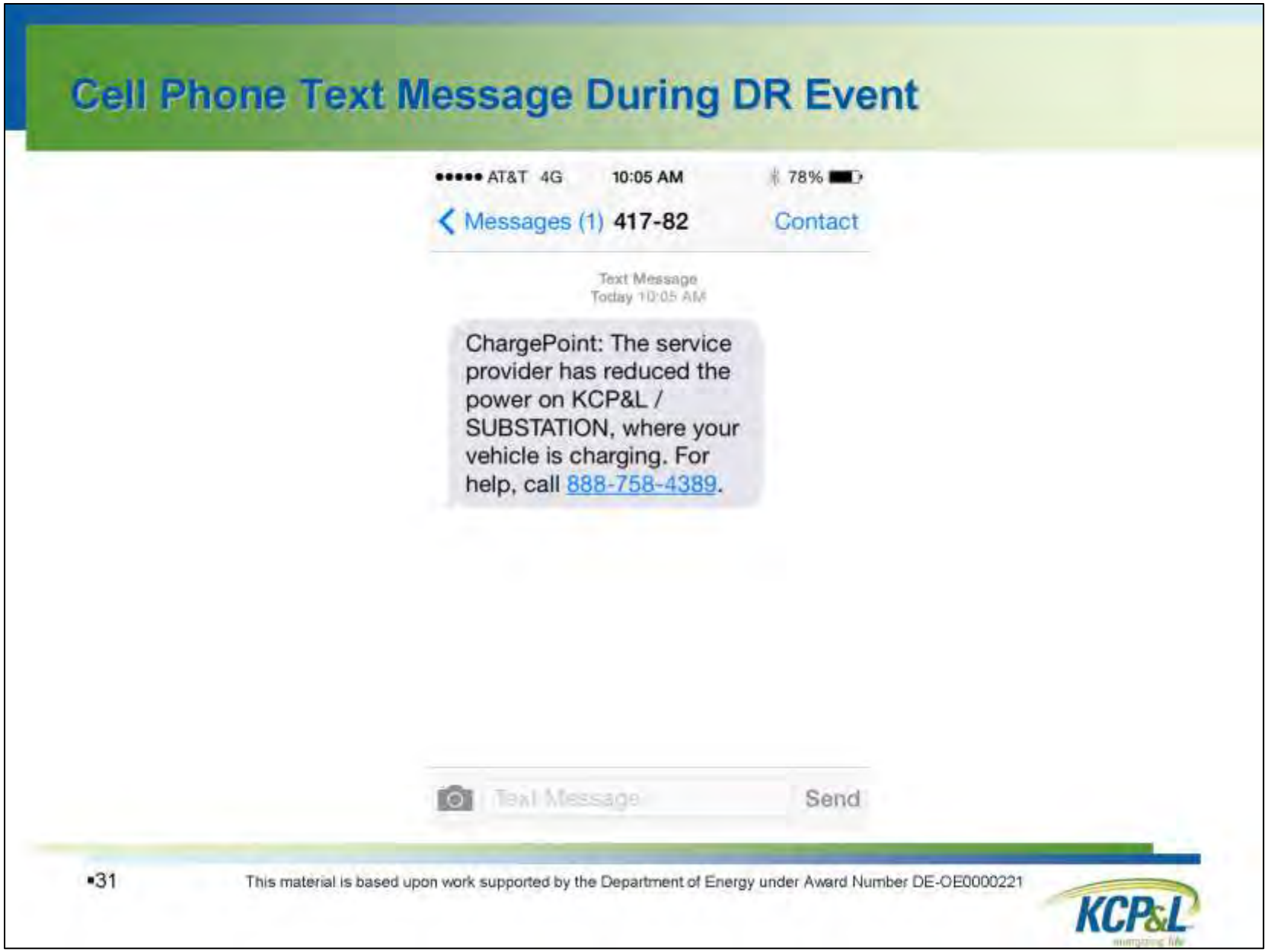
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

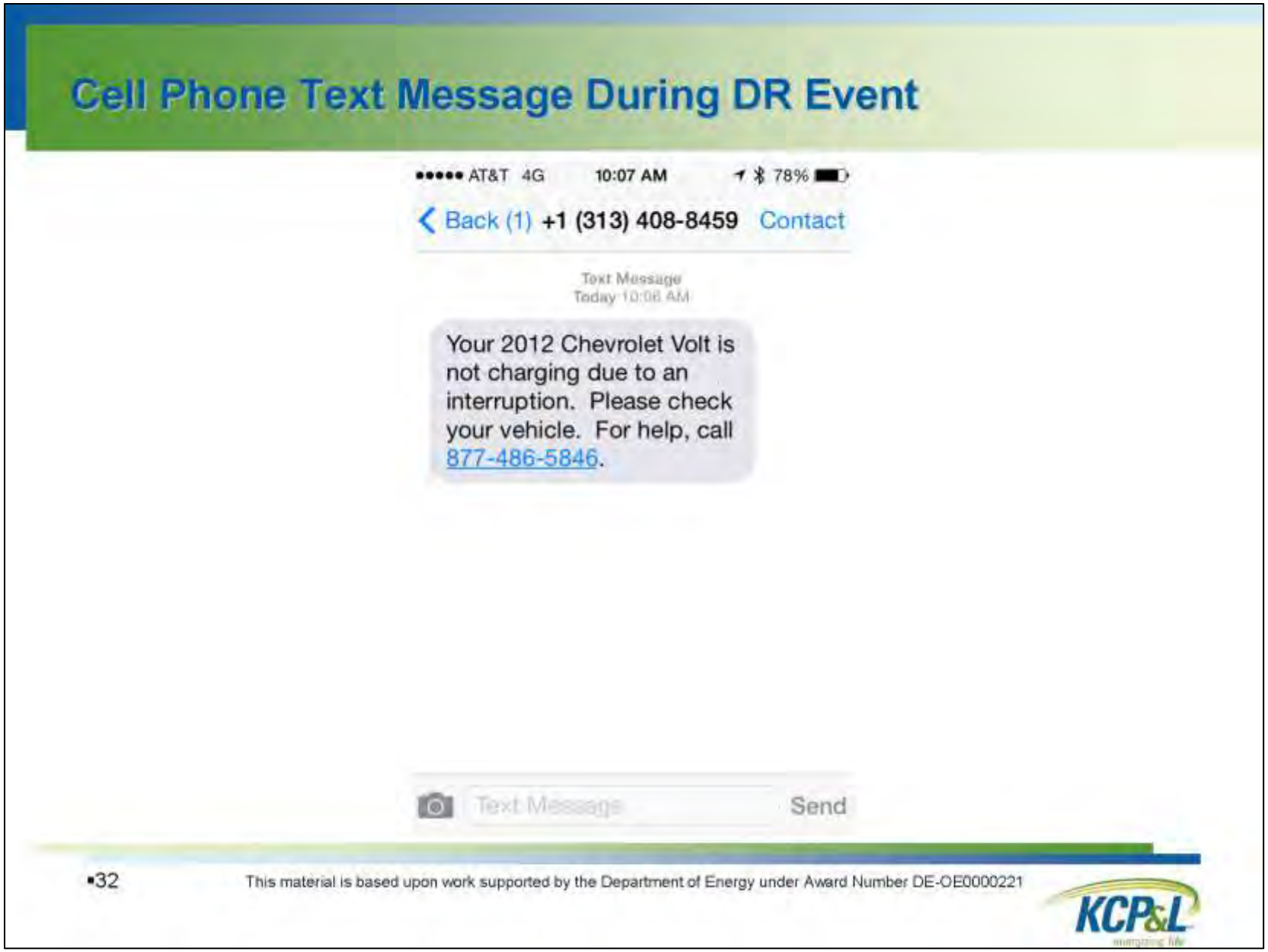
Status Change to "Active" After Event Sent from DERM



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221


ChargePoint: Load Shed = "Yes 100%"
ChargePoint
chargepoint
Dashboard
Manage Stations
Reports
Manage Energy
Organizations
Find Stations
Stations Overview
Station Status AVAILABLE
Port Status
Load Shed
Network Status REACHABLE
OTA Updates
Software Version
30
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L


Cell Phone Text Message During DR Event
AT&T 4G 10:05 AM 78%
Messages (1) 417-82 Contact
Text Message
Today 10:05 AM
ChargePoint: The service provider has reduced the power on KCP&L / SUBSTATION, where your vehicle is charging. For help, call 888-758-4389.
Text Message
Send
31
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L


Cell Phone Text Message During DR Event
AT&T 4G 10:07 AM 78%
Back (1) +1 (313) 408-8459 Contact
Text Message
Today 10:06 AM
Your 2012 Chevrolet Volt is not charging due to an interruption. Please check your vehicle. For help, call 877-486-5846.
Text Message
Send
32
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

EV Dashboard: During DR Event

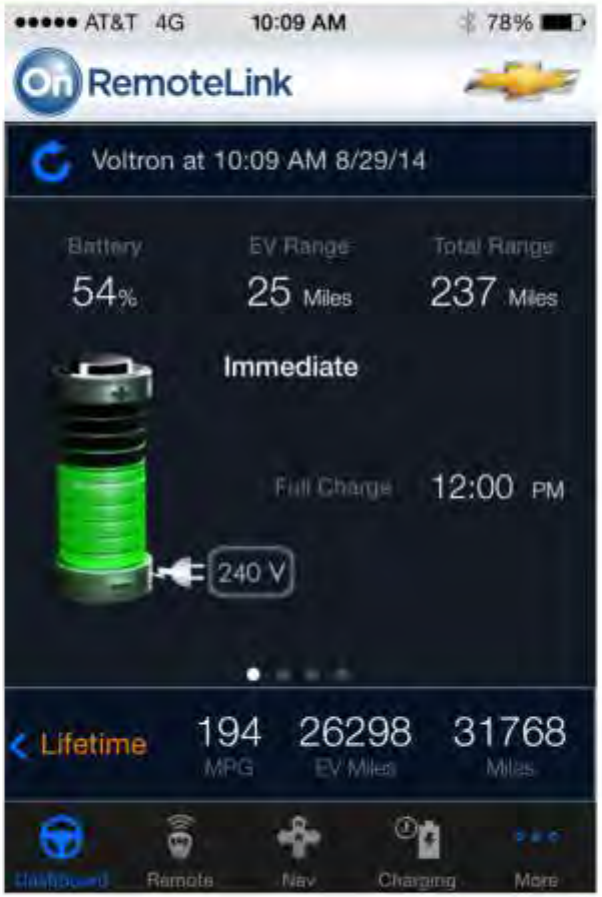
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

KCP&L energizing life

EV Dashboard: During DR Event

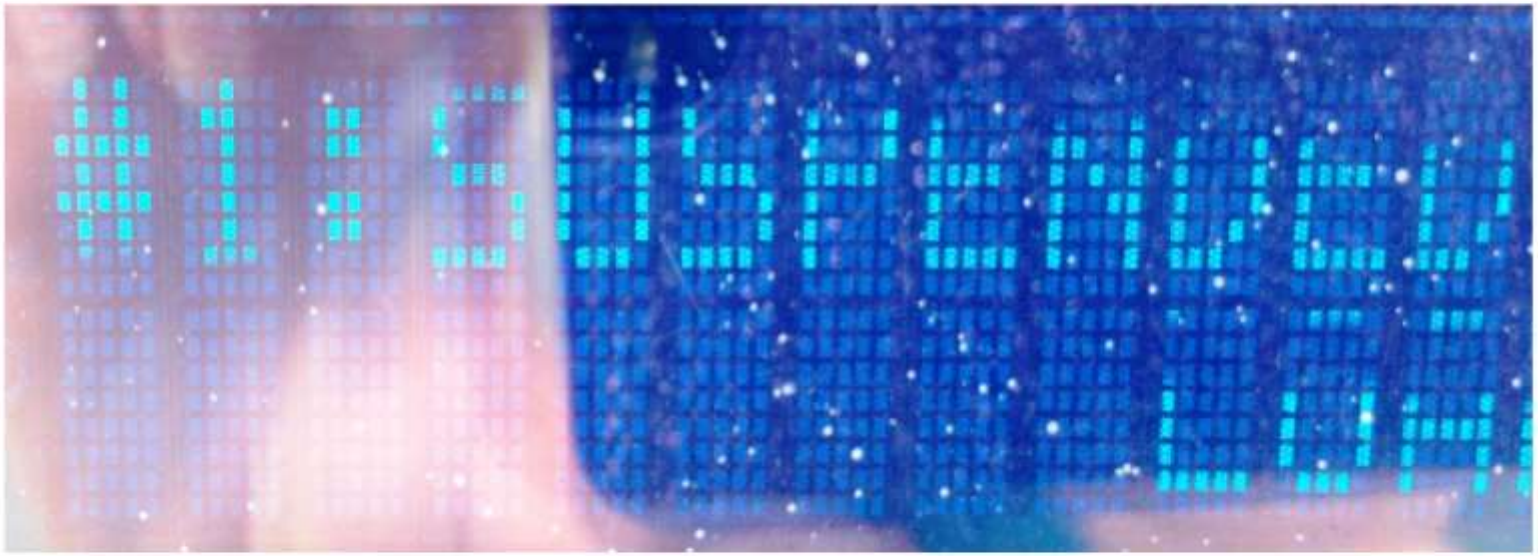
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Cell Phone App: During DR Event



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

EVCS Display: EV Plugged in During DR Event

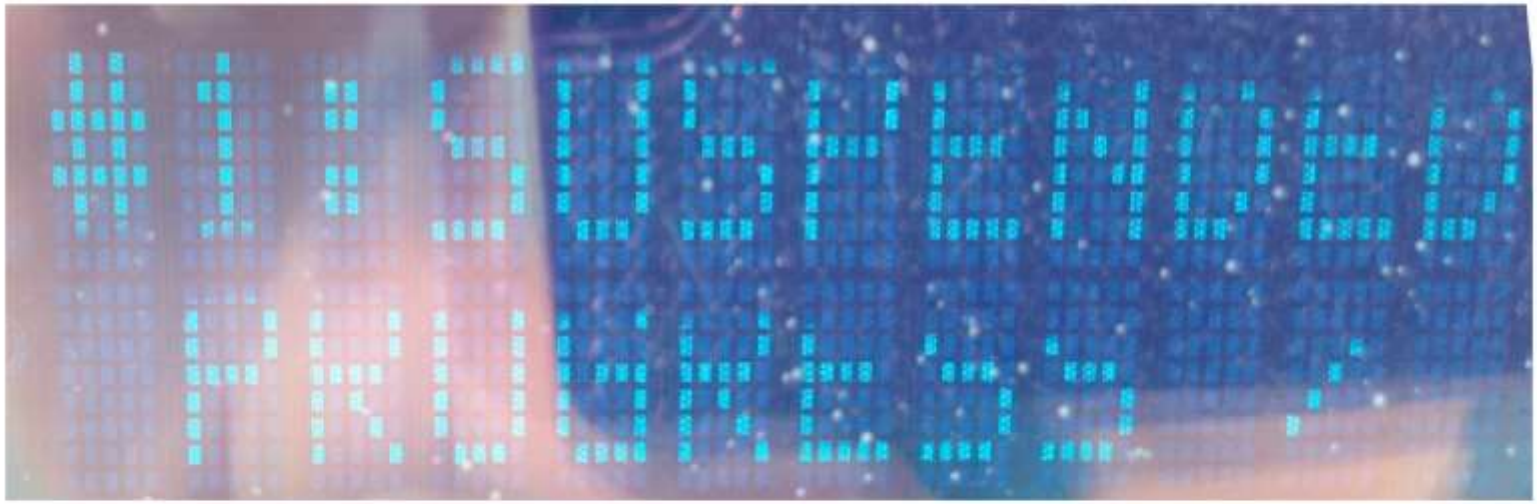


This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

EVCS Display: EV Plugged in During DR Event

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

EVCS Display: EV Plugged in During DR Event



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

EVCS Display: EV Plugged in During DR Event

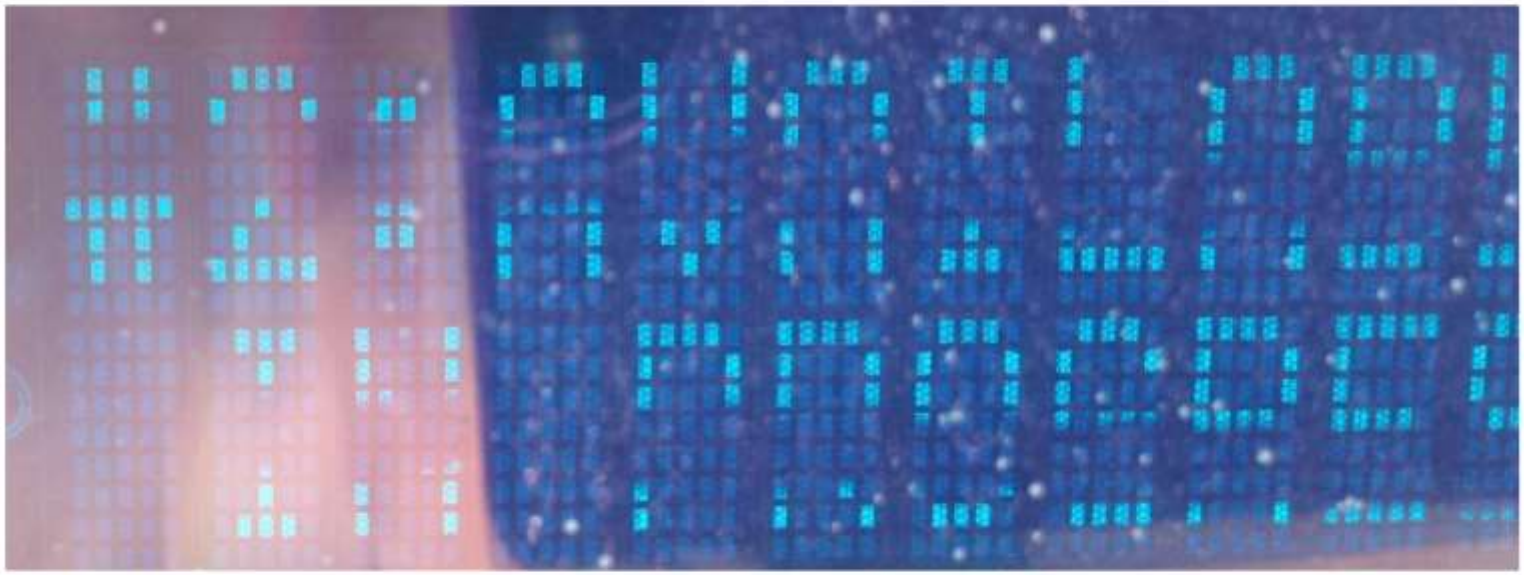
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

KCP&L energizing life

EVCS Display: EV Plugged in During DR Event

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

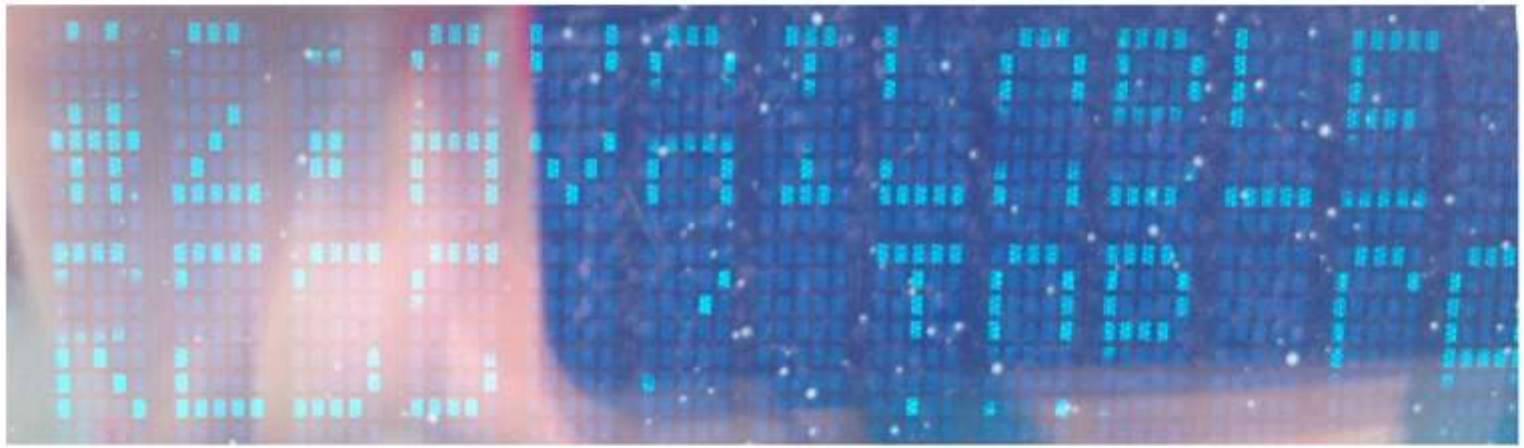
EVCS Display: EV Plugged in During DR Event



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

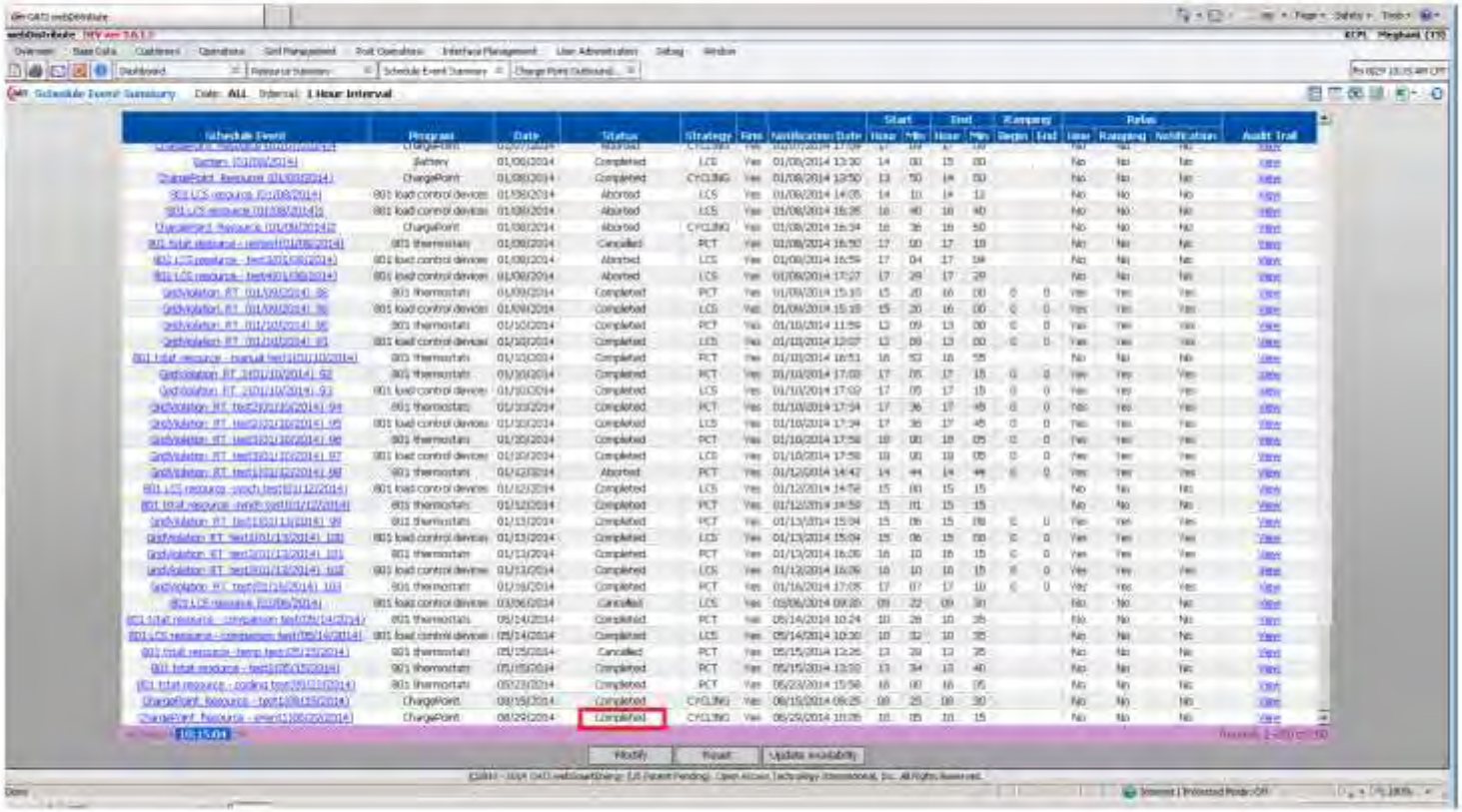
KCP&L energizing life

EVCS Display: EV Plugged in During DR Event



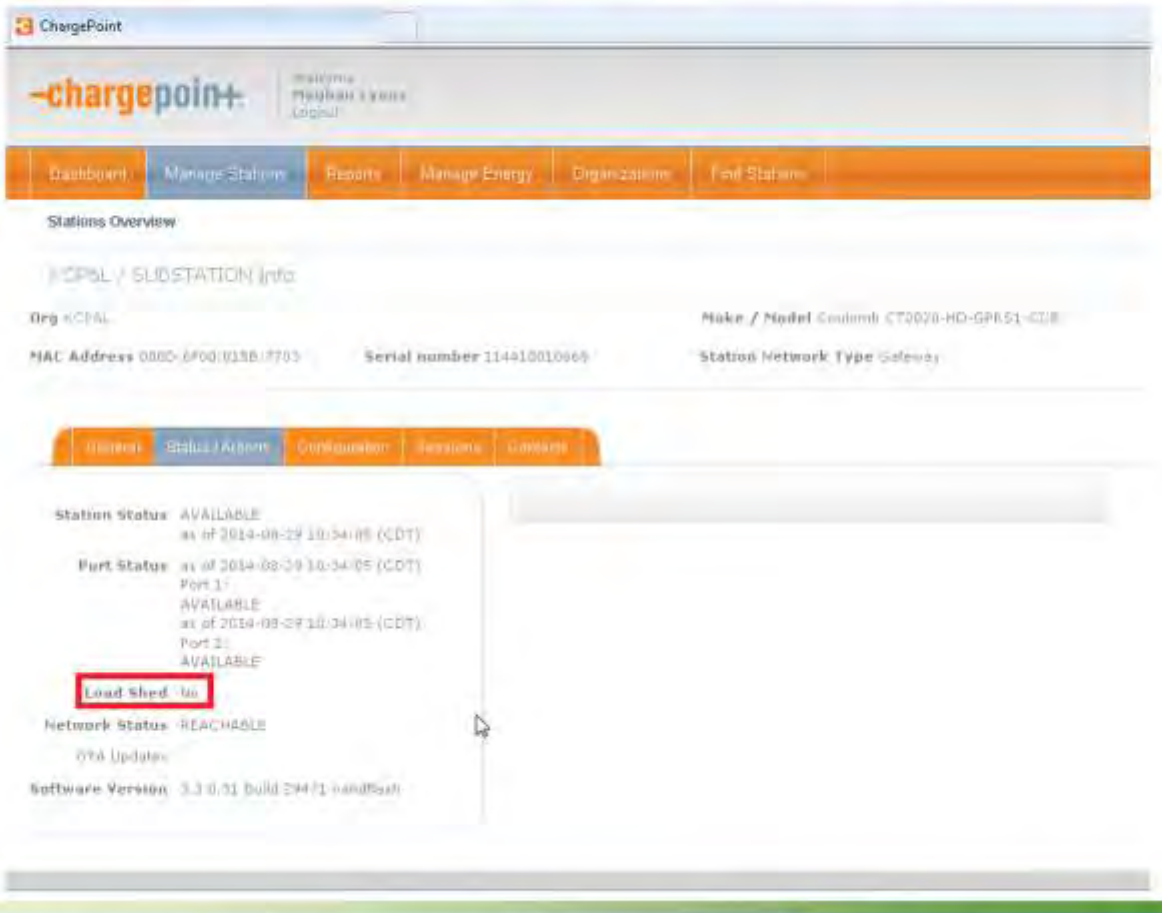
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

DERM: Event Complete

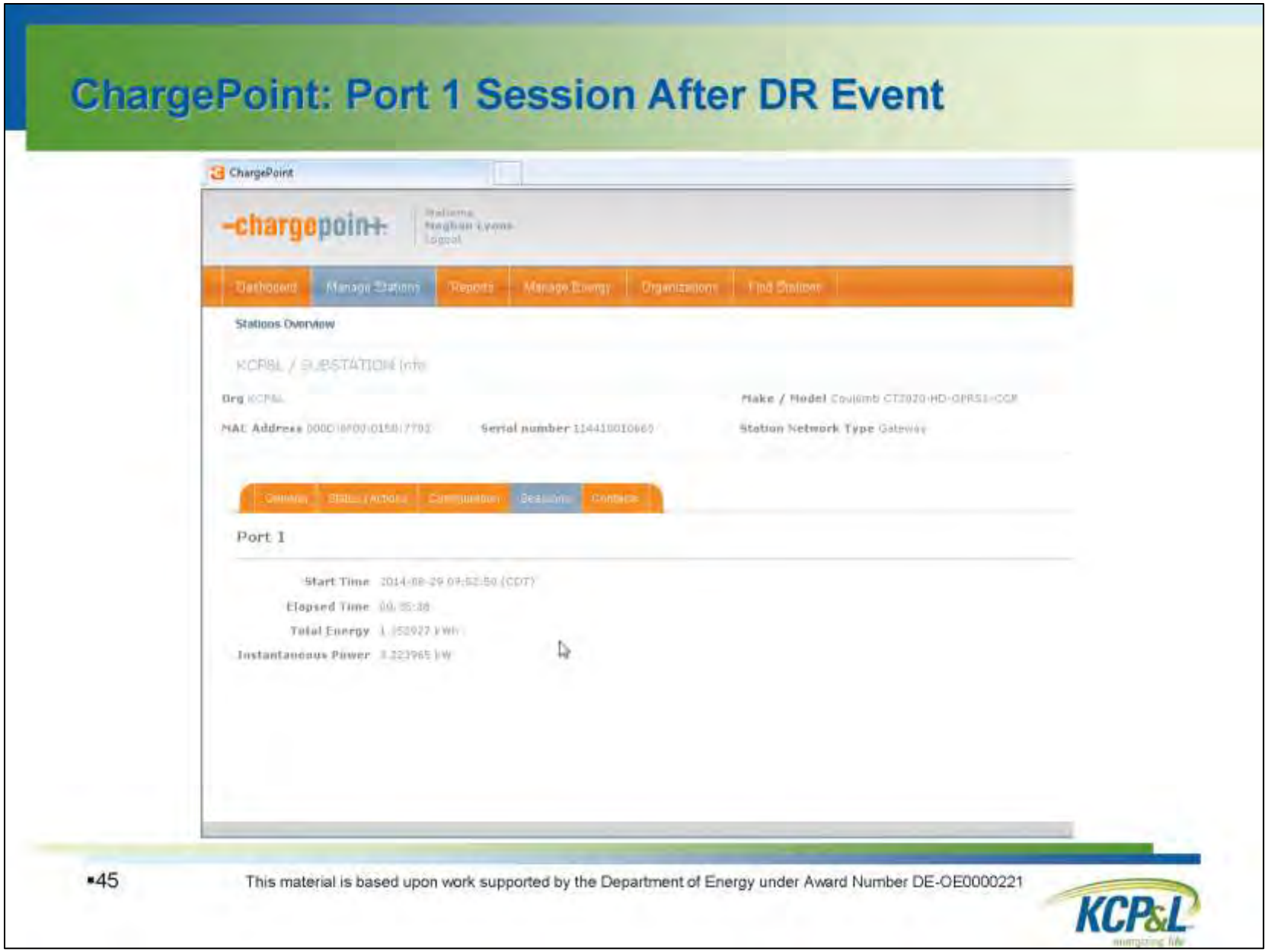


This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

ChargePoint: Load Shed = "No" at Event Completion



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221


ChargePoint: Port 1 Session After DR Event
ChargePoint
chargepoint
Dashboard
Manage Stations
Reports
Manage Energy
Organizations
Find Stations
Stations Overview
Org
Make / Model
MAC Address
Serial number
Station Network Type
Port 1
Start Time
Elapsed Time
Total Energy
Instantaneous Power
45
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

EV Dashboard: Post DR Event

▪46

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

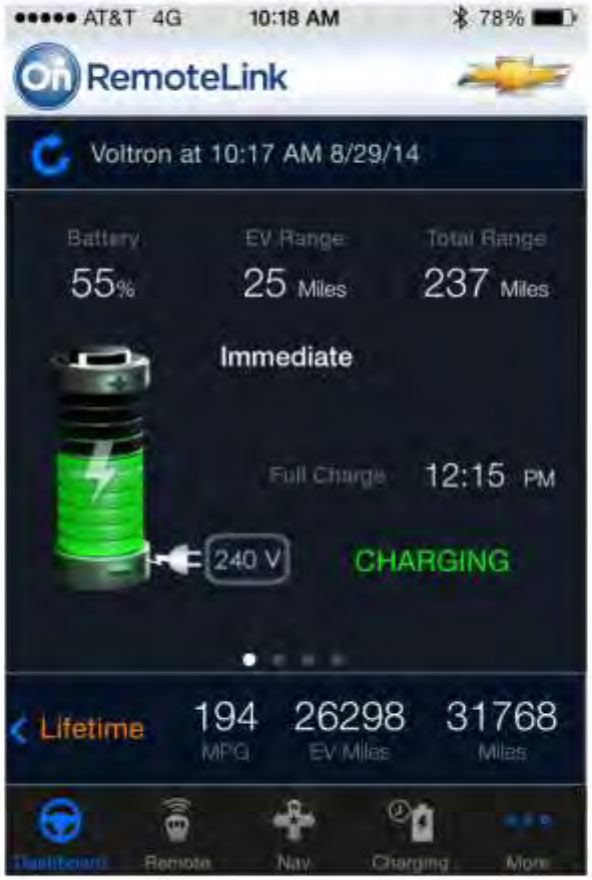
KCP&L energizing life

EV Dashboard: Post DR Event

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

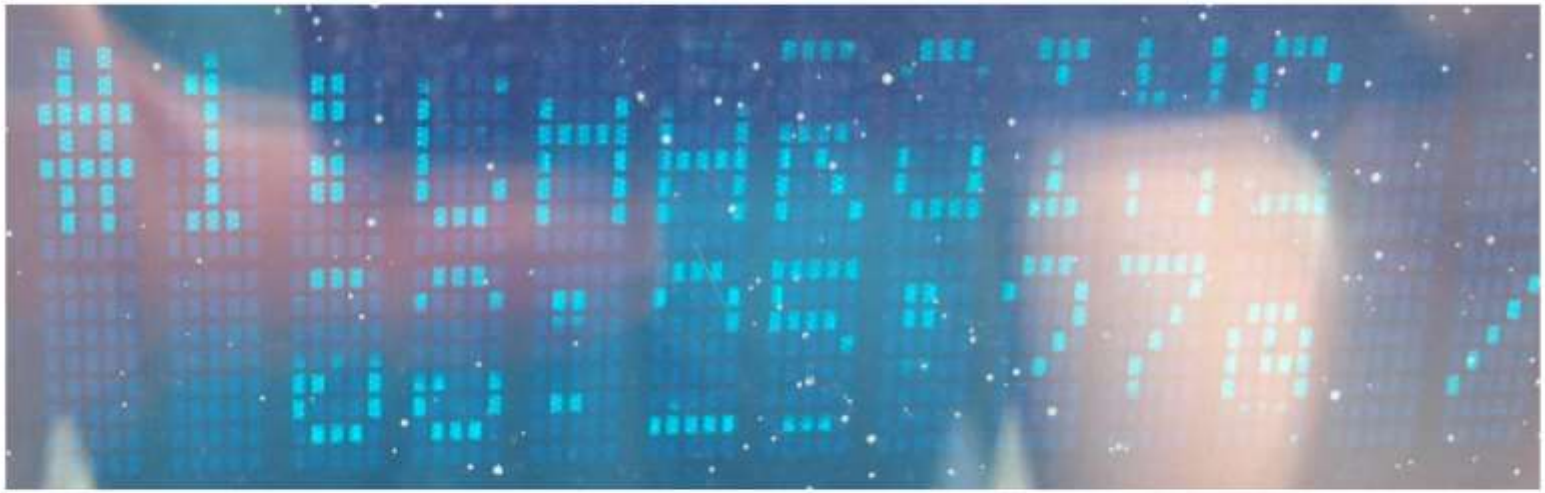
KCP&L energizing life

Cell Phone App: Post DR Event



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

EVCS Display: EV Plugged in Post DR Event



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

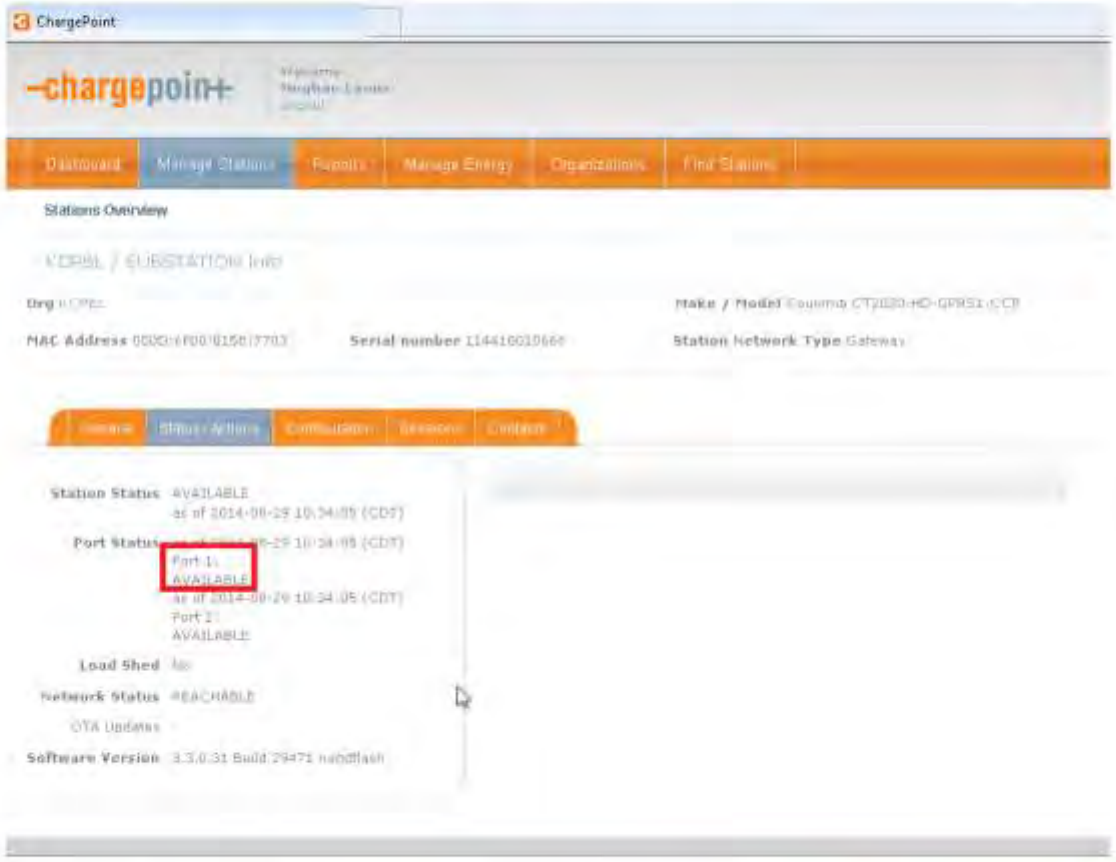
EVCS Display: EV Plugged in Post DR Event

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

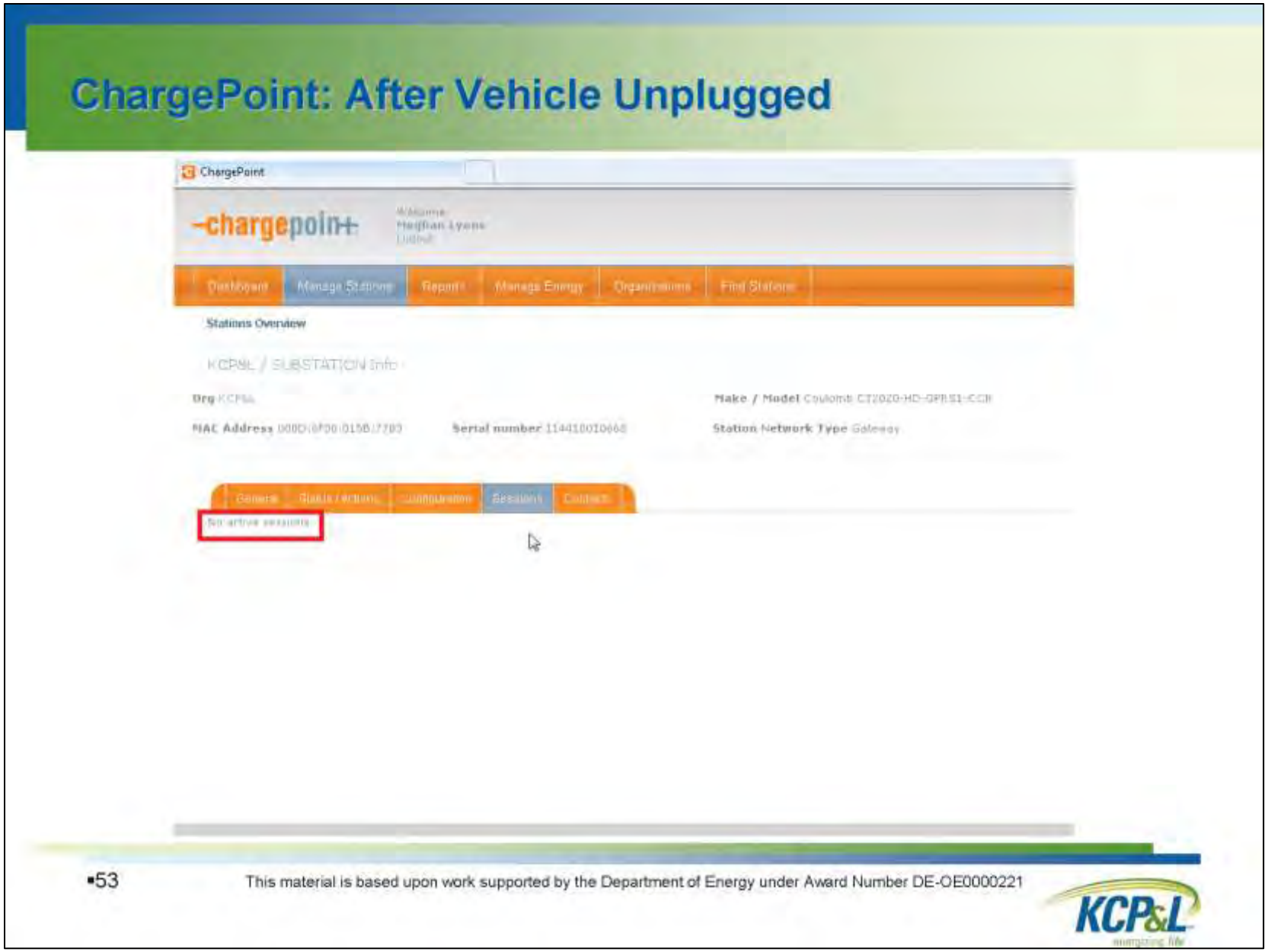
EVCS Display: EV Plugged in Post DR Event

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

ChargePoint: After Vehicle Unplugged

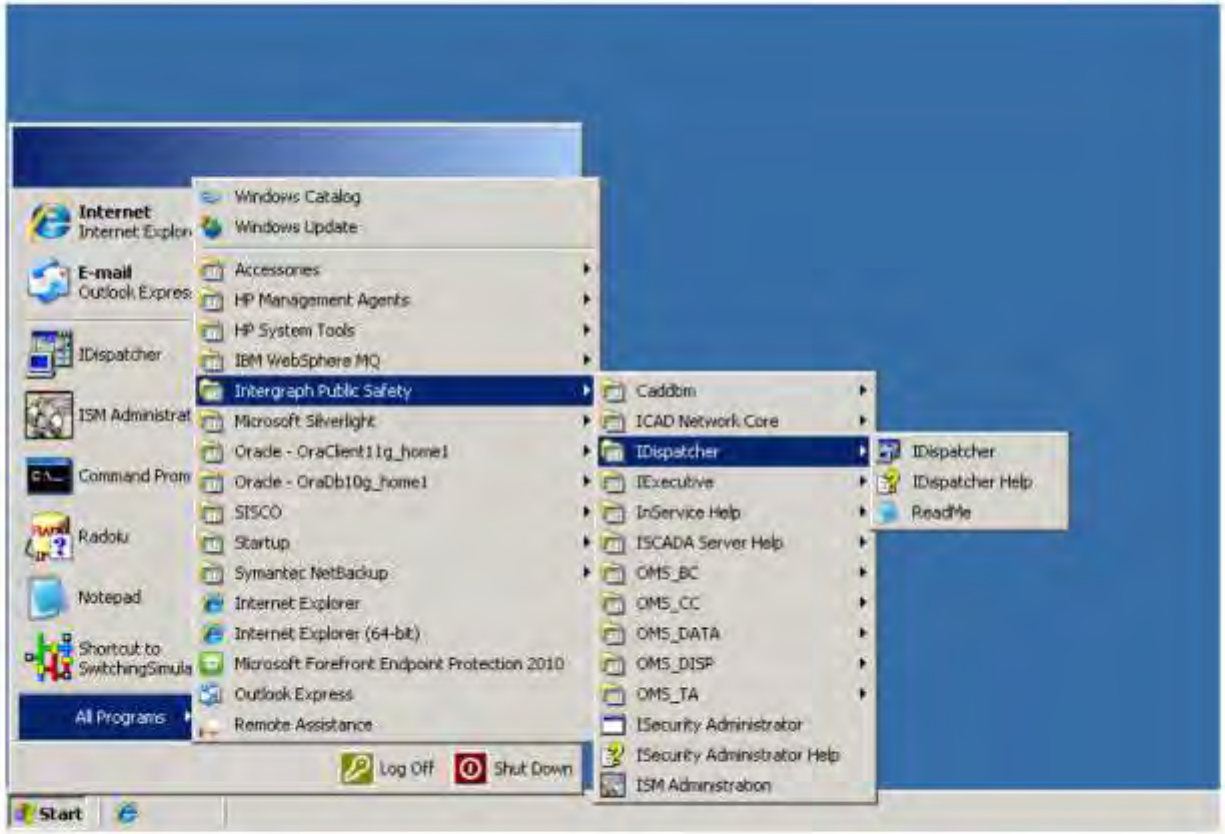


This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221


ChargePoint: After Vehicle Unplugged
ChargePoint
chargepoint
Dashboard
Manage Stations
Reports
Manage Energy
Organizations
Find Stations
Stations Overview
KCP&L / SUBSTATION Info
Org KCP&L
Make / Model
NAC Address
Serial number
Station Network Type
General
Status / Actions
Configuration
Sessions
Content
No active sessions
53
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L


1st Responder Volt Var Control
- KC Green Impact Zone Initiative
- DOE Regional SmartGrid Demonstration Program
- EPRI SmartGrid Demonstration Program
KCP&L
SmartGrid
the future of energy

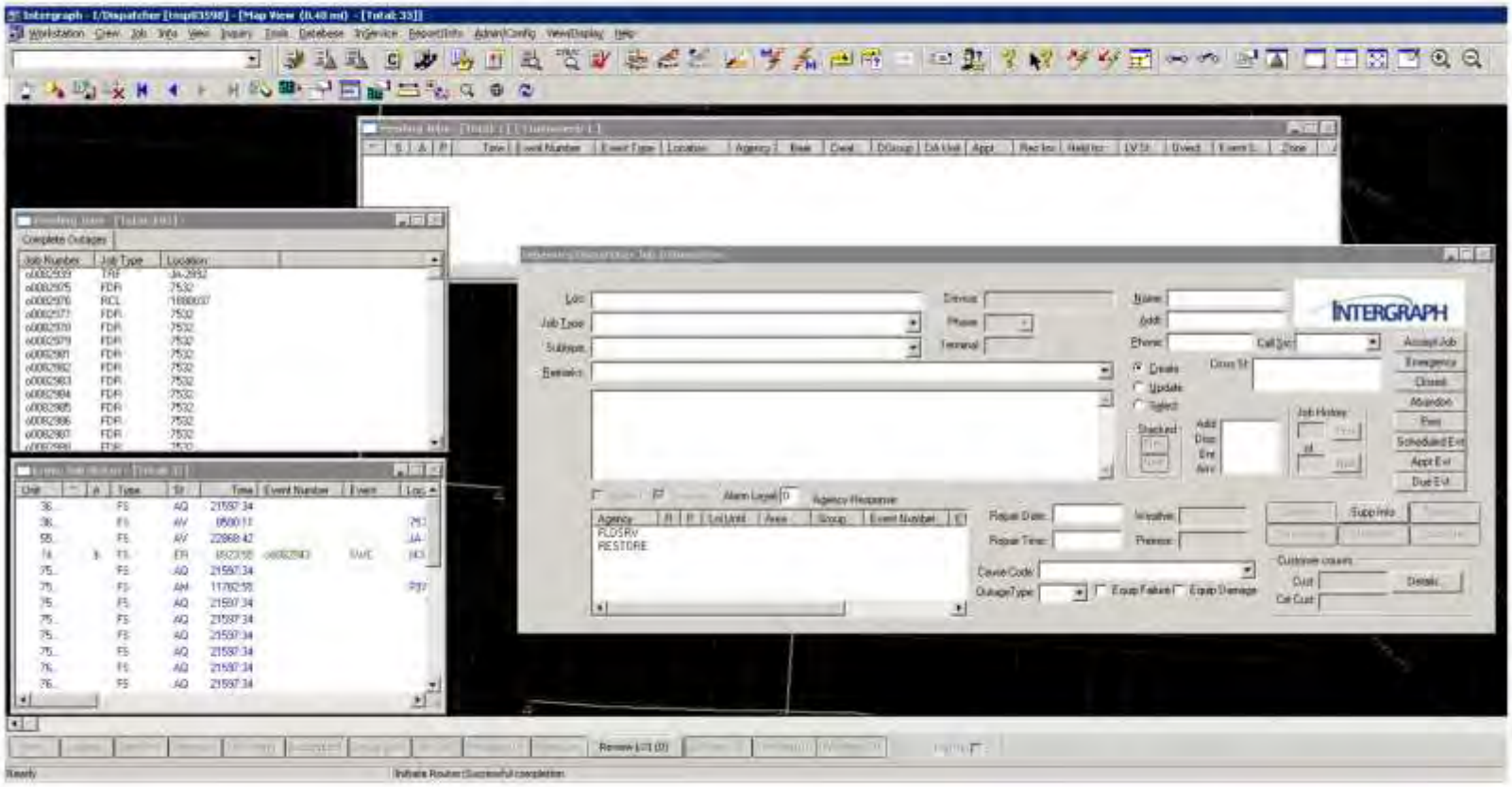
Launch InService I/Dispatcher



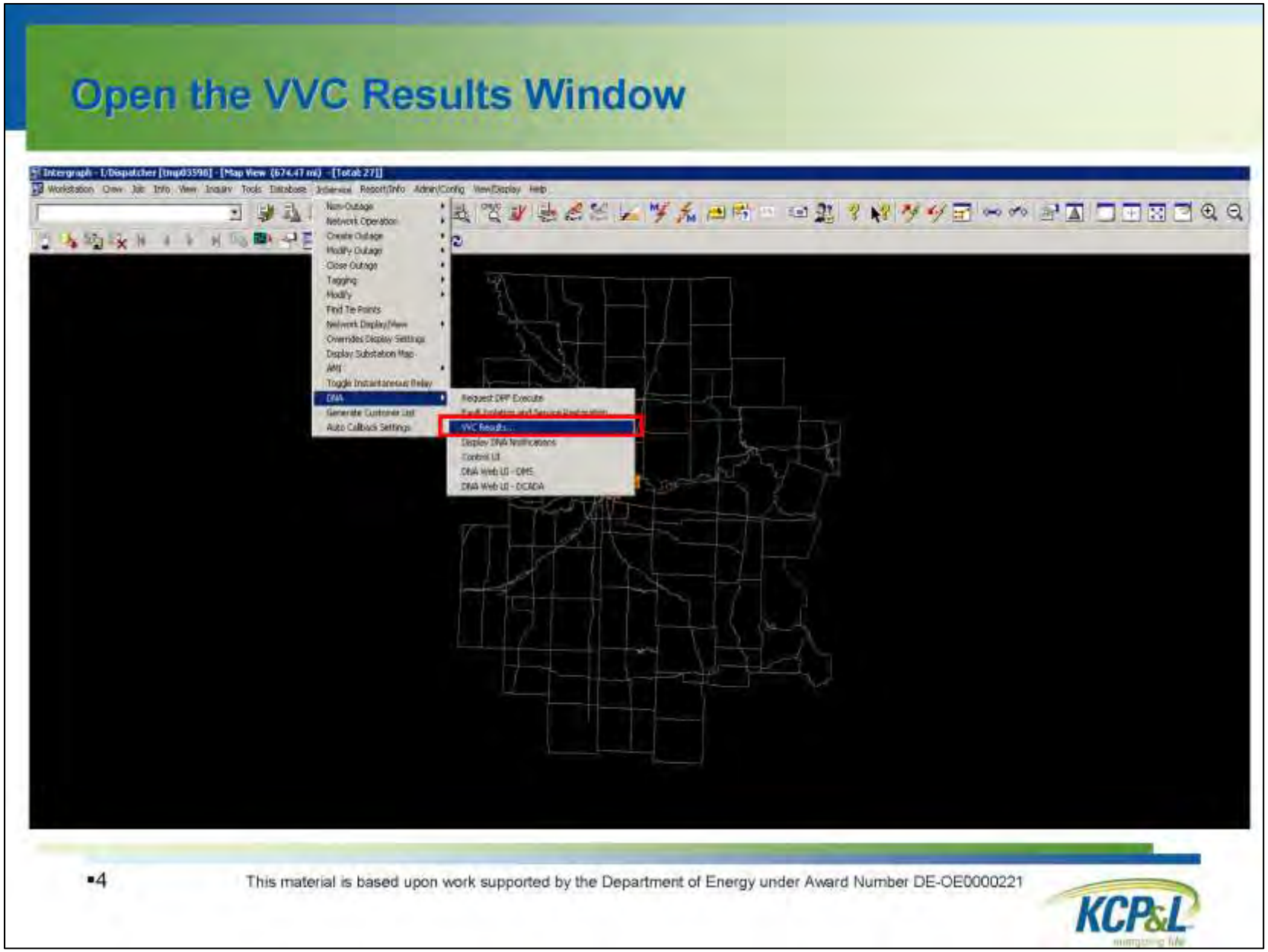
▪2

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

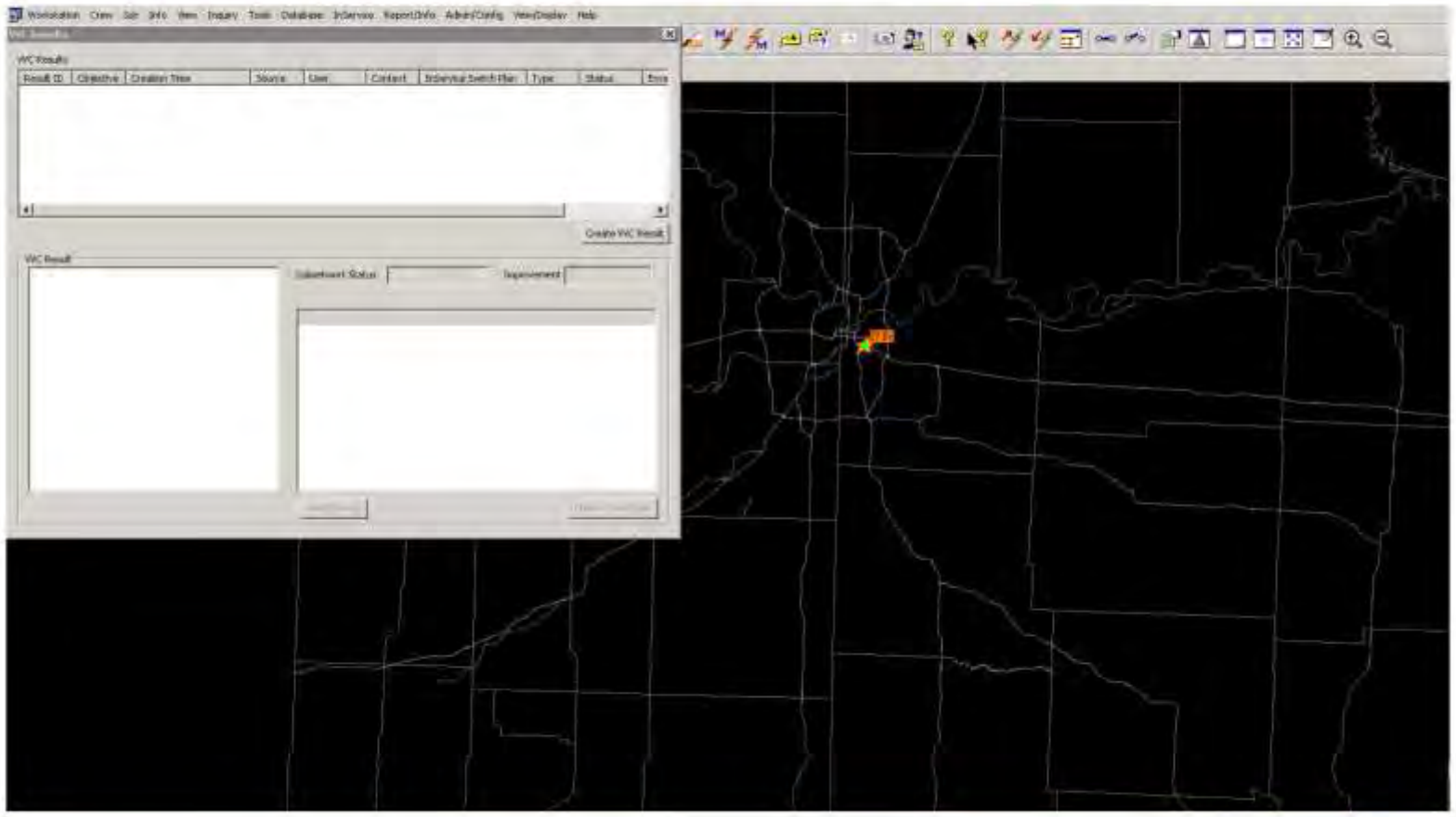
InService I/Dispatcher Main Screen



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

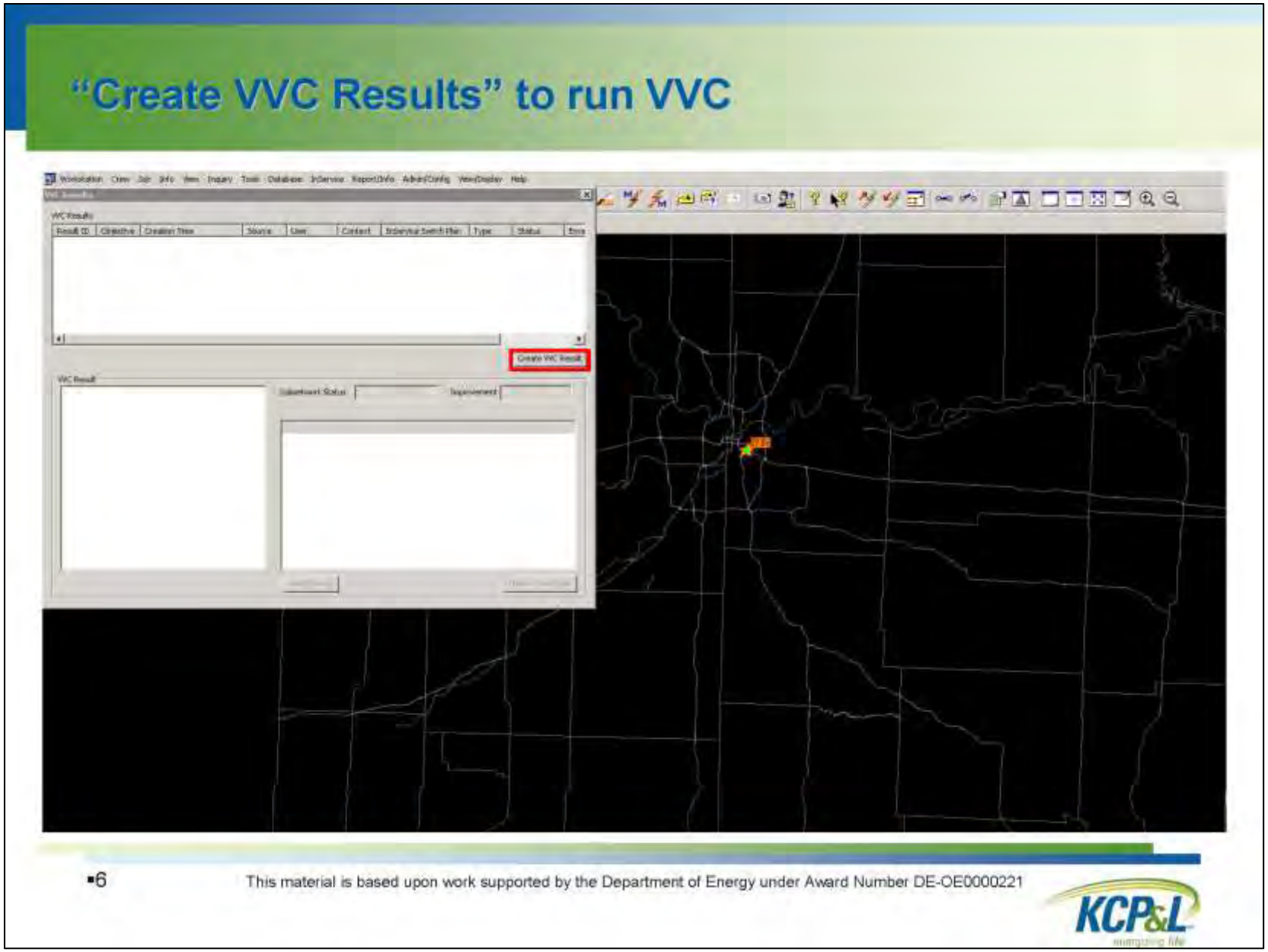

Open the VVC Results Window
Intergraph - I:/Dispatcher [tmp03598] - [Map View (674.47 mi) - [Total: 27]]
Workstation Crew Job Info View Inquiry Tools Database Jobservice Report/Info Admin/Config View/Display Help
Non-Outage
Network Operation
Create Outage
Modify Outage
Close Outage
Tagging
Modify
Find Tie Points
Network Display/View
Overrides Display Settings
Display Substation Map
AMI
Toggle Instantaneous Relay
DNA
Generate Customer List
Auto Callback Settings
Request DMF Execute
VVC Results...
Display DNA Notifications
Control UI
DNA Web UI - DMS
DNA Web UI - DCADA
4
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

VVC Results Window

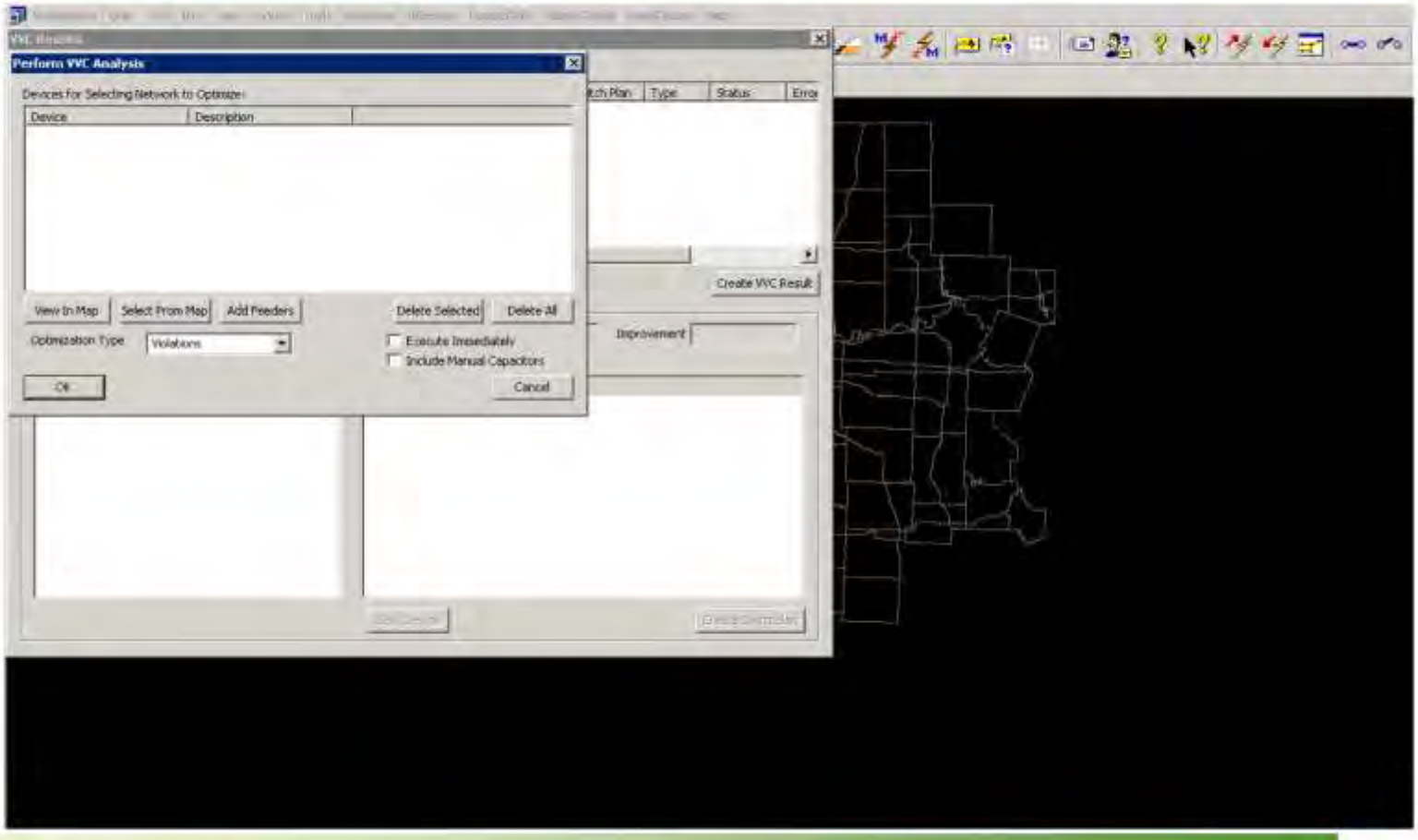


This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

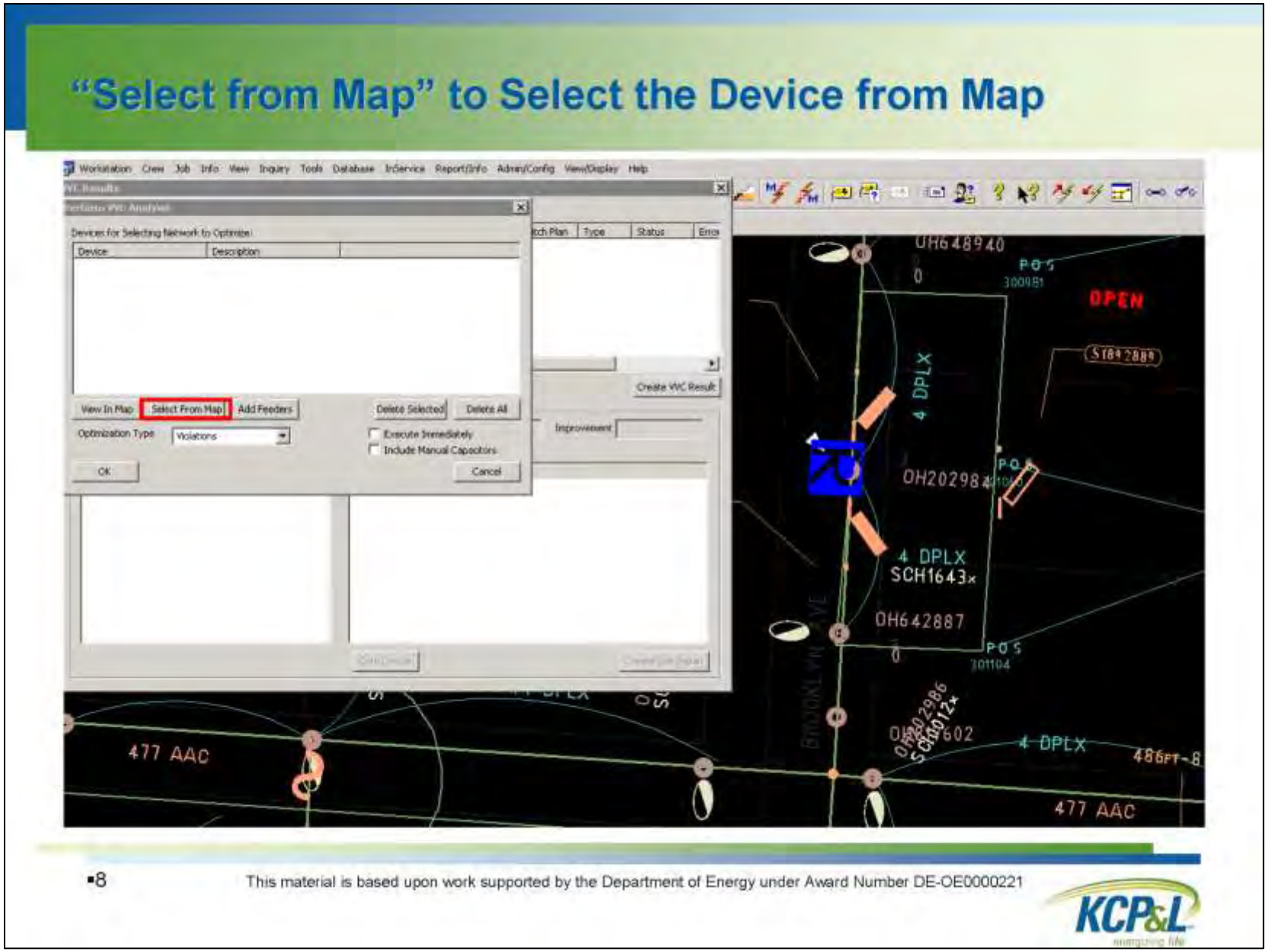
KCP&L energizing life

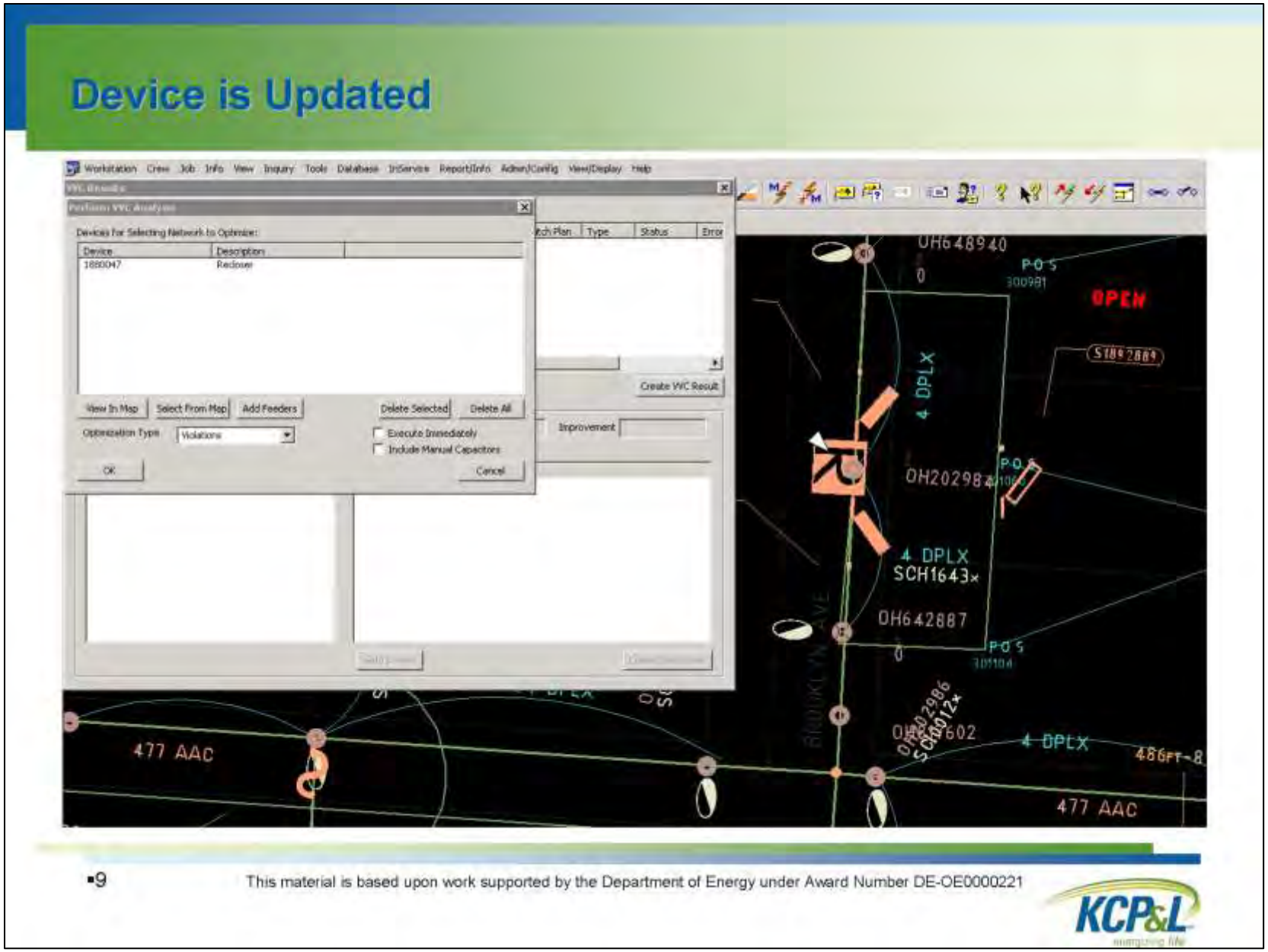

"Create VVC Results" to run VVC
6
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

New Window Opened to Select Device

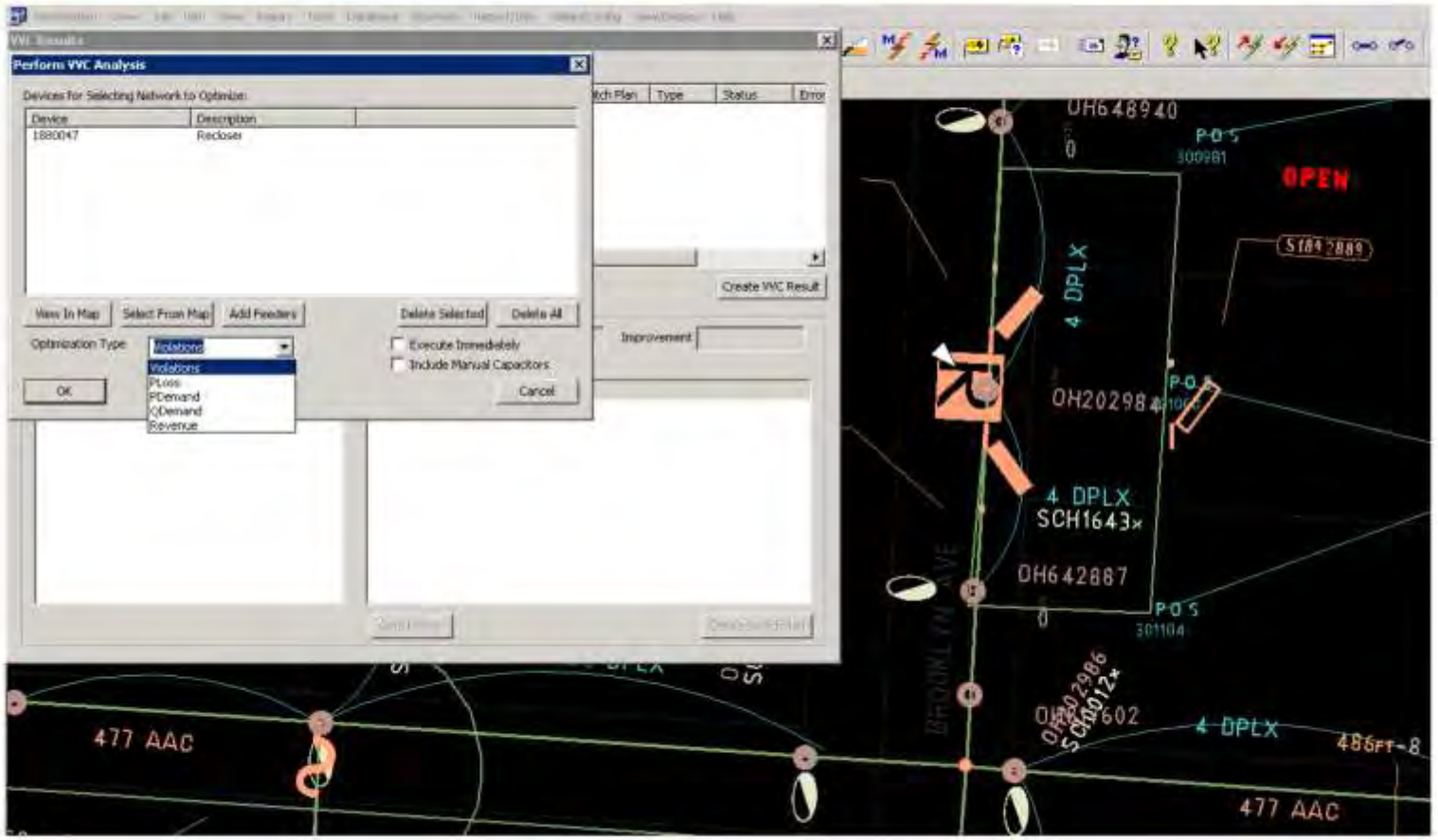


This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

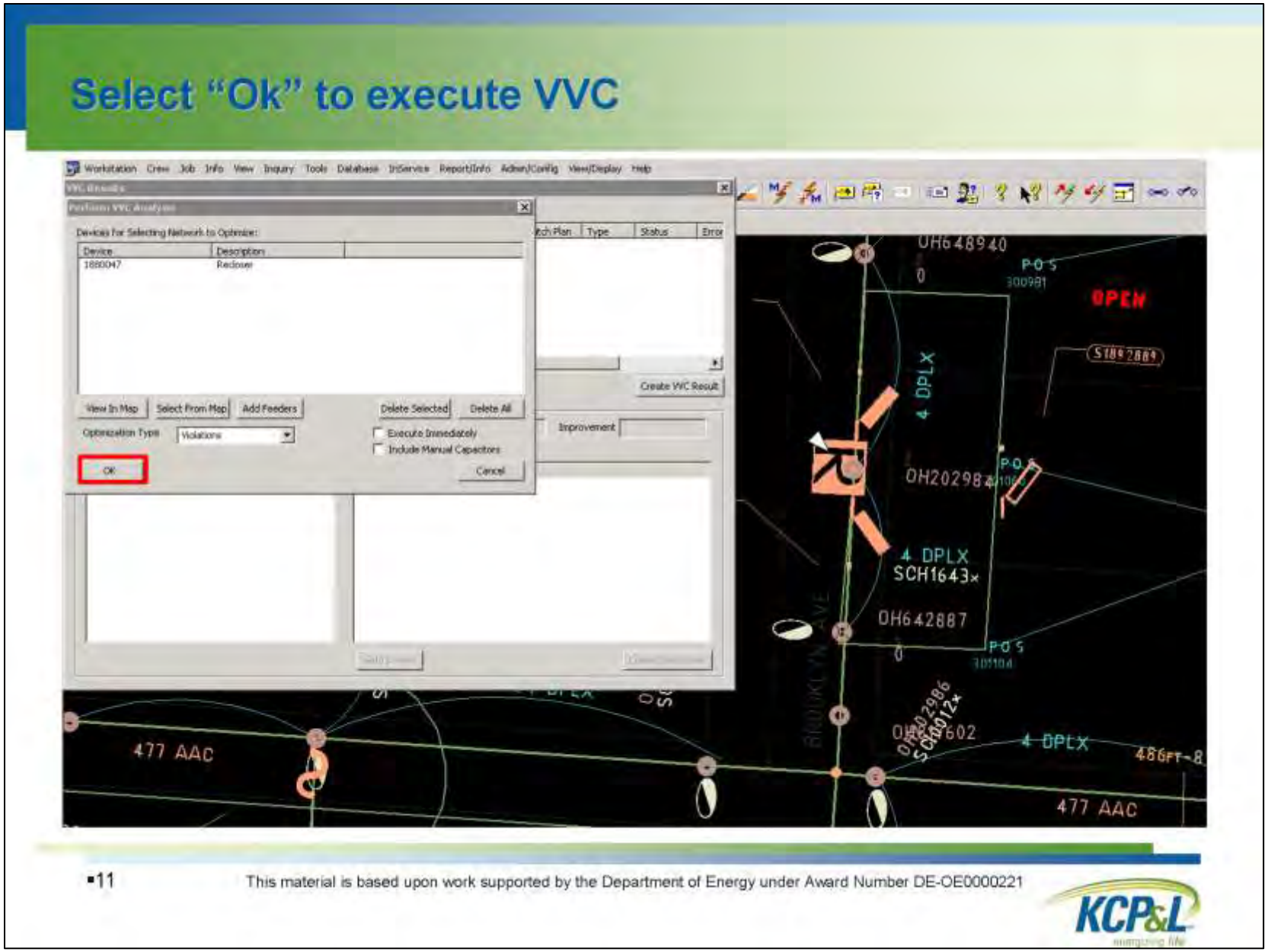

"Select from Map" to Select the Device from Map
Workstation Crew Job Info View Inquiry Tools Database InService Report/Info Admin/Config View/Display Help
Devices for Selecting Network to Optimize
Device
Description
View In Map
Select From Map
Add Feeders
Delete Selected
Delete All
Optimization Type
Violations
Execute Immediately
Include Manual Capacitors
OK
Cancel
Create VVC Result
OH648940
POS
OPEN
4 DPLX
OH202984
4 DPLX
SCH1643x
OH642887
POS
301104
477 AAC
4 DPLX
486FT-8
477 AAC
8
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

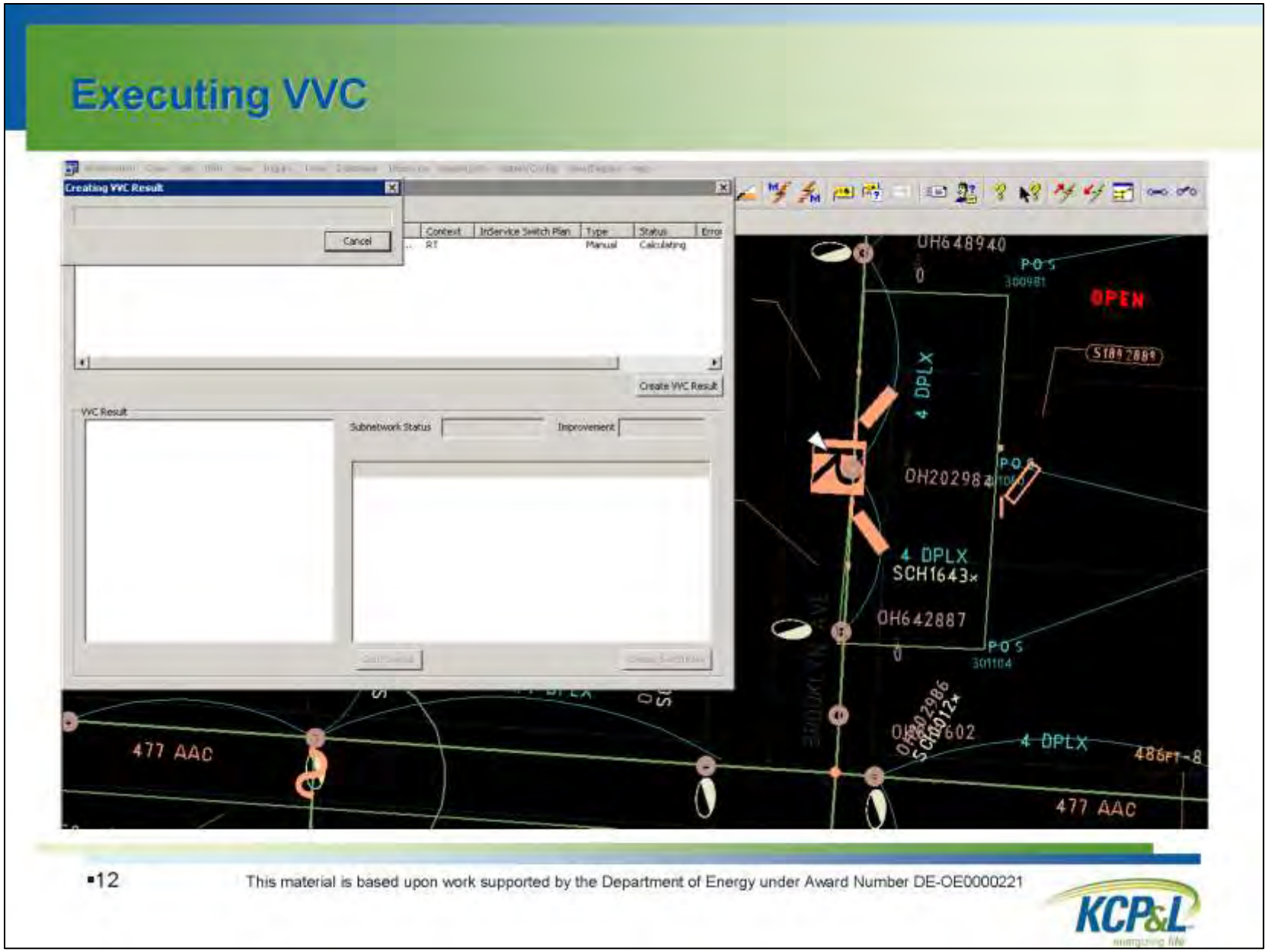

Device is Updated
Workstation Crew Job Info View Inquiry Tools Database InService Report/Info Admin/Config View/Display Help
Devices For Selecting Network to Optimize:
Device
Description
1888047
Recloser
Type
Status
View In Map
Select From Map
Add Feeders
Delete Selected
Delete All
Optimization Type
Violations
Execute Immediately
Include Manual Capacitors
OK
Cancel
Create WC Result
Improvement
OH648940
P O S
300981
OPEN
4 DPLX
OH202984
4 DPLX
SCH1643x
OH642887
P O S
300104
477 AAC
4 DPLX
486FT-8
477 AAC
9
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

Select the Optimization Type to Run VVC

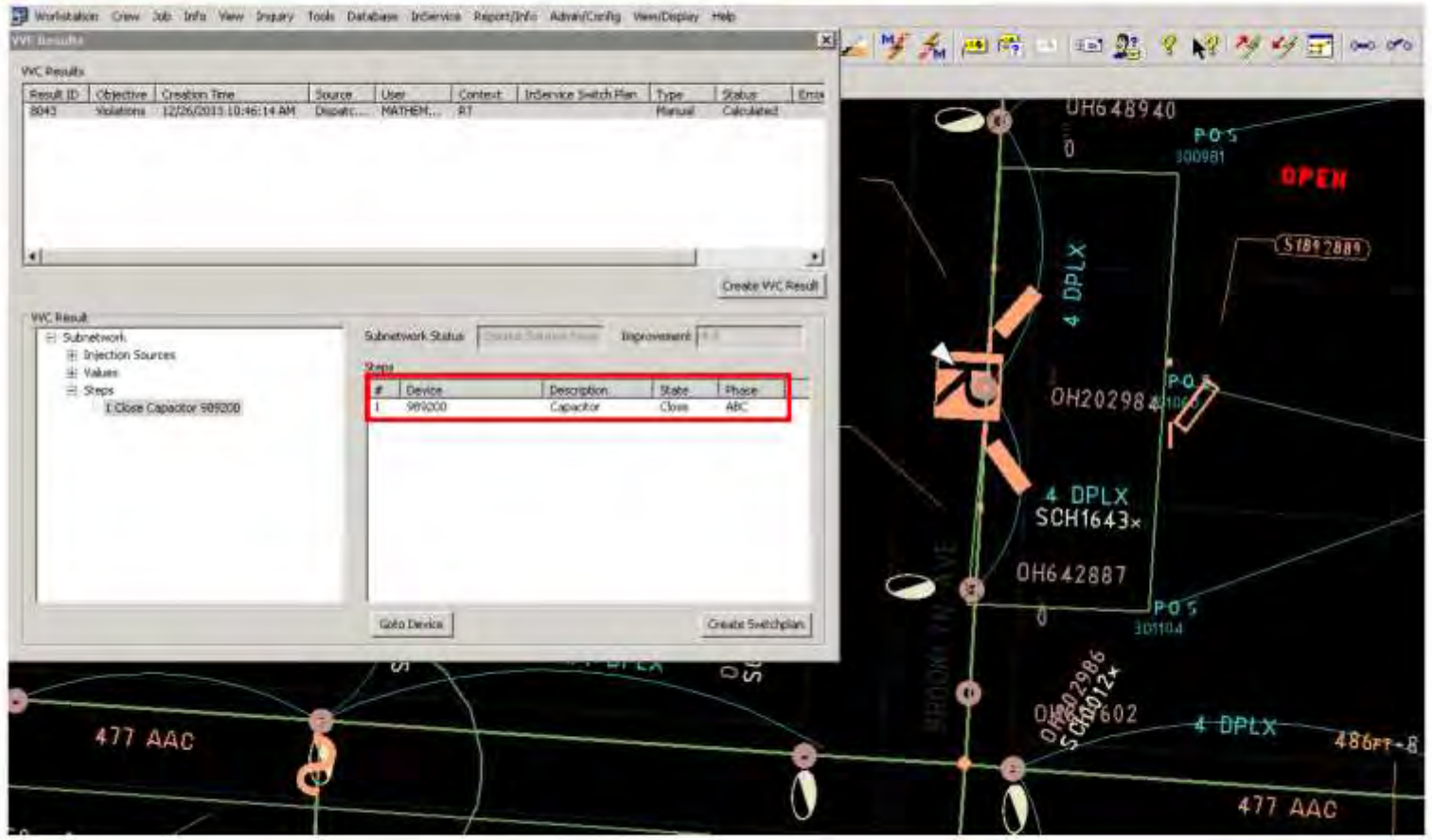


This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221


Select "Ok" to execute VVC
Devices For Selecting Network to Optimize:
Device
Description
1888047
Recloser
View In Map
Select From Map
Add Feeders
Delete Selected
Delete All
Optimization Type
Violations
Execute Immediately
Include Manual Capacitors
OK
Cancel
Create VVC Result
Improvement
OH648940
POS
OPEN
4 DPLX
OH2029842
4 DPLX
SCH1643x
OH642887
477 AAC
4 DPLX
486FT-8
477 AAC
11
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L


Executing VVC
Creating VVC Result
Cancel
Context
InService Switch Plan
Type
Status
Manual
Calculating
Create VVC Result
VVC Result
Subnetwork Status
Improvement
OH648940
POS
OPEN
4 DPLX
OH202984
4 DPLX
SCH1643x
OH642887
POS
477 AAC
4 DPLX
486FT-8
477 AAC
12
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

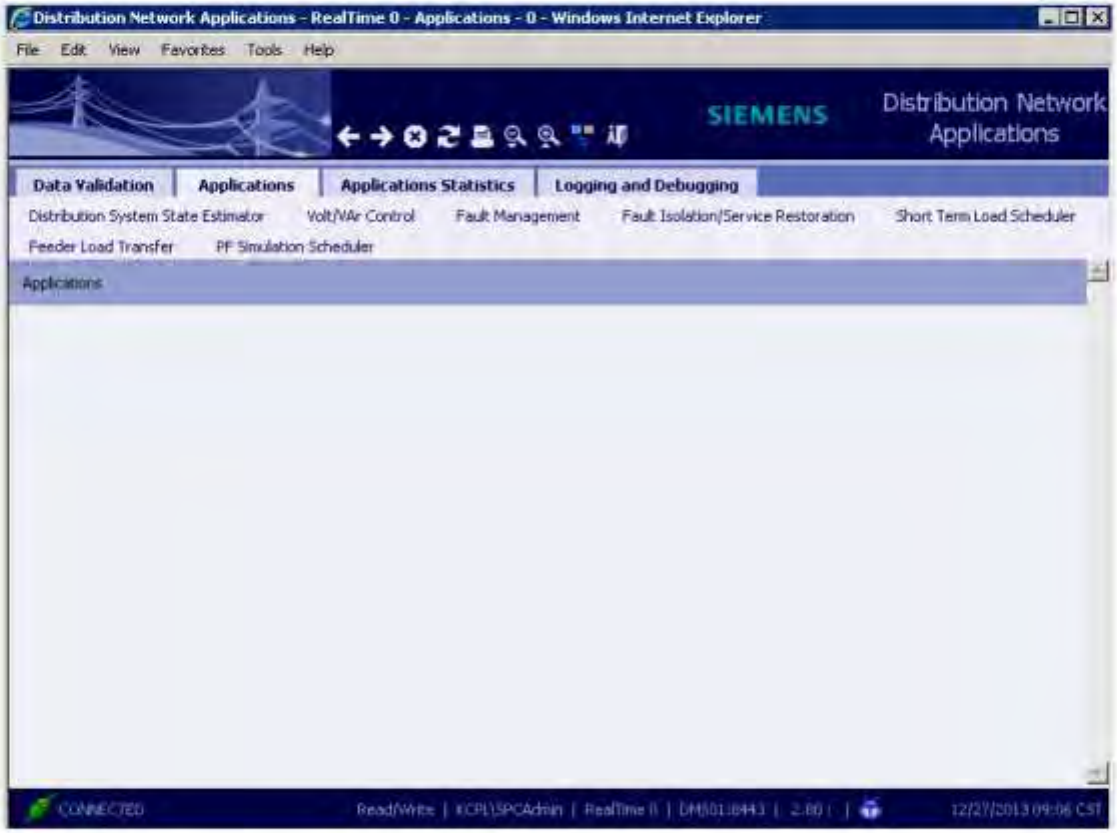
VVC Results



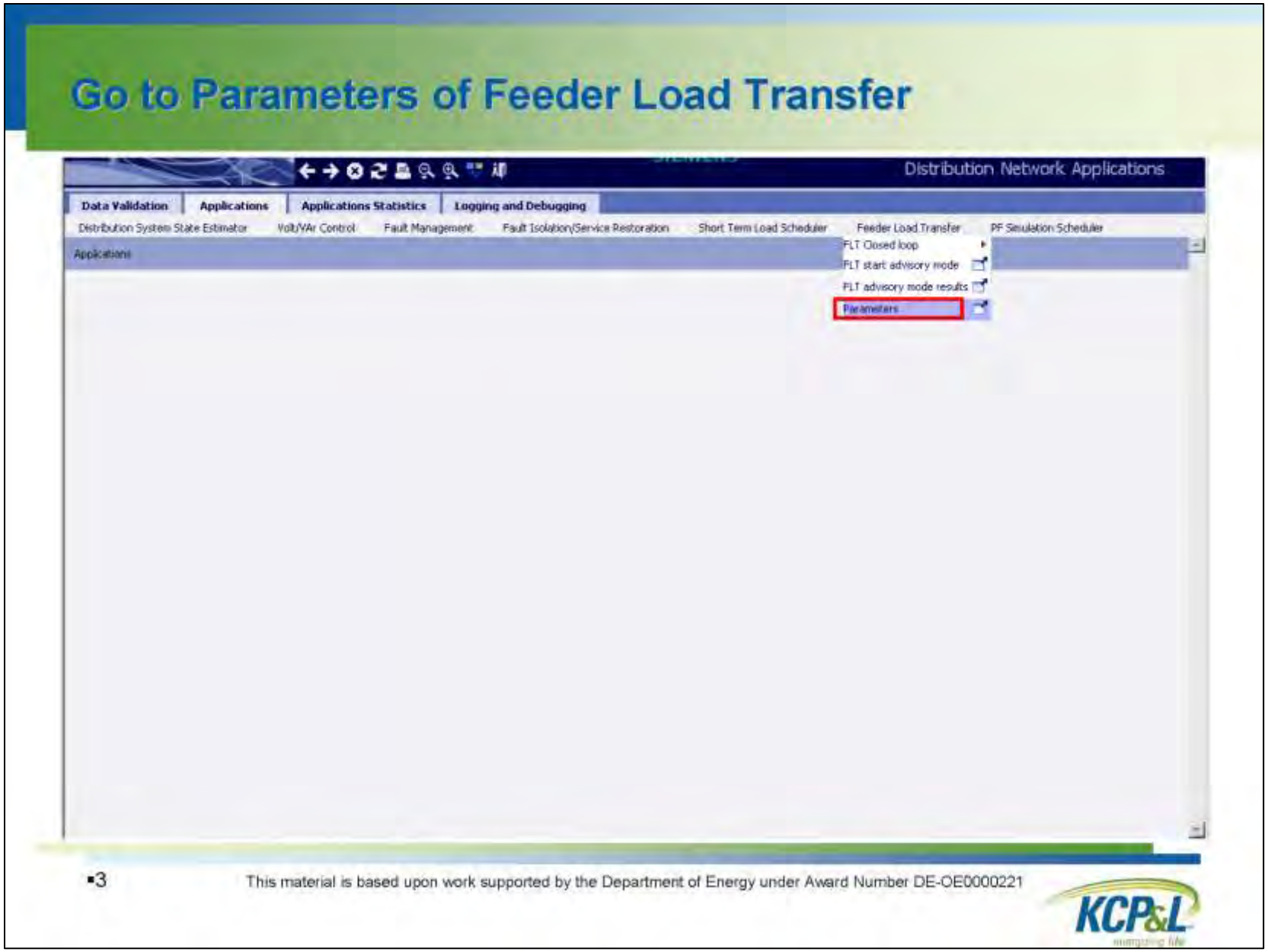
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

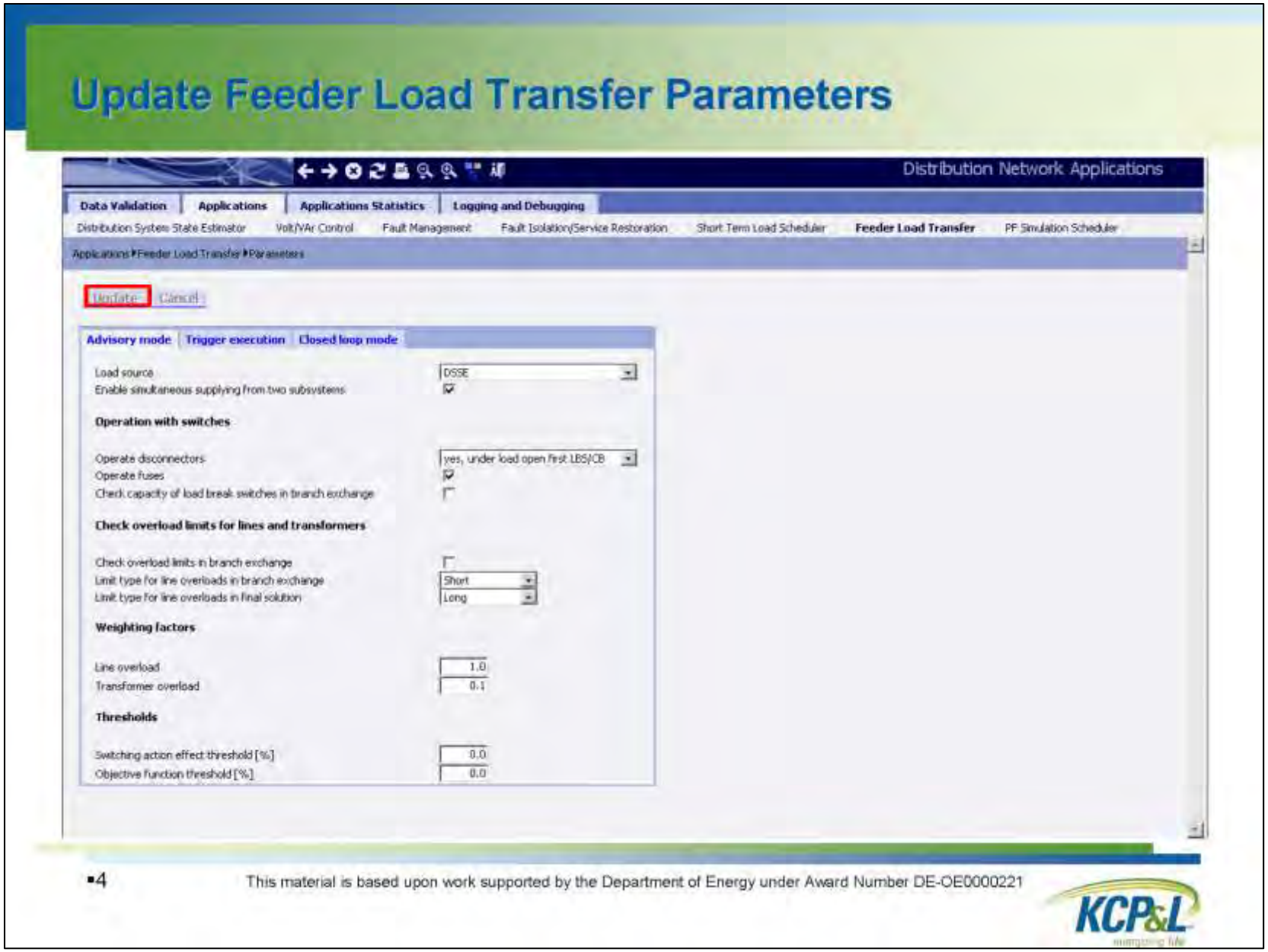

1st Responder Feeder Load Transfer
- KC Green Impact Zone Initiative
- DOE Regional SmartGrid Demonstration Program
- EPRI SmartGrid Demonstration Program
KCP&L
SmartGrid
the future of energy

Launch DNA WebUI

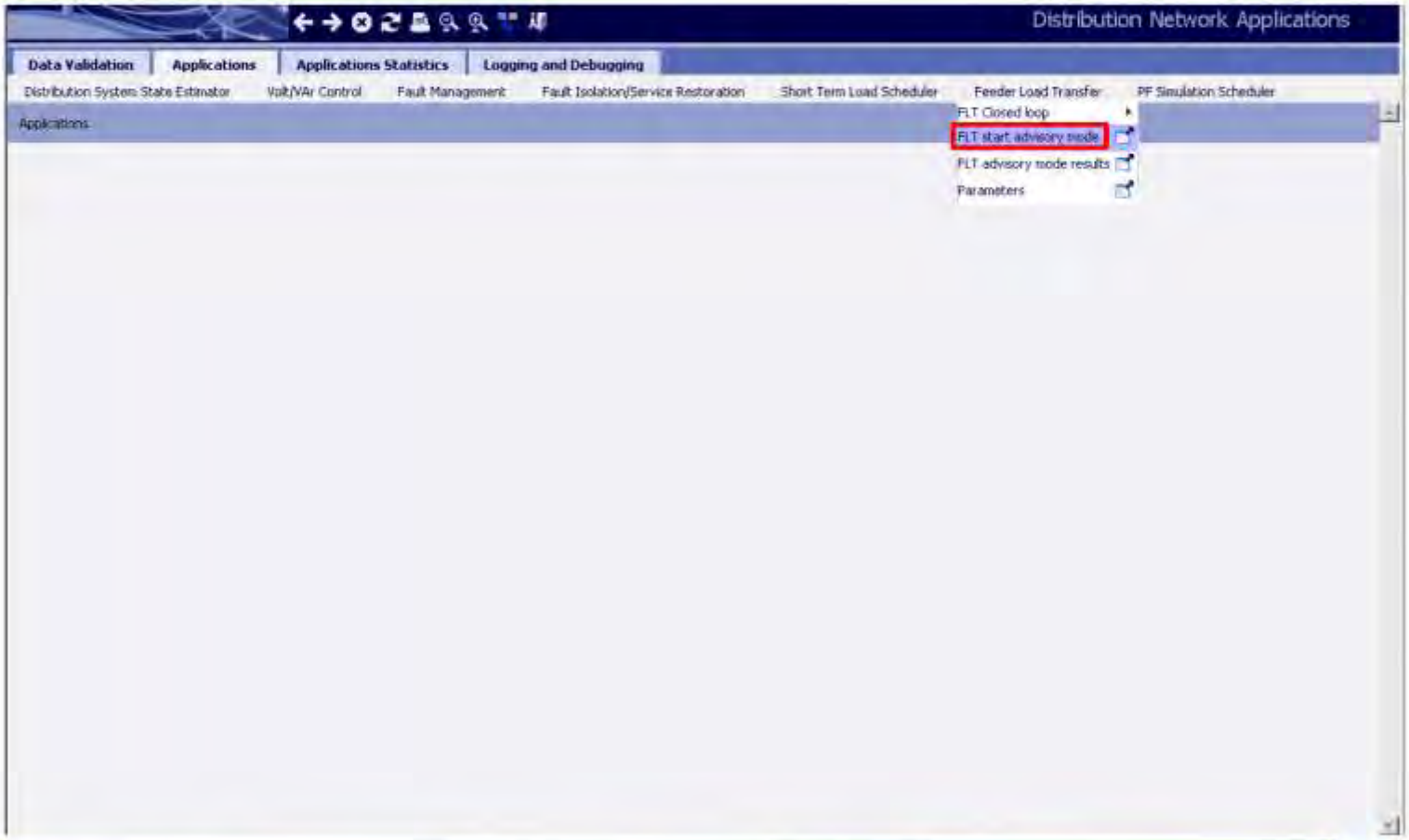


This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

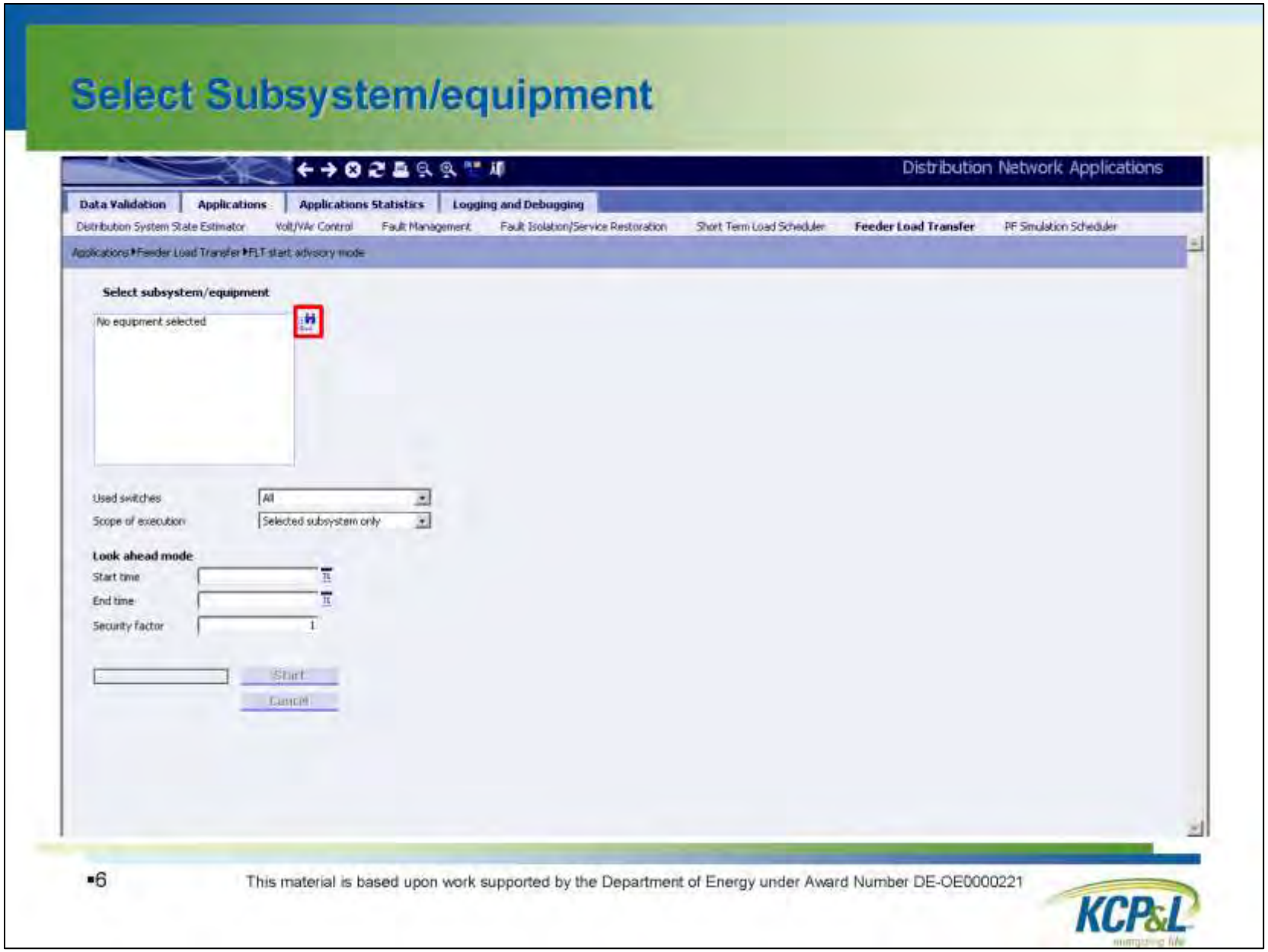

Go to Parameters of Feeder Load Transfer
Distribution Network Applications
Data Validation
Applications
Applications Statistics
Logging and Debugging
Distribution System State Estimator
Volt/VAr Control
Fault Management
Fault Isolation/Service Restoration
Short Term Load Scheduler
Feeder Load Transfer
PF Simulation Scheduler
Applications
FLT Closed loop
FLT start advisory mode
FLT advisory mode results
Parameters
3
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

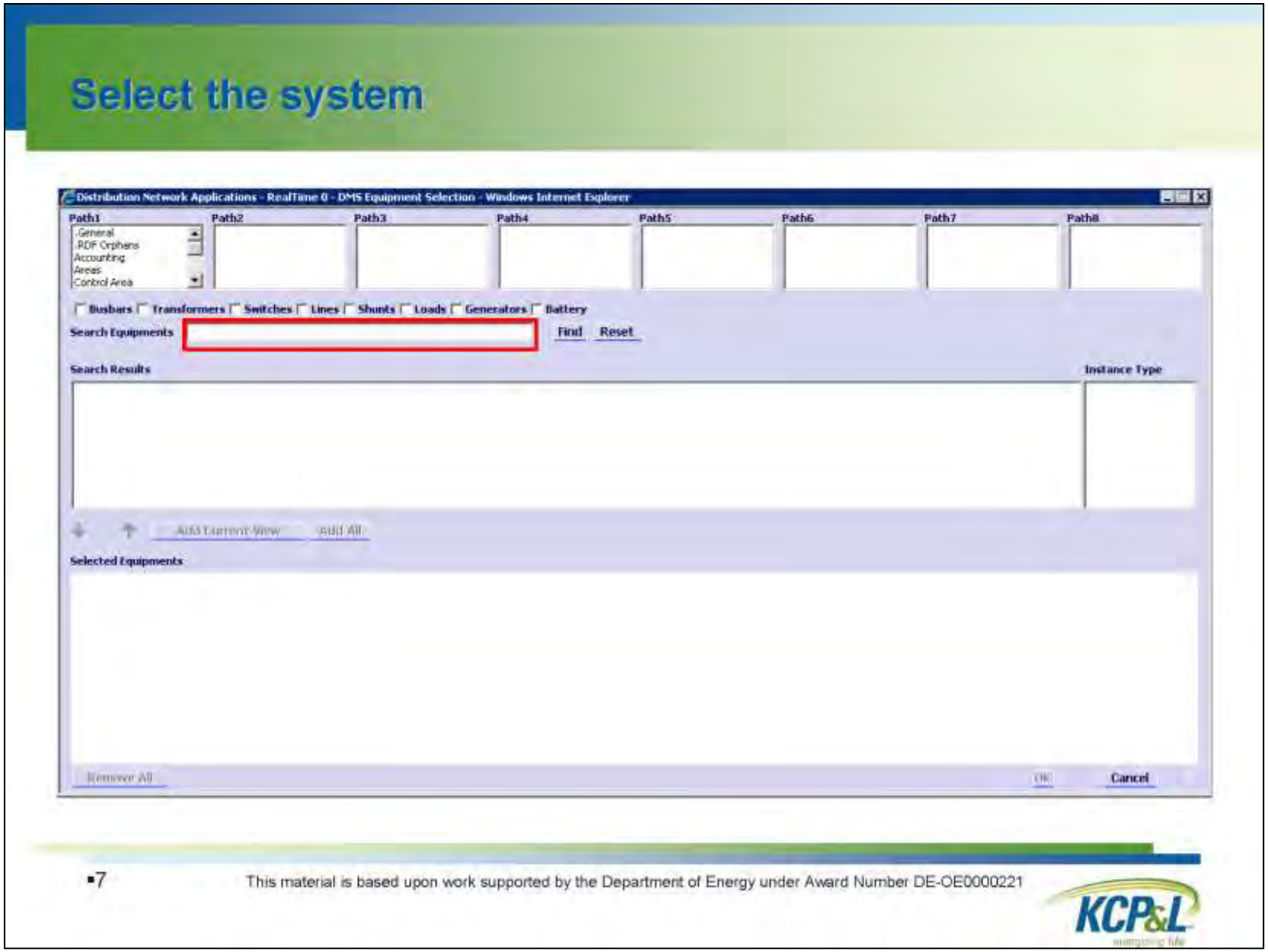

Update Feeder Load Transfer Parameters
Distribution Network Applications
Data Validation
Applications
Applications Statistics
Logging and Debugging
Distribution System State Estimator
Volt/VAr Control
Fault Management
Fault Isolation/Service Restoration
Short Term Load Scheduler
Feeder Load Transfer
PF Simulation Scheduler
Applications ▸ Feeder Load Transfer ▸ Parameters
Update
Cancel
Advisory mode
Trigger execution
Closed loop mode
Load source
DSSE
Enable simultaneous supplying from two subsystems
Operation with switches
Operate disconnectors
yes, under load open first LBS/CB
Operate fuses
Check capacity of load break switches in branch exchange
Check overload limits for lines and transformers
Check overload limits in branch exchange
Limit type for line overloads in branch exchange
Short
Limit type for line overloads in final solution
Long
Weighting factors
Line overload
1.0
Transformer overload
0.1
Thresholds
Switching action effect threshold [%]
0.0
Objective function threshold [%]
0.0
▪4
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

"FLT Start Advisory Mode"

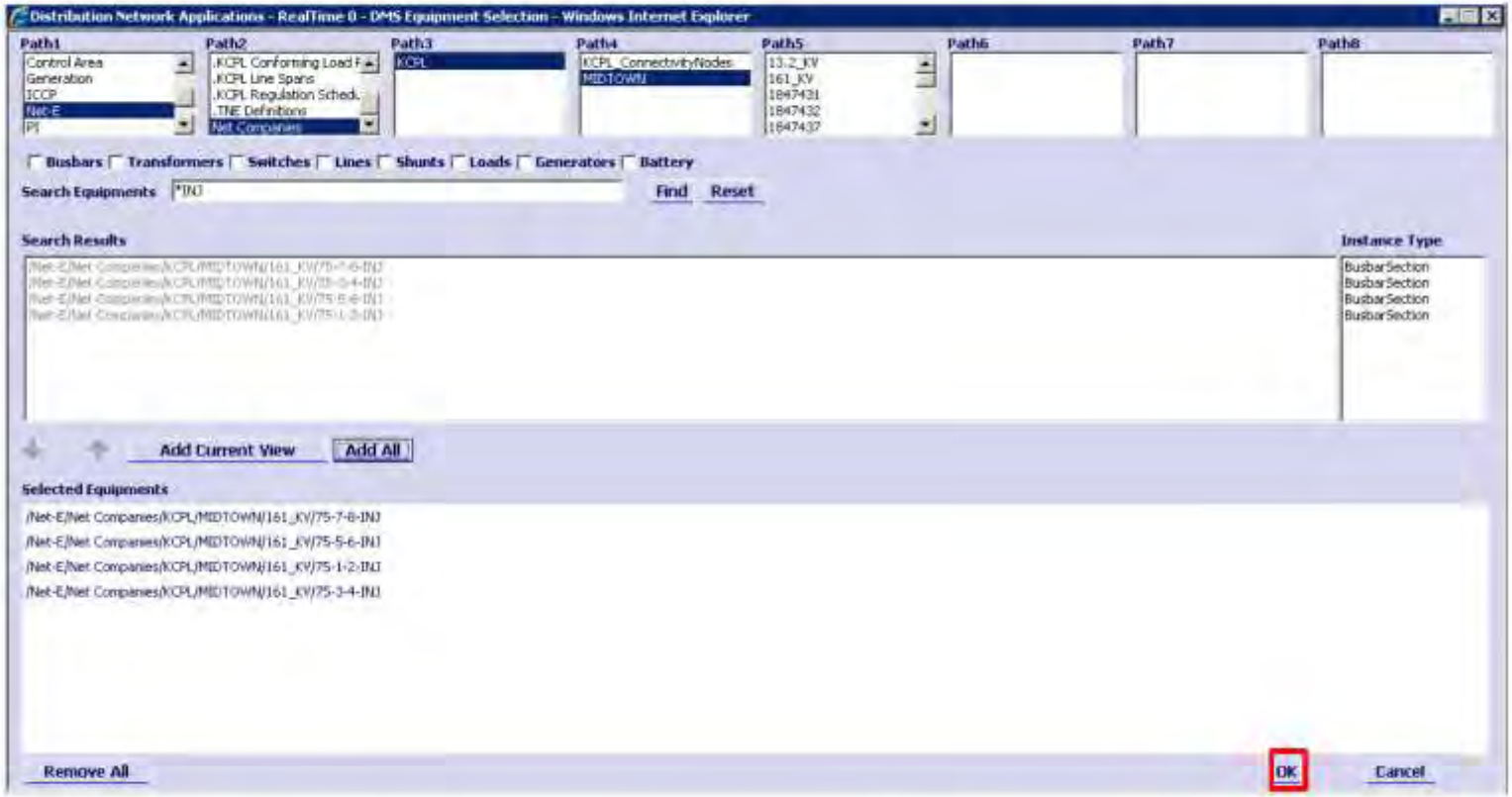


This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

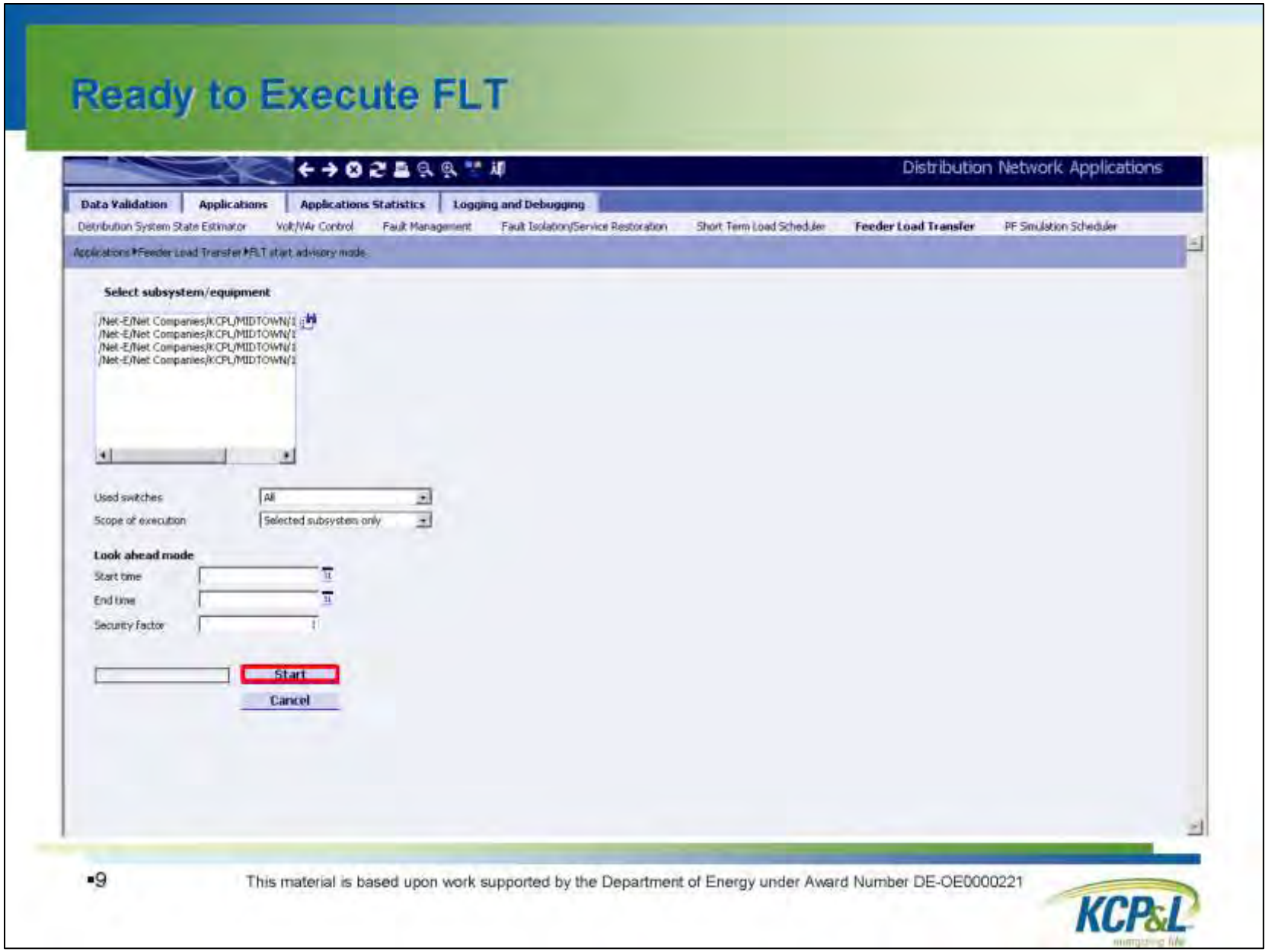

Select Subsystem/equipment
Distribution Network Applications
Data Validation
Applications
Applications Statistics
Logging and Debugging
Distribution System State Estimator
Volt/VAr Control
Fault Management
Fault Isolation/Service Restoration
Short Term Load Scheduler
Feeder Load Transfer
PF Simulation Scheduler
Applications ▸Feeder Load Transfer ▸FLT start advisory mode
Select subsystem/equipment
No equipment selected
Used switches
All
Scope of execution
Selected subsystem only
Look ahead mode
Start time
End time
Security factor
1
Start
Cancel
6
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

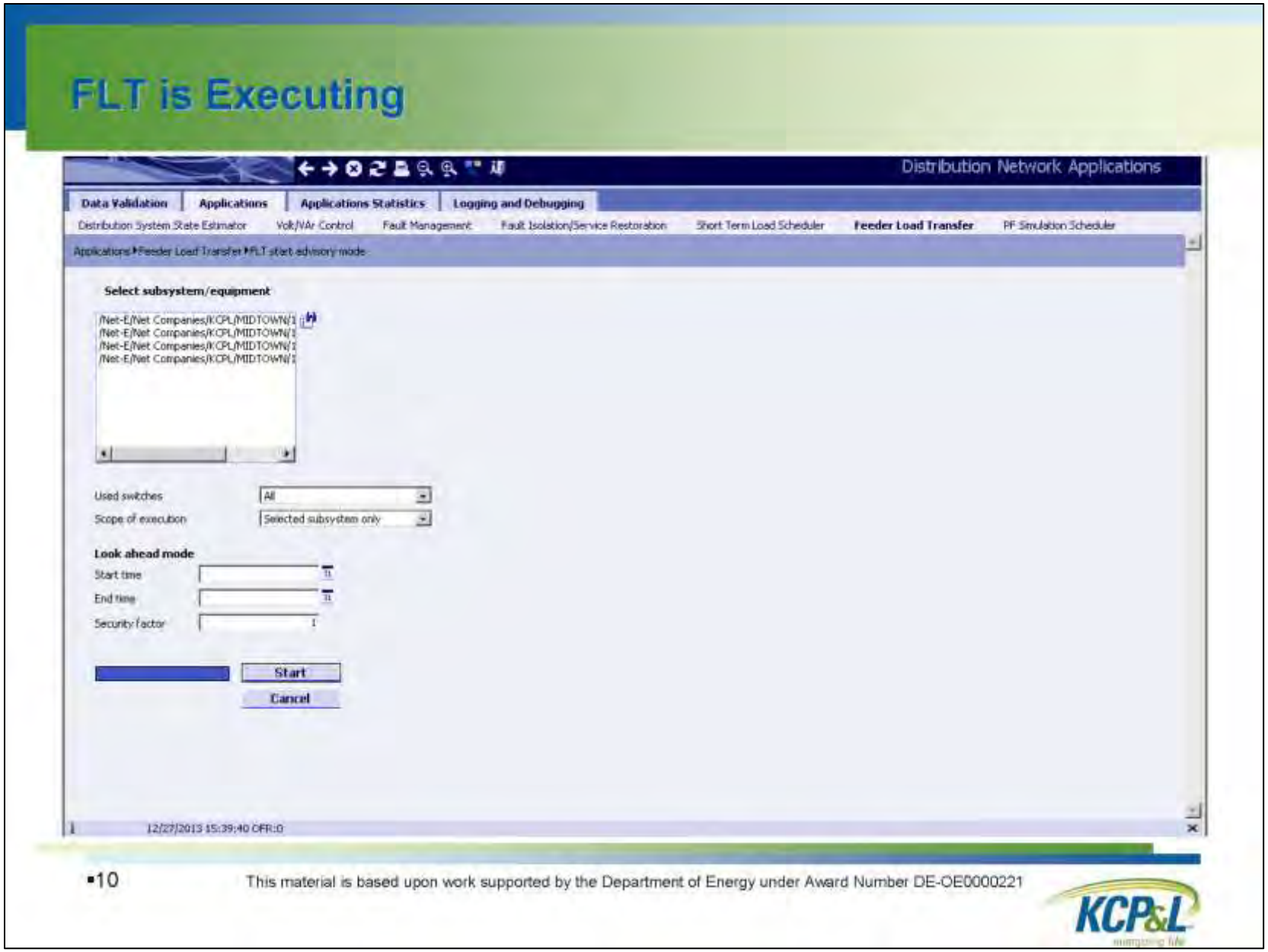

Select the system
Distribution Network Applications - RealTime 0 - DMS Equipment Selection - Windows Internet Explorer
Path1
Path2
Path3
Path4
Path5
Path6
Path7
Path8
.General
.RDF Orphans
Accounting
Areas
Control Area
Busbars
Transformers
Switches
Lines
Shunts
Loads
Generators
Battery
Search Equipments
Find
Reset
Search Results
Instance Type
Add Current View
Add All
Selected Equipments
Remove All
OK
Cancel
7
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

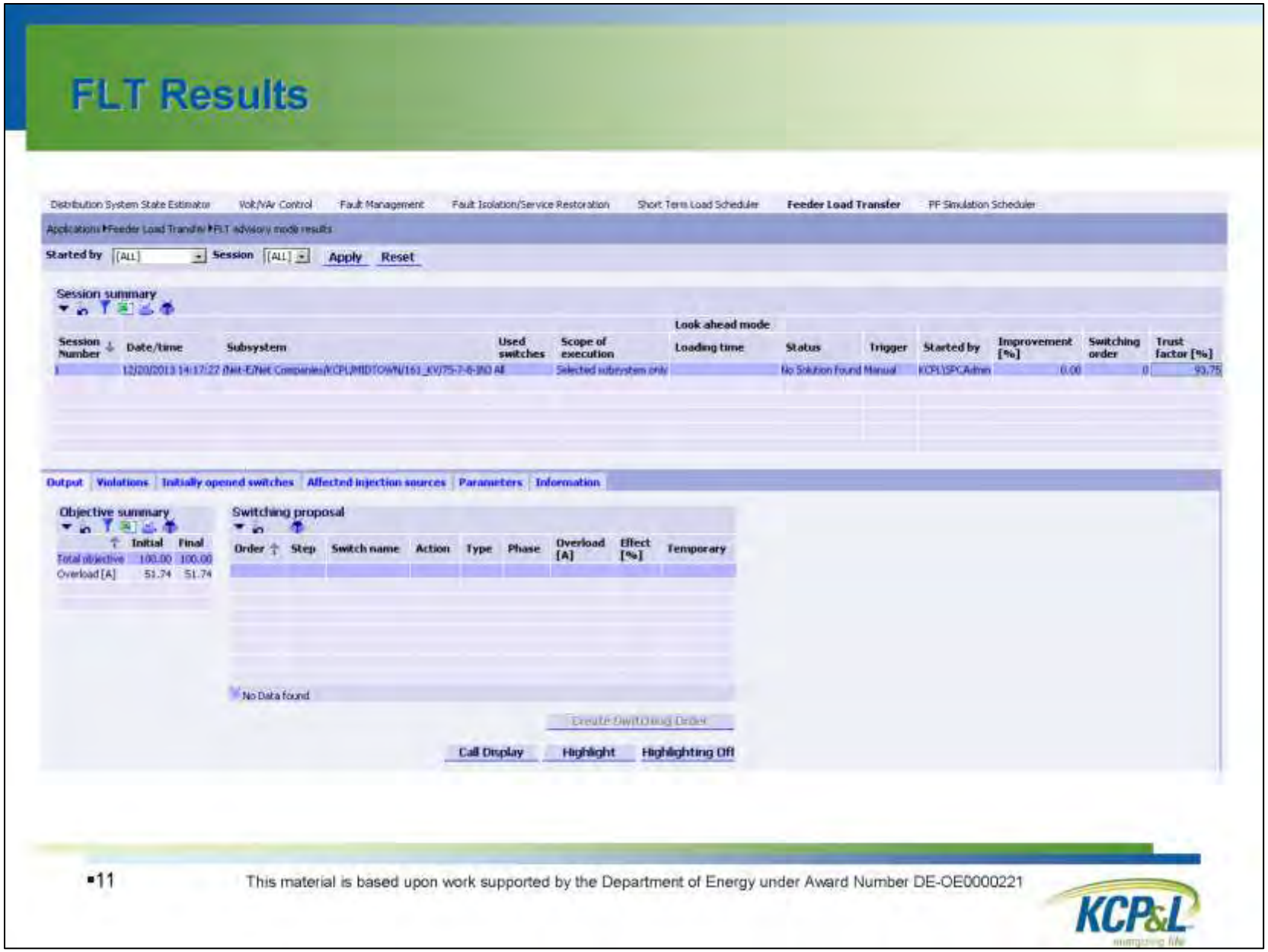
System Selected



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

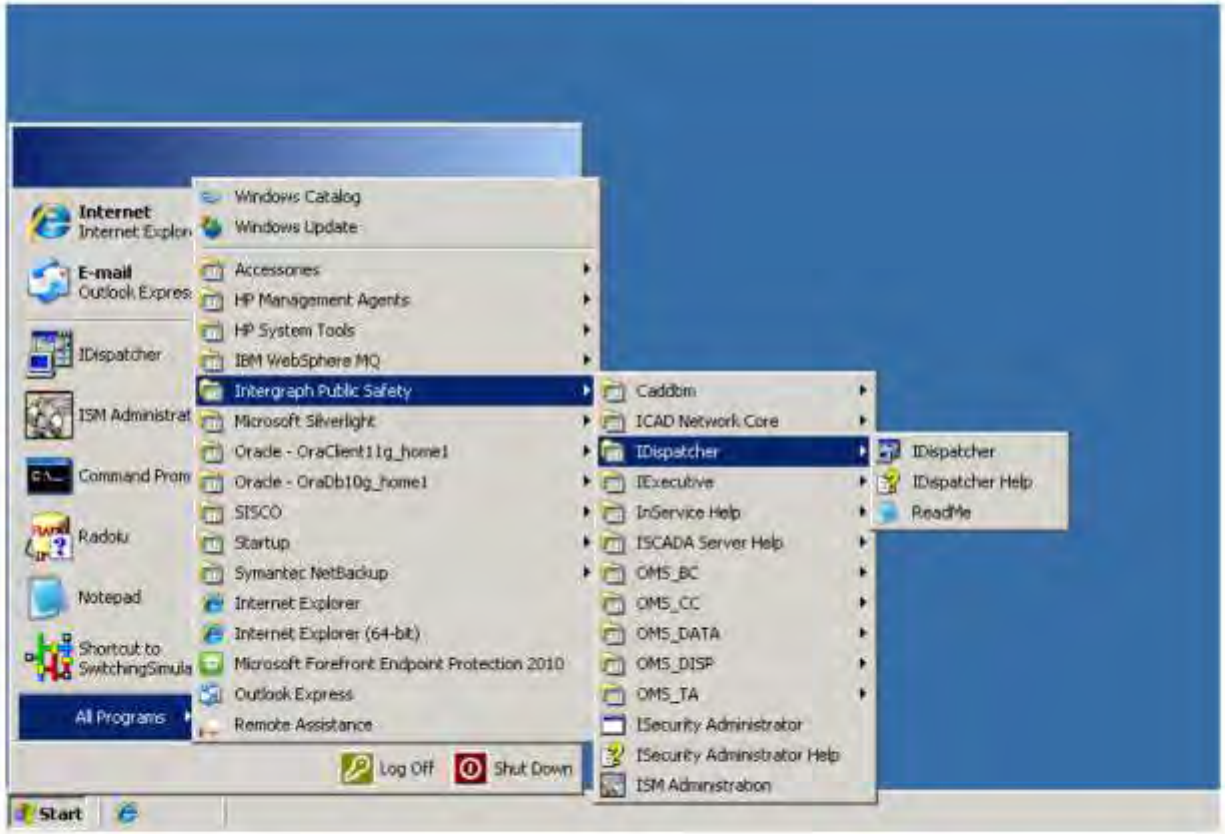

Ready to Execute FLT
Distribution Network Applications
Data Validation
Applications
Applications Statistics
Logging and Debugging
Distribution System State Estimator
Volt/VAr Control
Fault Management
Fault Isolation/Service Restoration
Short Term Load Scheduler
Feeder Load Transfer
PF Simulation Scheduler
Applications ▸Feeder Load Transfer ▸FLT start advisory mode
Select subsystem/equipment
/Net-E/Net Companies/KCPL/MIDTOWN/1
/Net-E/Net Companies/KCPL/MIDTOWN/1
/Net-E/Net Companies/KCPL/MIDTOWN/1
/Net-E/Net Companies/KCPL/MIDTOWN/1
Used switches
All
Scope of execution
Selected subsystem only
Look ahead mode
Start time
End time
Security factor
Start
Cancel
9
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L


FLT is Executing
Distribution Network Applications
Data Validation
Applications
Applications Statistics
Logging and Debugging
Distribution System State Estimator
Volt/VAr Control
Fault Management
Fault Isolation/Service Restoration
Short Term Load Scheduler
Feeder Load Transfer
PF Simulation Scheduler
Applications ▸Feeder Load Transfer ▸FLT start advisory mode
Select subsystem/equipment
/Net-E/Net Companies/KCPL/MIDTOWN/1
/Net-E/Net Companies/KCPL/MIDTOWN/1
/Net-E/Net Companies/KCPL/MIDTOWN/1
/Net-E/Net Companies/KCPL/MIDTOWN/1
Used switches
All
Scope of execution
Selected subsystem only
Look ahead mode
Start time
End time
Security factor
Start
Cancel
12/27/2013 15:39:40 CFR:0
▪10
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L


FLT Results
Distribution System State Estimator
Volt/VAr Control
Fault Management
Fault Isolation/Service Restoration
Short Term Load Scheduler
Feeder Load Transfer
PF Simulation Scheduler
Applications ▸Feeder Load Transfer ▸FLT advisory mode results
Started by [ALL]
Session [ALL]
Apply
Reset
Session summary
Look ahead mode
Session Number
Date/time
Subsystem
Used switches
Scope of execution
Loading time
Status
Trigger
Started by
Improvement [%]
Switching order
Trust factor [%]
1 12/20/2013 14:17:22 /Net-E/Net Companies/KCPL/MIDTOWN/161_kV/75-7-6-BD All Selected subsystem only No Solution Found Manual KCPL\SPCAdmin 0.00 0 93.75
Output
Violations
Initially opened switches
Affected injection sources
Parameters
Information
Objective summary
Initial
Final
Total objective 100.00 100.00
Overload [A] 51.74 51.74
Switching proposal
Order
Step
Switch name
Action
Type
Phase
Overload [A]
Effect [%]
Temporary
No Data found
Create Switching Order
Call Display
Highlight
Highlighting Off
11
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L
energizing life


1st Responder Fault Isolation and Service Restoration
- KC Green Impact Zone Initiative
- DOE Regional SmartGrid Demonstration Program
- EPRI SmartGrid Demonstration Program
KCP&L
SmartGrid
the future of energy

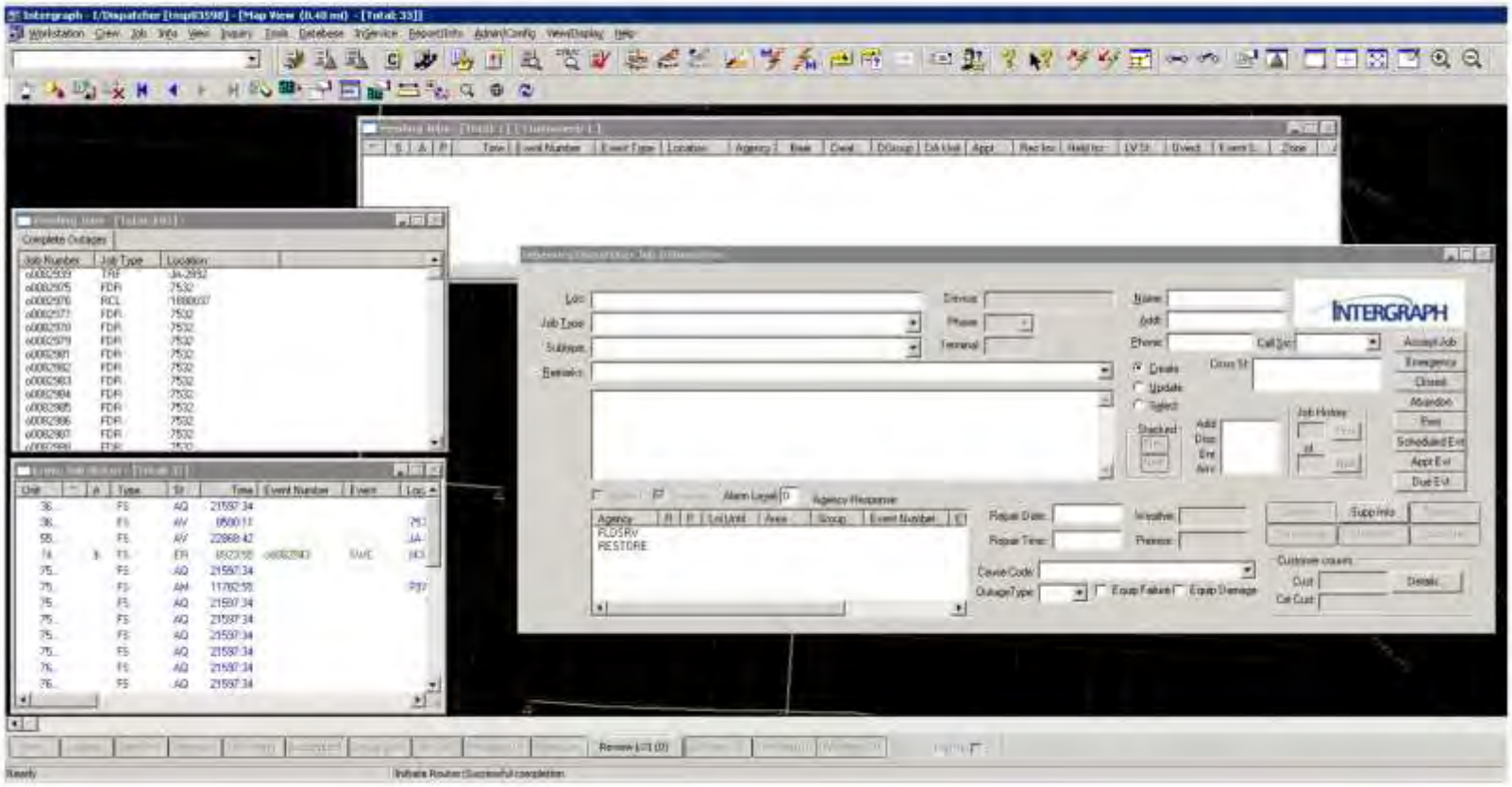
Launch InService I/Dispatcher



▪2

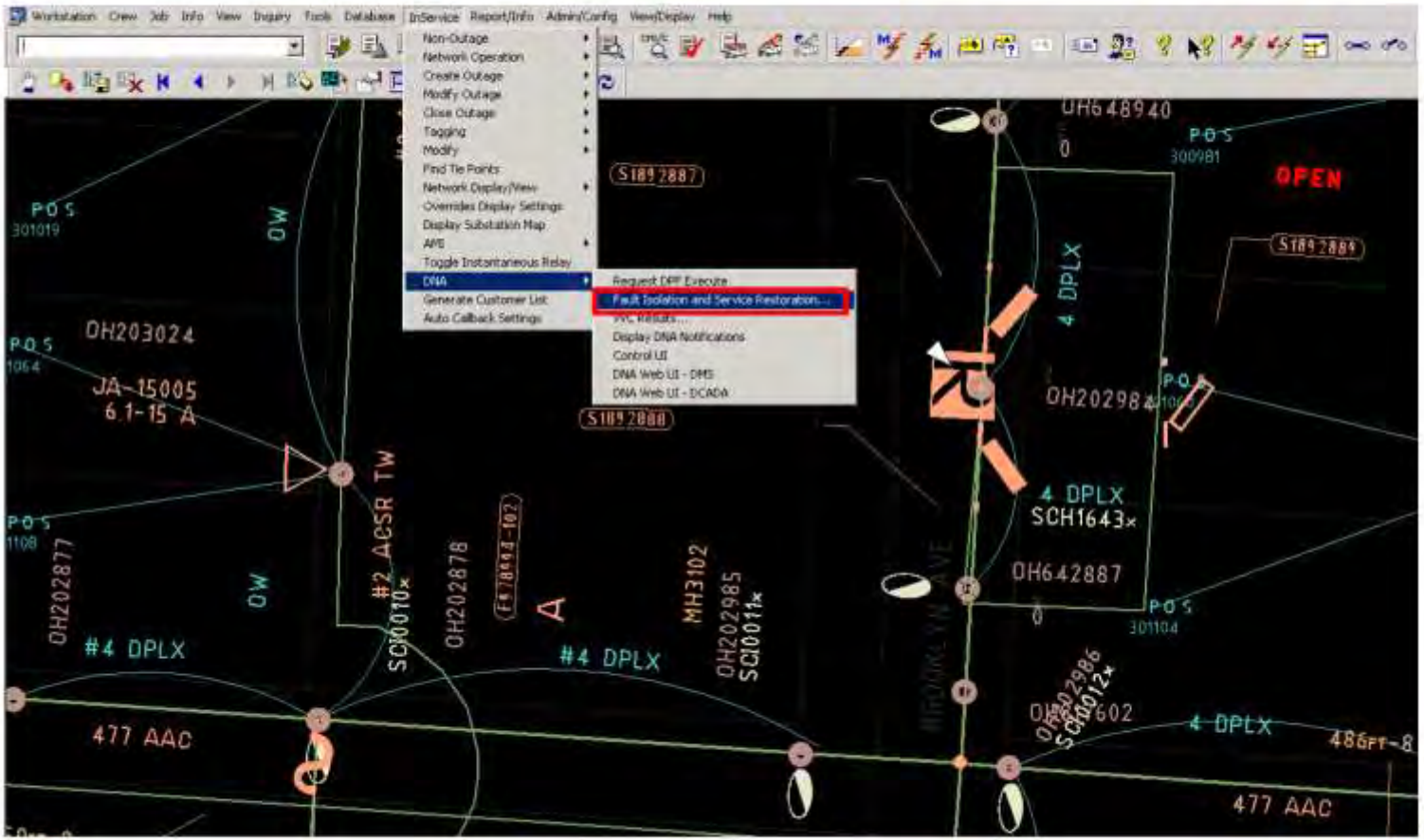
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

InService I/Dispatcher Main Screen



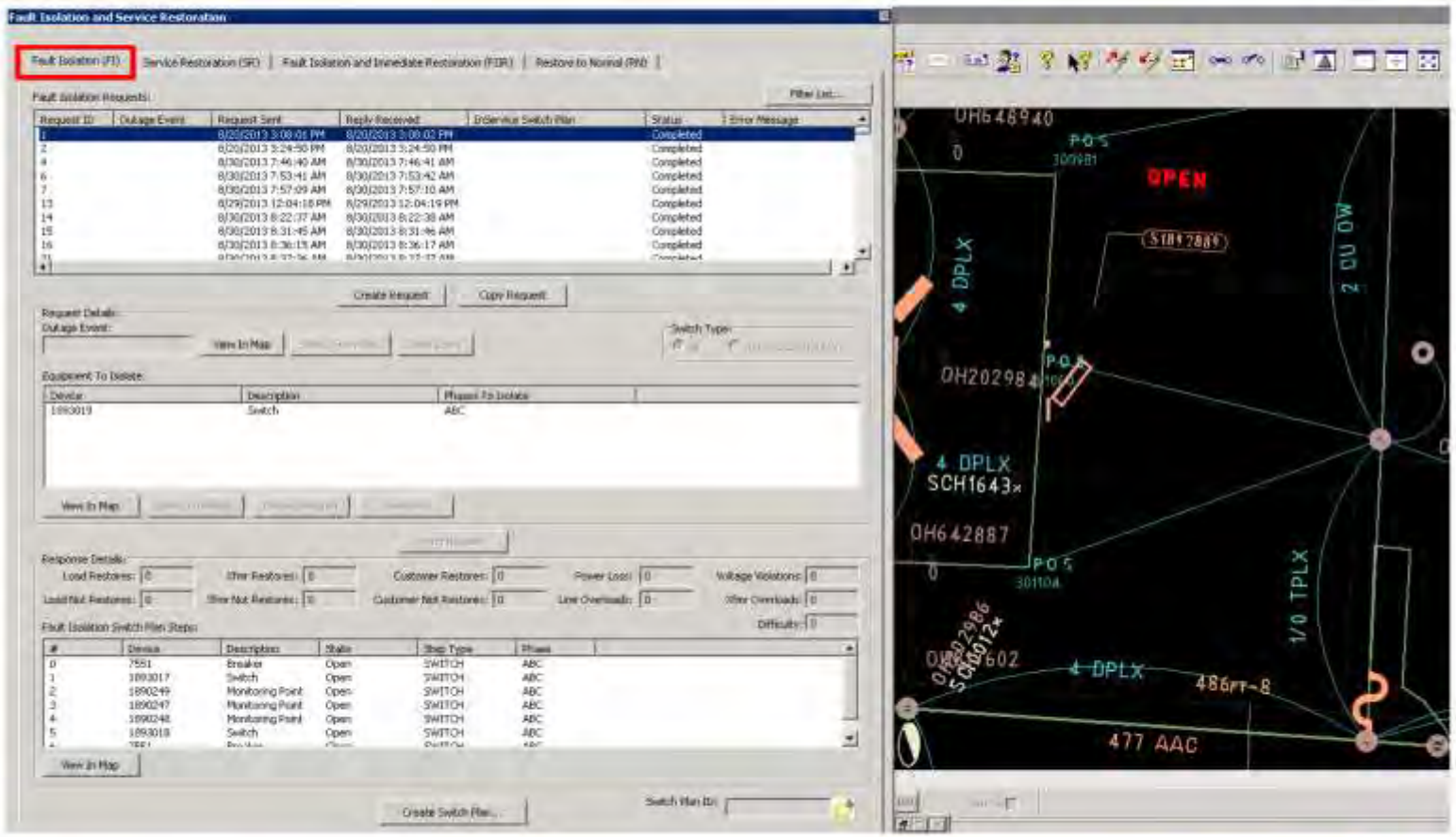
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Open the Fault Isolation and Service Restoration Window



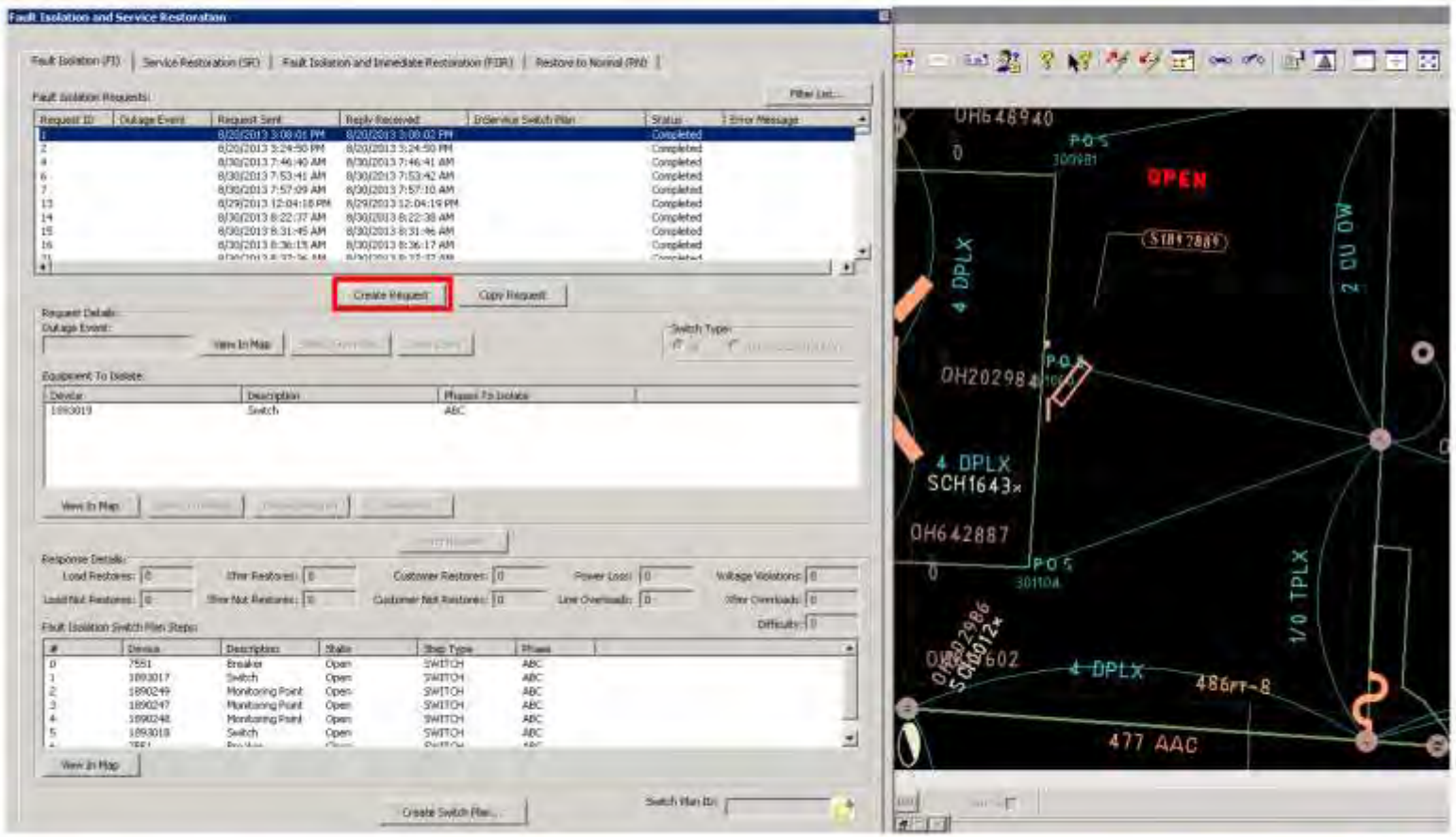
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

FISR Window: Fault Isolation



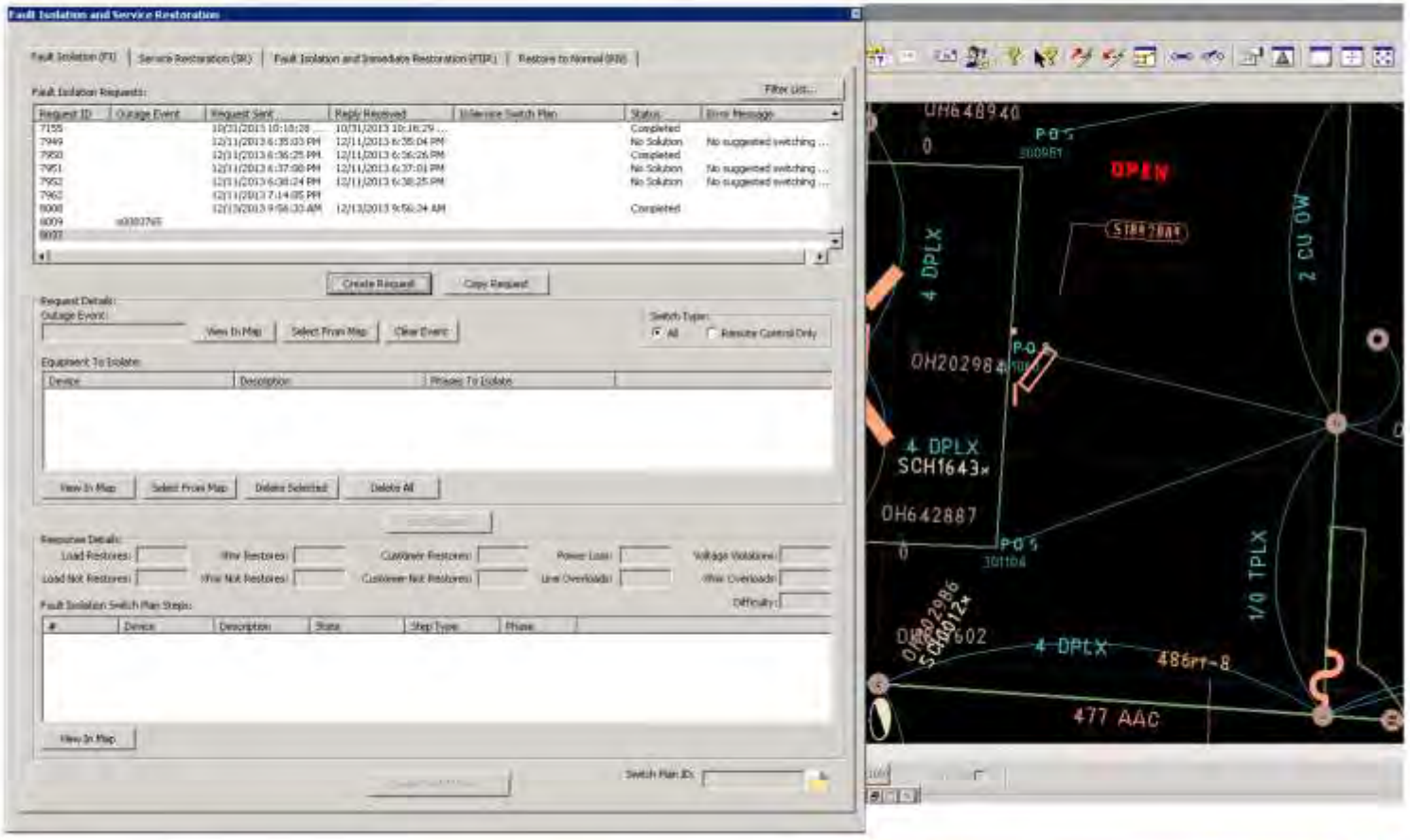
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

"Create Request" for Fault Isolation

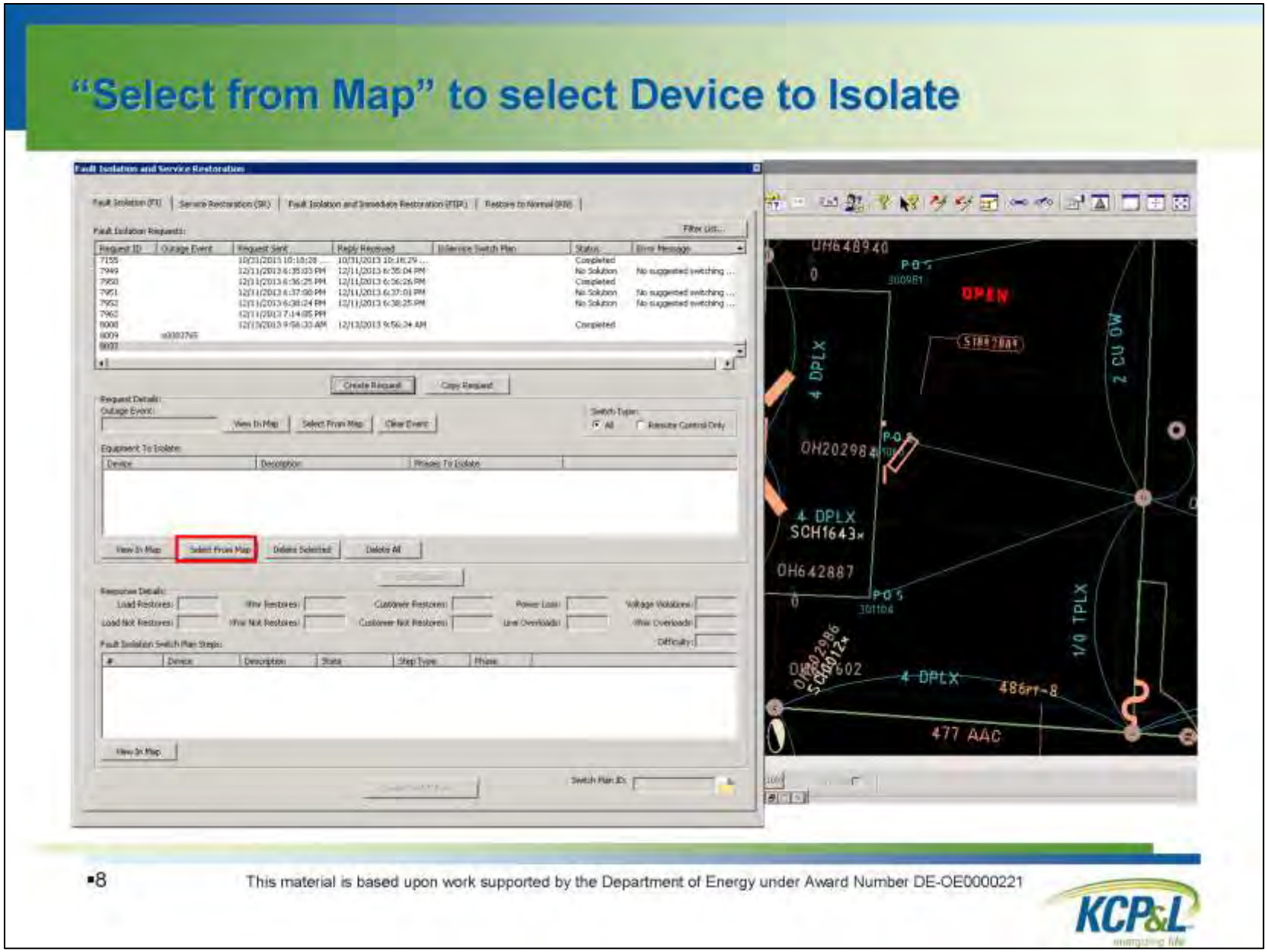


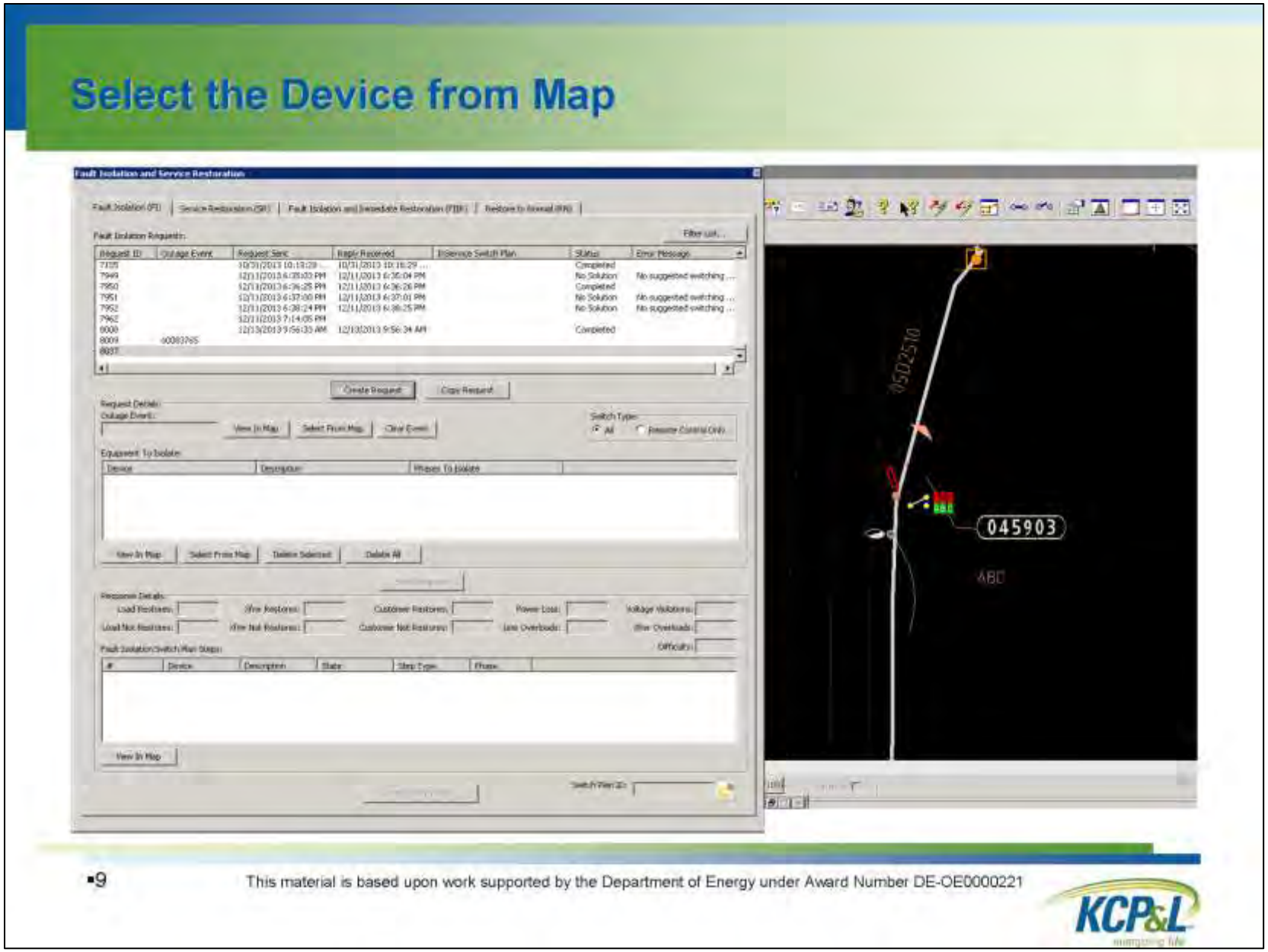
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

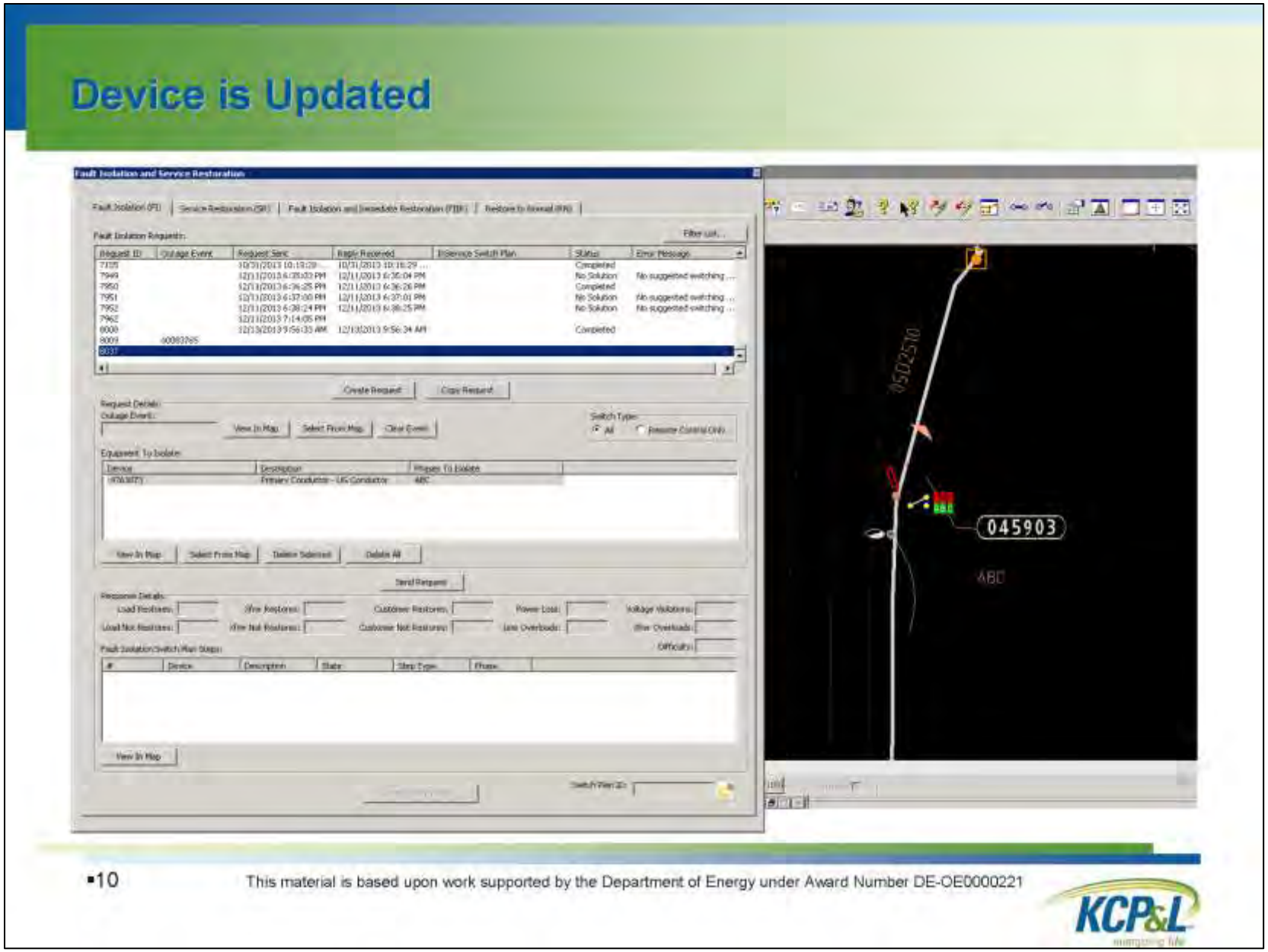
Request Created

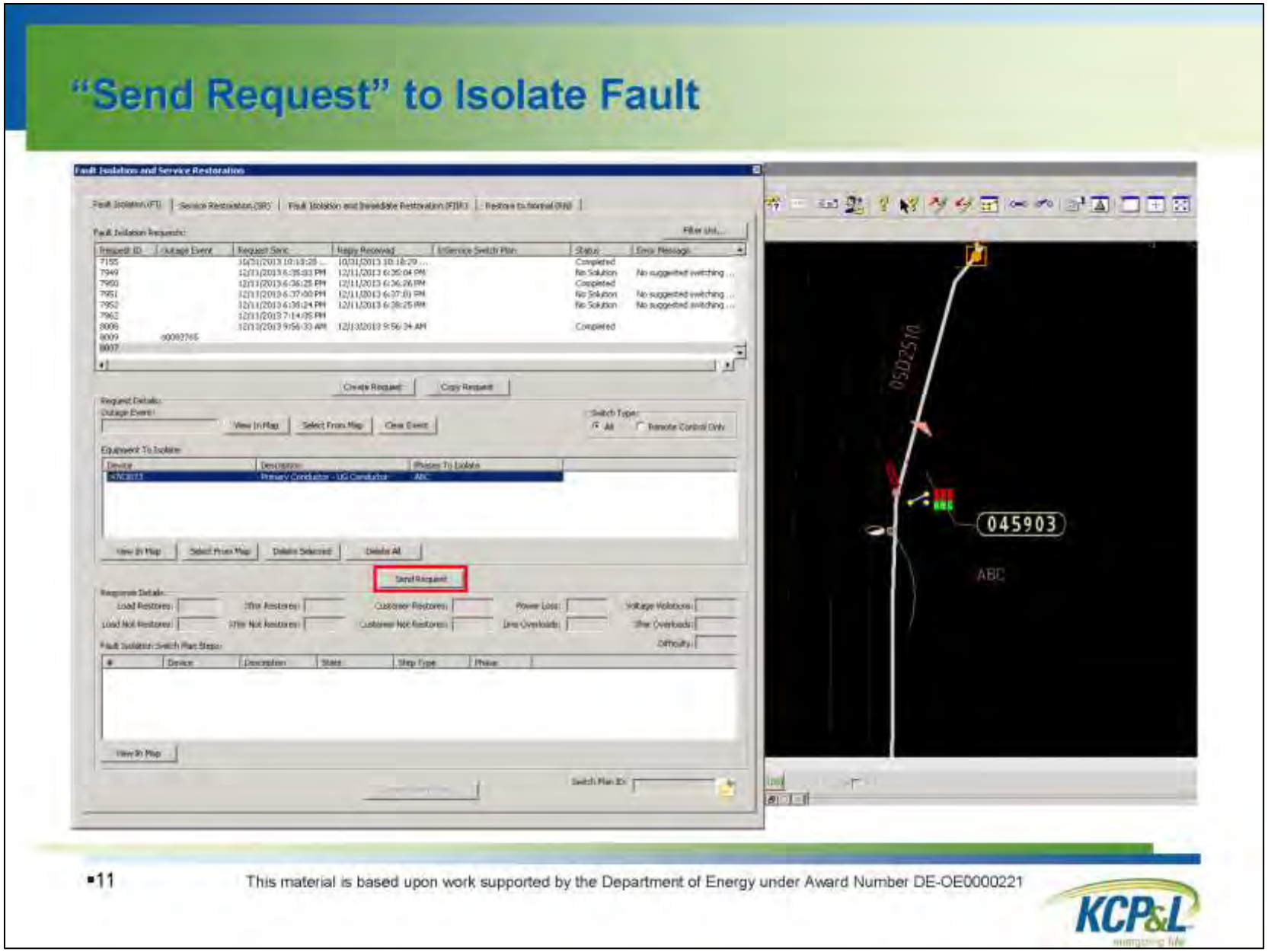


This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

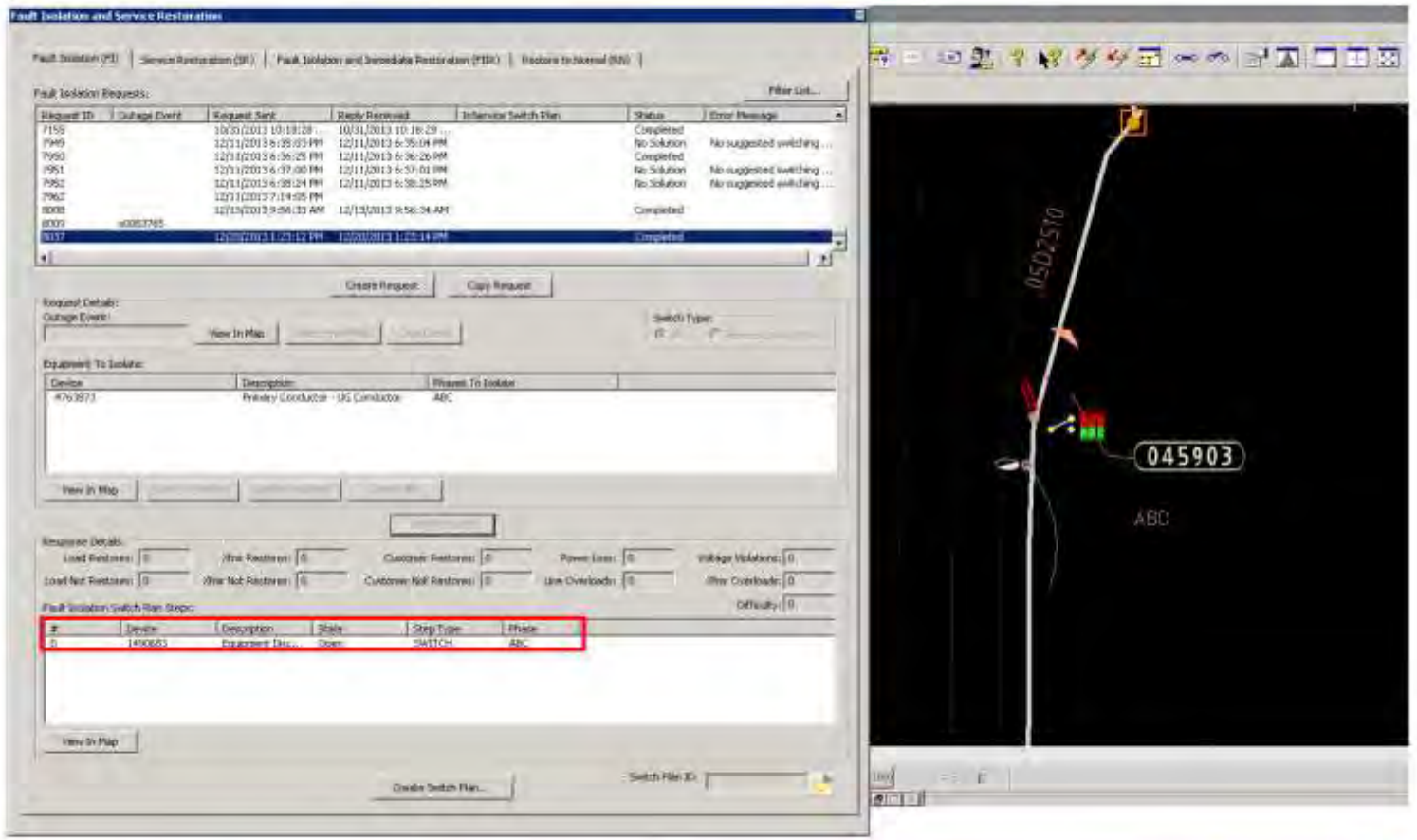

"Select from Map" to select Device to Isolate
Fault Isolation and Service Restoration
Fault Isolation Requests:
Request ID
Outage Event
Request Sent
Reply Received
Status
Error Message
Create Request
Copy Request
Request Details:
Outage Event:
View In Map
Select From Map
Clear Event
Switch Type:
All
Remote Control Only
Equipment To Isolate:
Device
Description
Phases To Isolate
View In Map
Select From Map
Delete Selected
Delete All
Response Details:
Load Restored:
Customer Restored:
Power Loss:
Voltage Violations:
Load Not Restored:
Customer Not Restored:
Line Overloads:
Fault Isolation Switch Plan Steps:
Step Type
Phase
View In Map
Switch Plan ID:
OH648940
OPEN
4 DPLX
2 CU OW
OH202984
4 DPLX
SCH1643
OH642887
1/0 TPLX
4 DPLX
486rr-8
477 AAC
8
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L
energizing life


Select the Device from Map
Fault Isolation and Service Restoration
045903
ABC
9
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L


Device is Updated
Fault Isolation and Service Restoration
045903
ABC
10
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

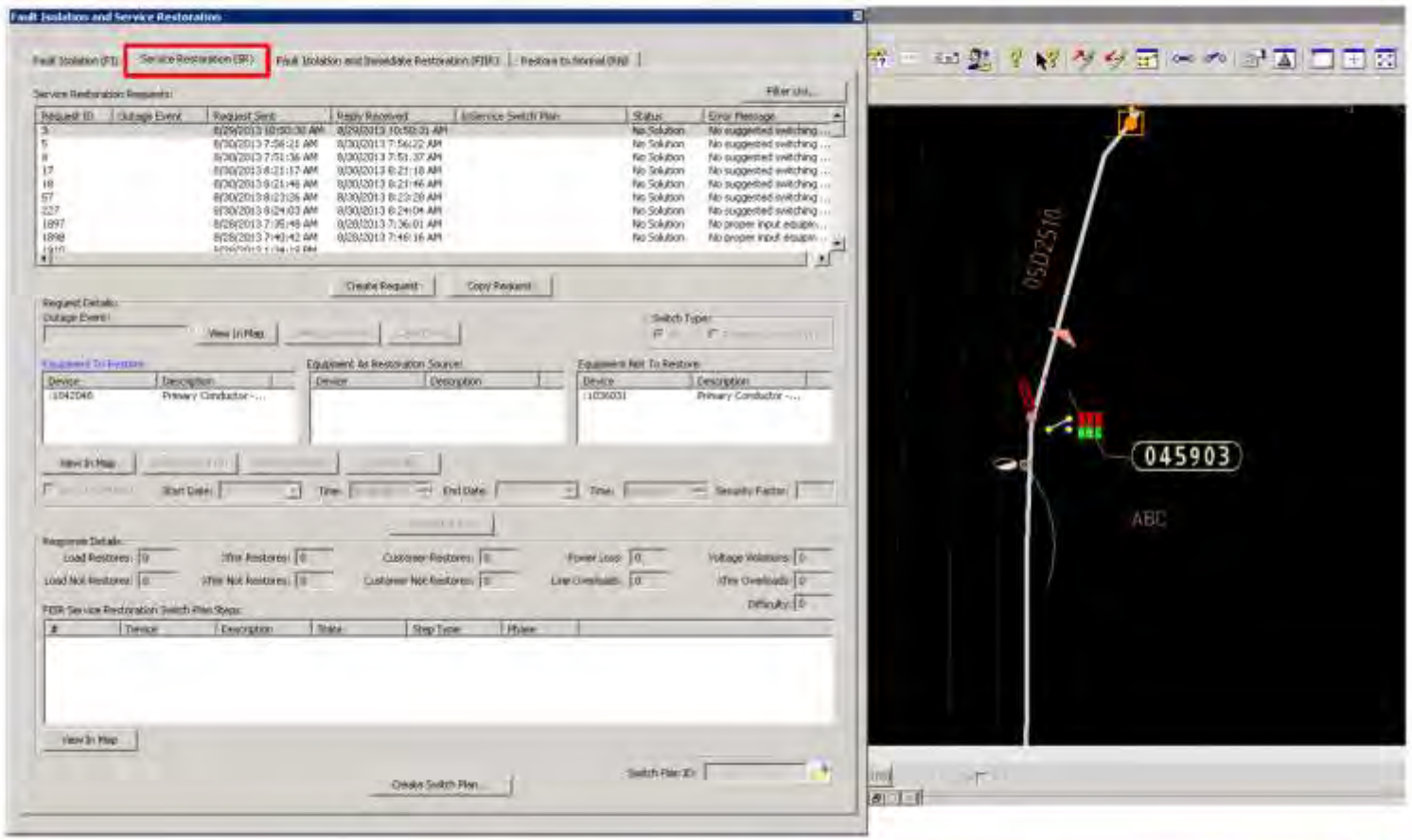

"Send Request" to Isolate Fault
Fault Isolation and Service Restoration
045903
ABC
11
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

Fault Isolation Results

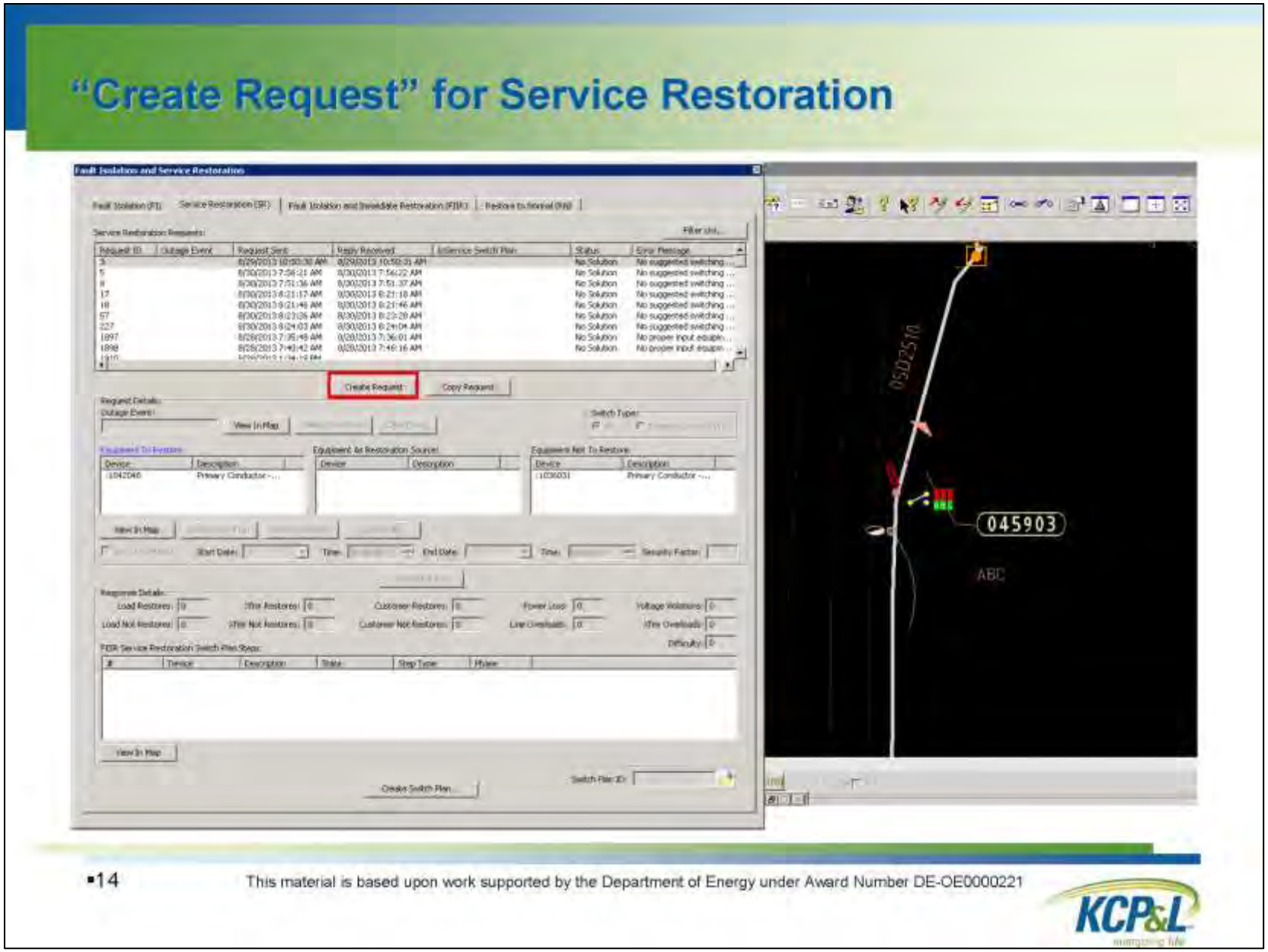


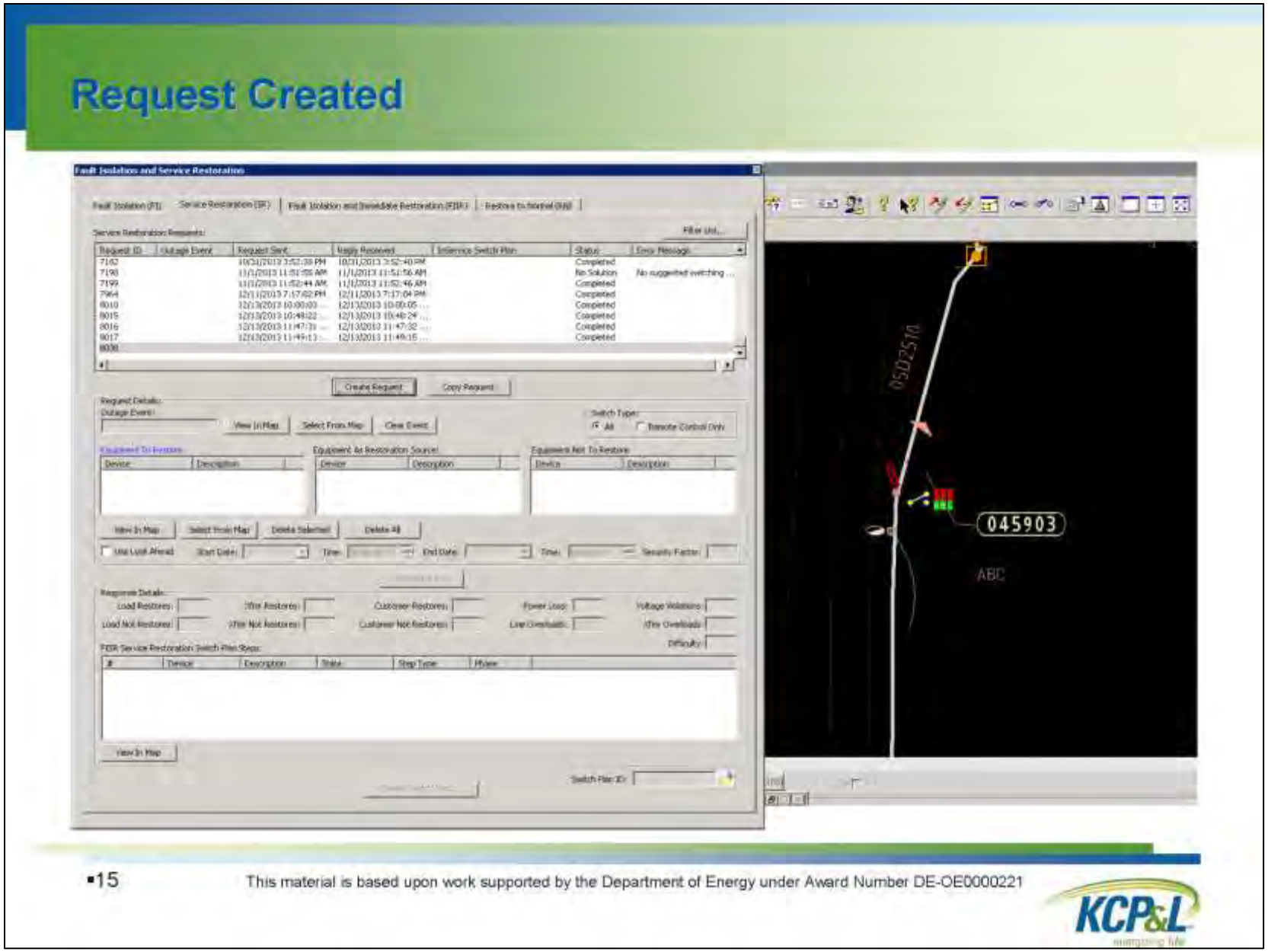
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

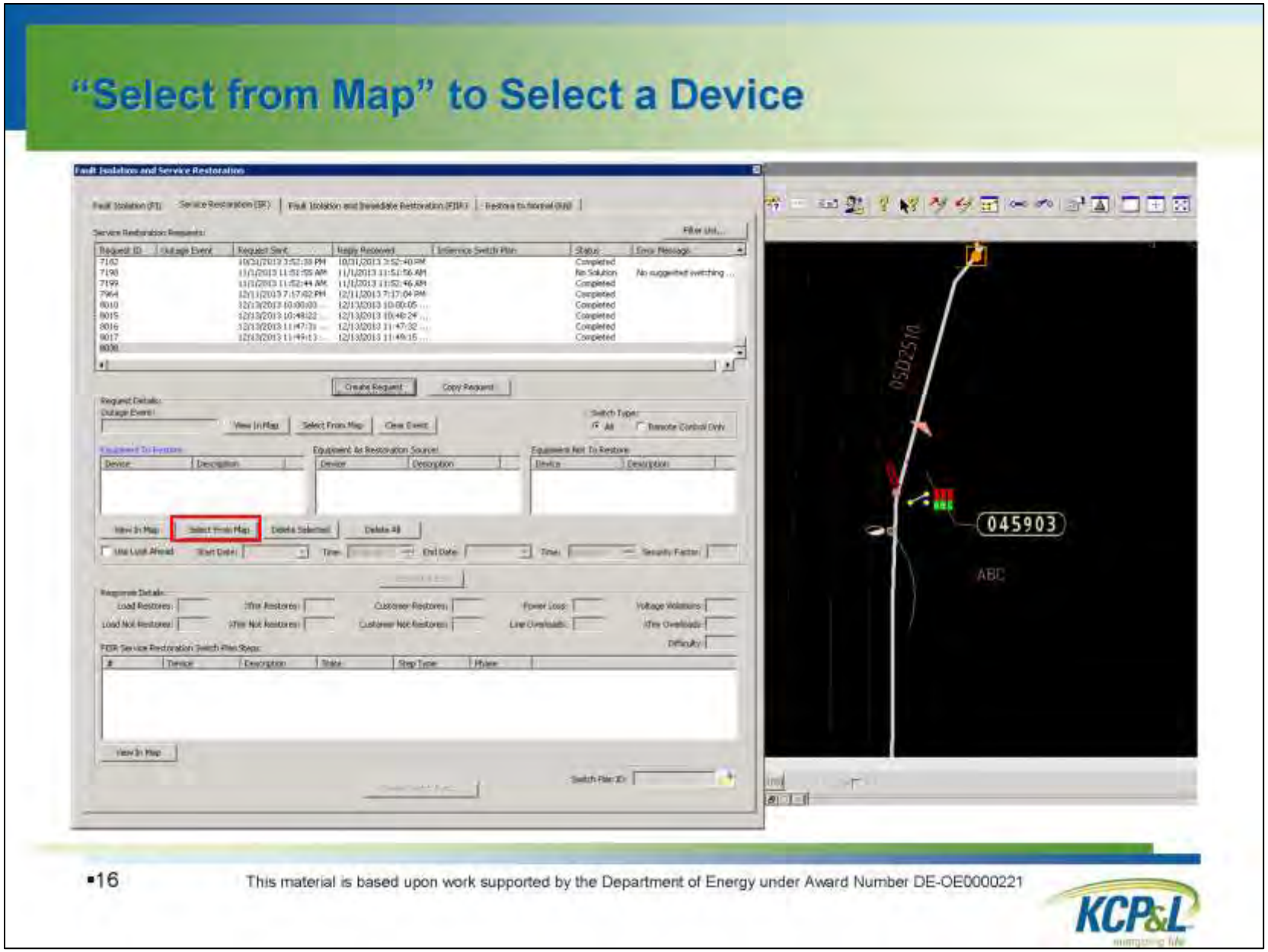
Open "Service Restoration" to Restore Faulted Device

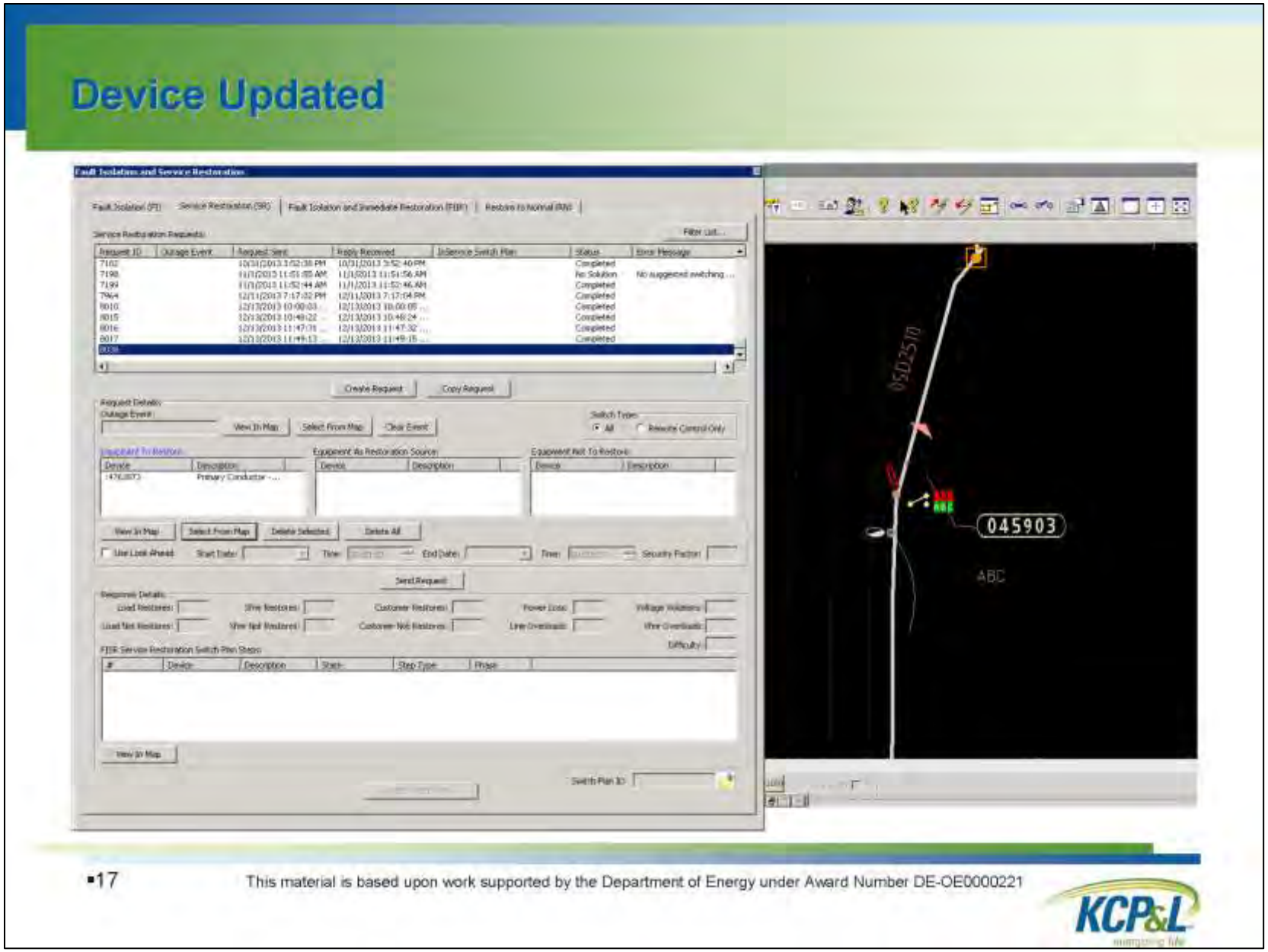


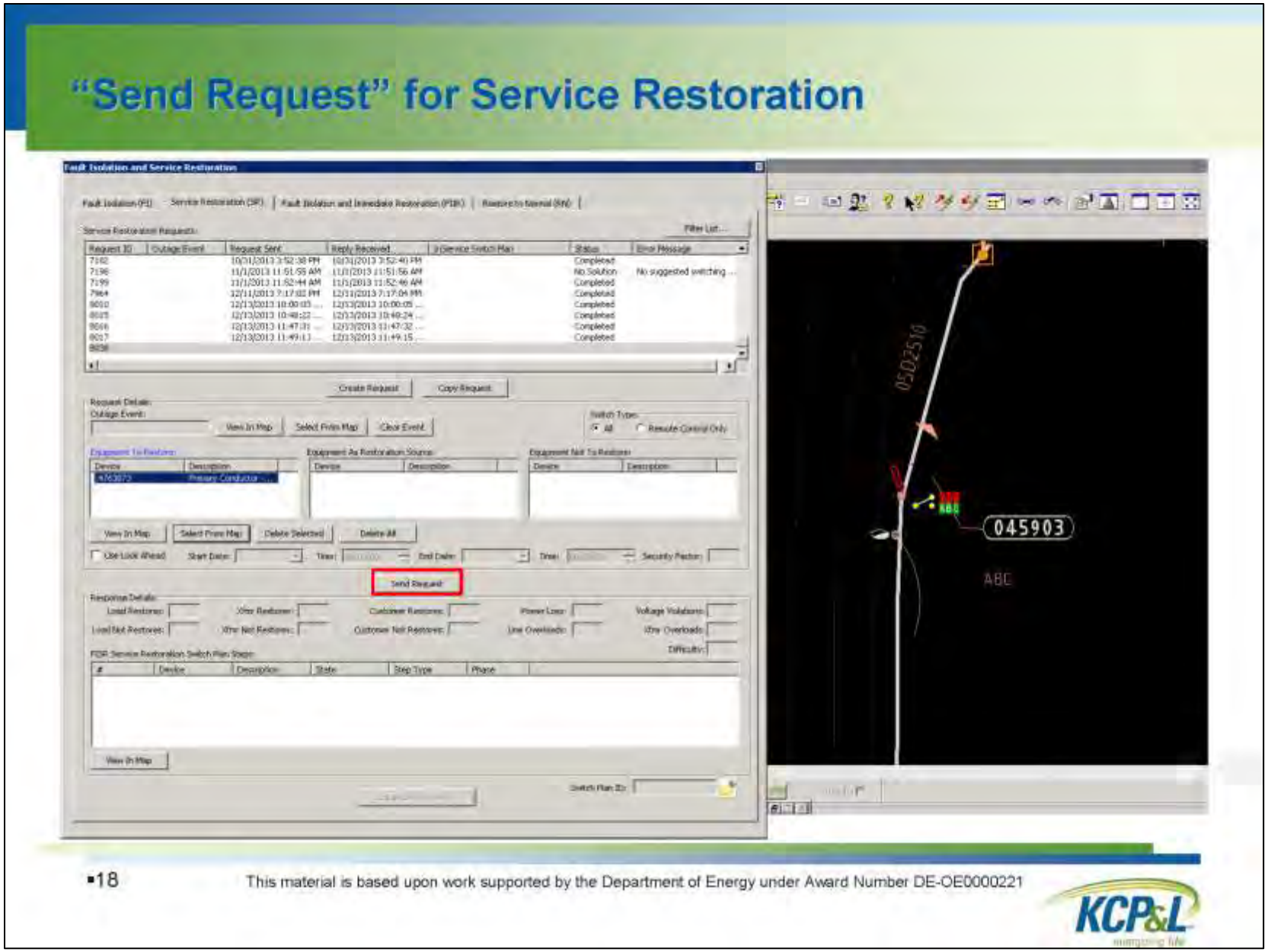
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

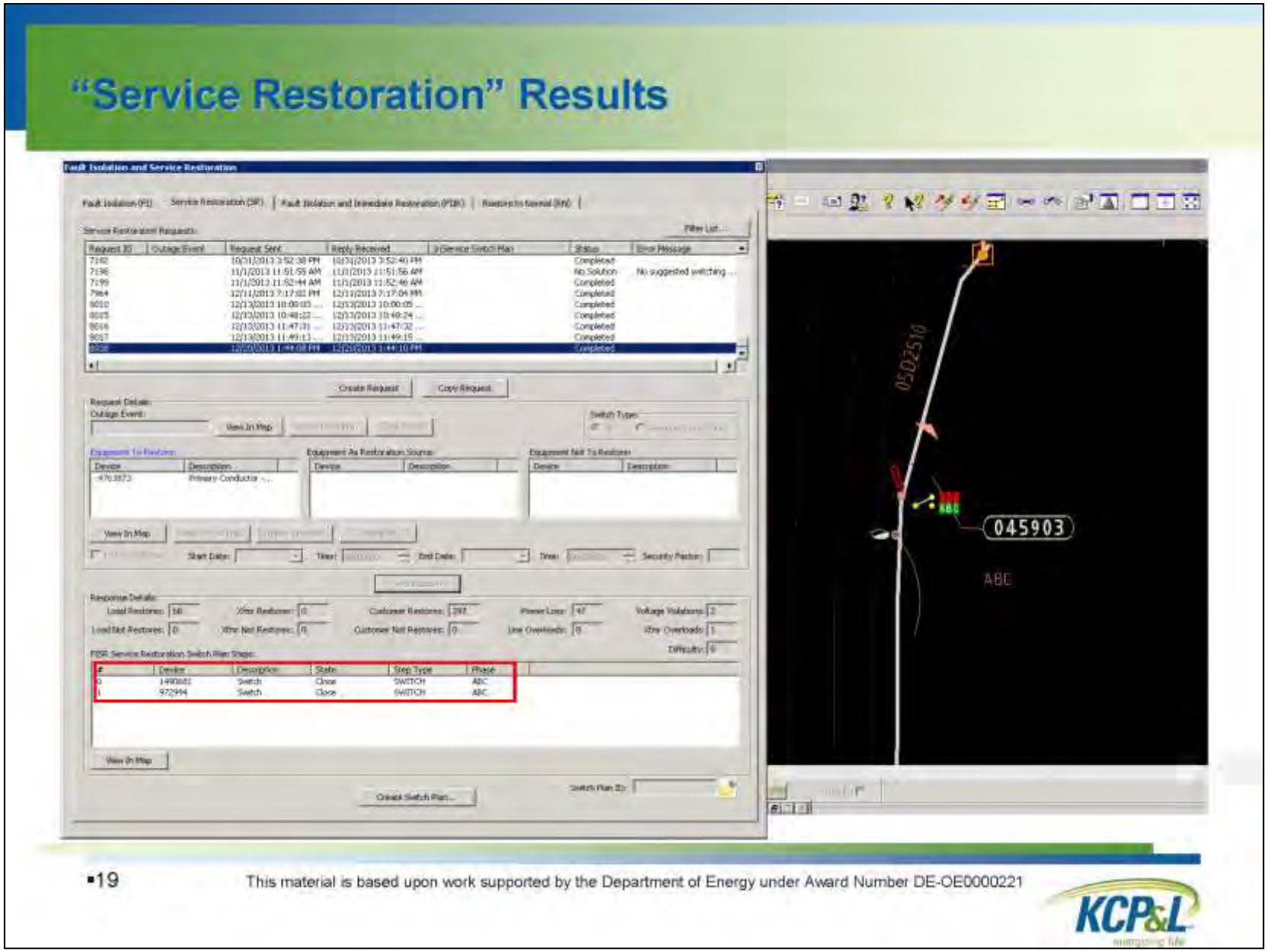

"Create Request" for Service Restoration
Fault Isolation and Service Restoration
Create Request
Copy Request
045903
ABC
14
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L


Request Created
Fault Isolation and Service Restoration
045903
ABC
15
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L


"Select from Map" to Select a Device
Fault Isolation and Service Restoration
Create Request
Copy Request
Select From Map
Delete Selected
Delete All
045903
ABC
16
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

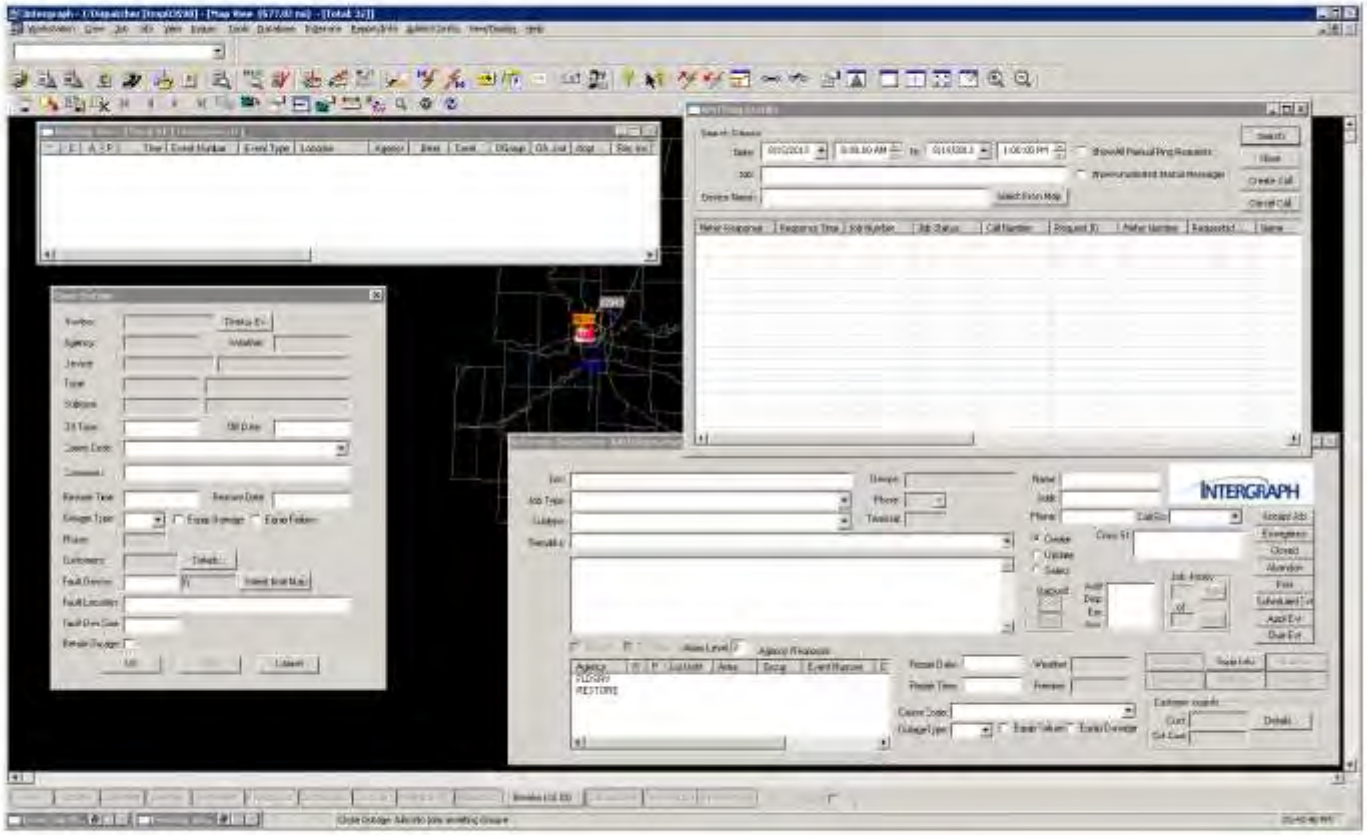

Device Updated
Fault Isolation and Service Restoration
045903
ABC
17
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L
energizing life


"Send Request" for Service Restoration
Fault Isolation and Service Restoration
Create Request
Copy Request
Send Request
045903
ABC
18
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L


"Service Restoration" Results
045903
ABC
19
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L


Outage and Restoration Events
- KC Green Impact Zone Initiative
- DOE Regional SmartGrid Demonstration Program
- EPRI SmartGrid Demonstration Program
KCP&L
SmartGrid
the future of energy

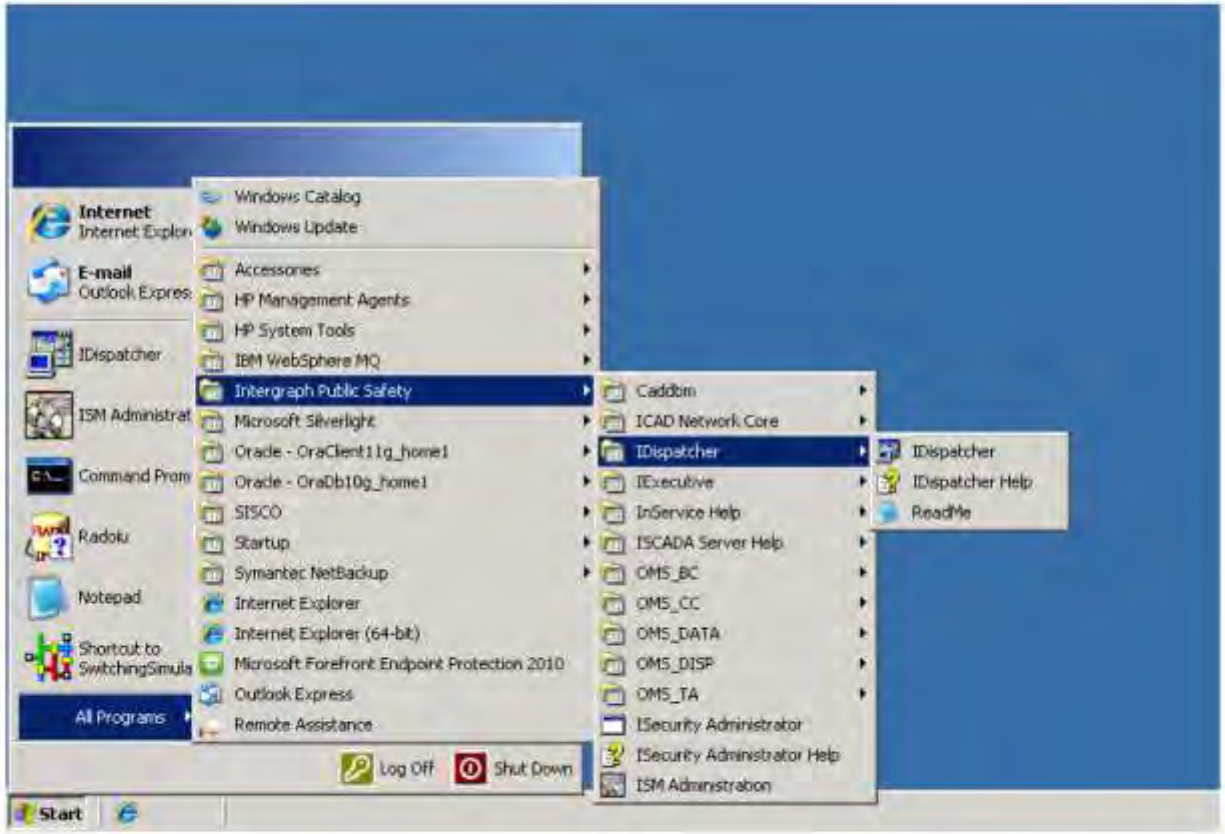
Windows Used for Outage and Restoration



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

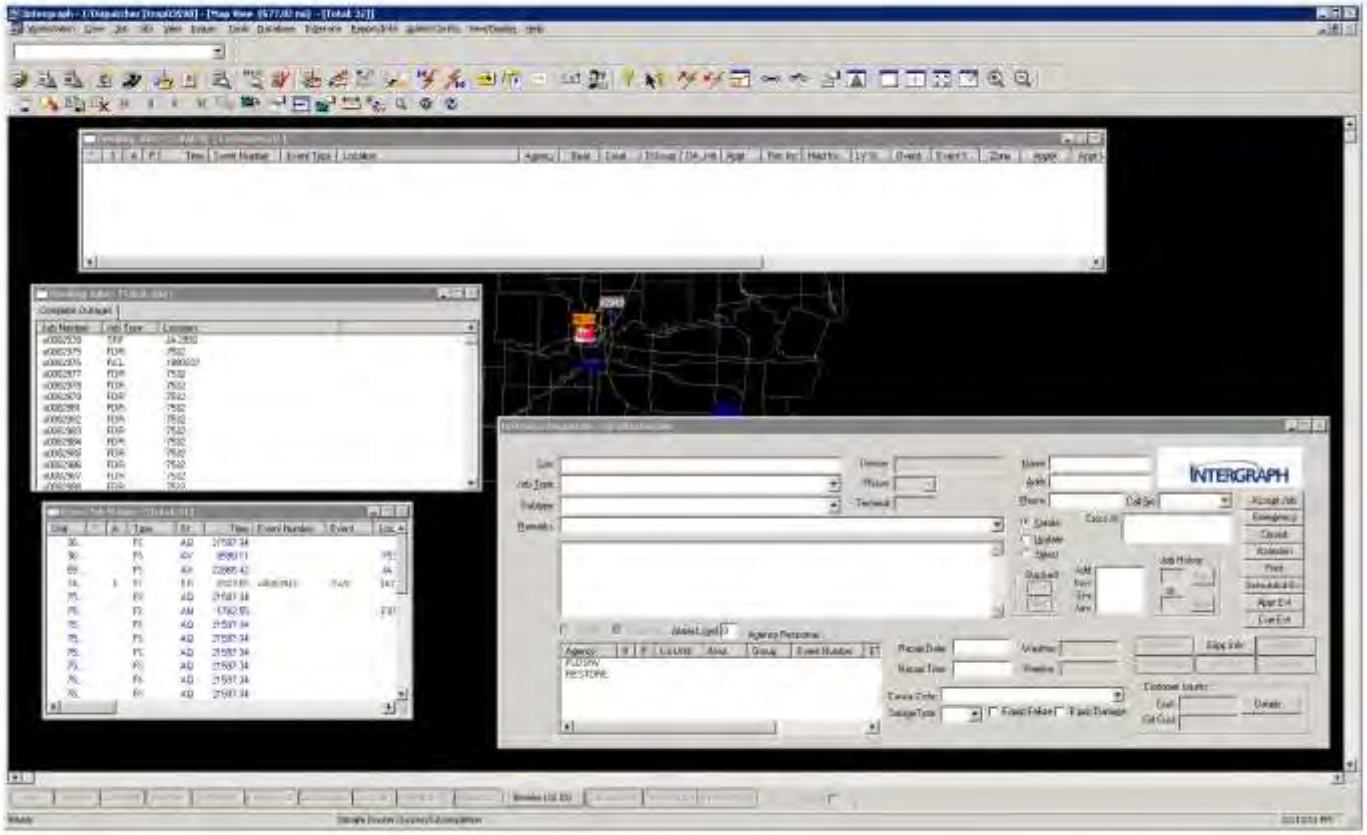
KCP&L energizing life

Launch InService I/Dispatcher



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

InService I/Dispatcher Main Screen

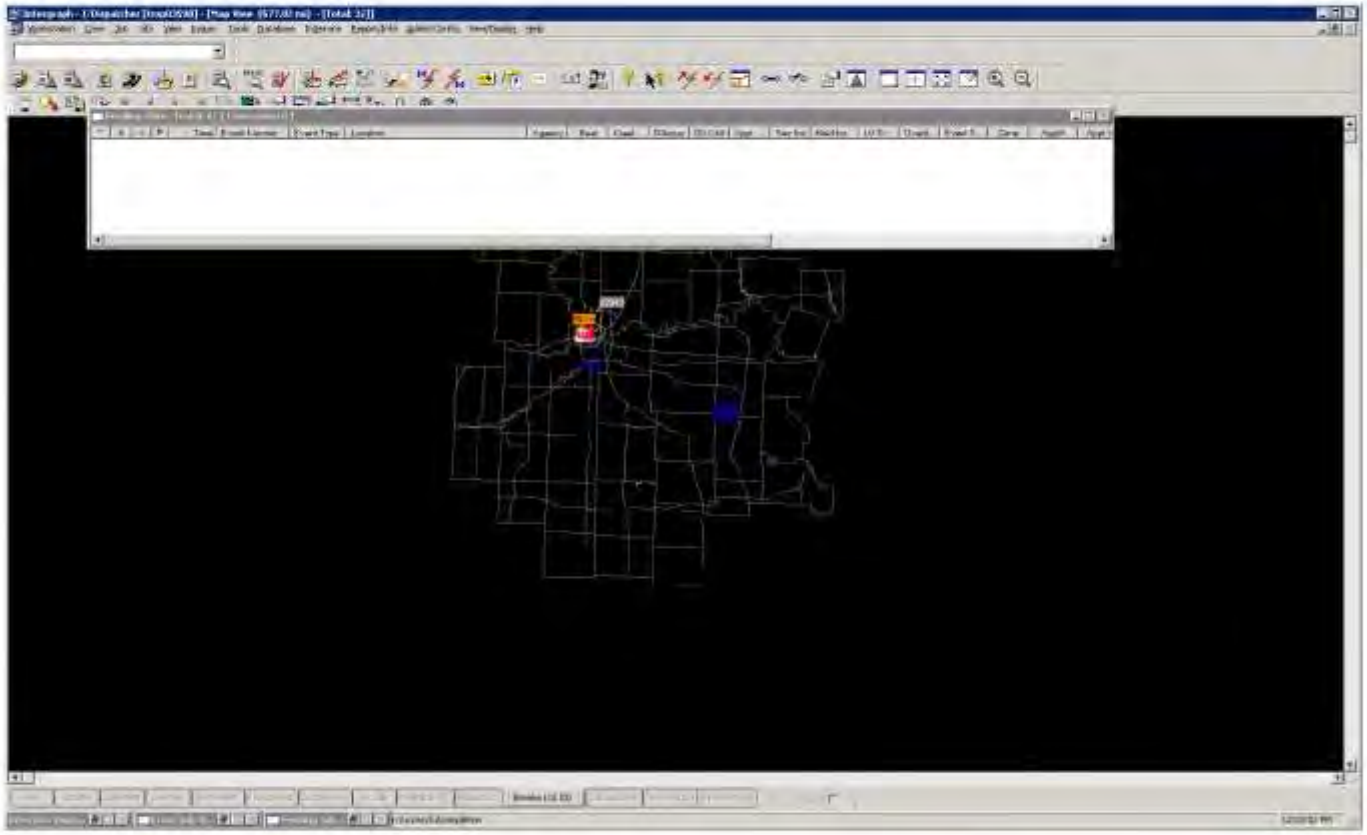


▪4

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

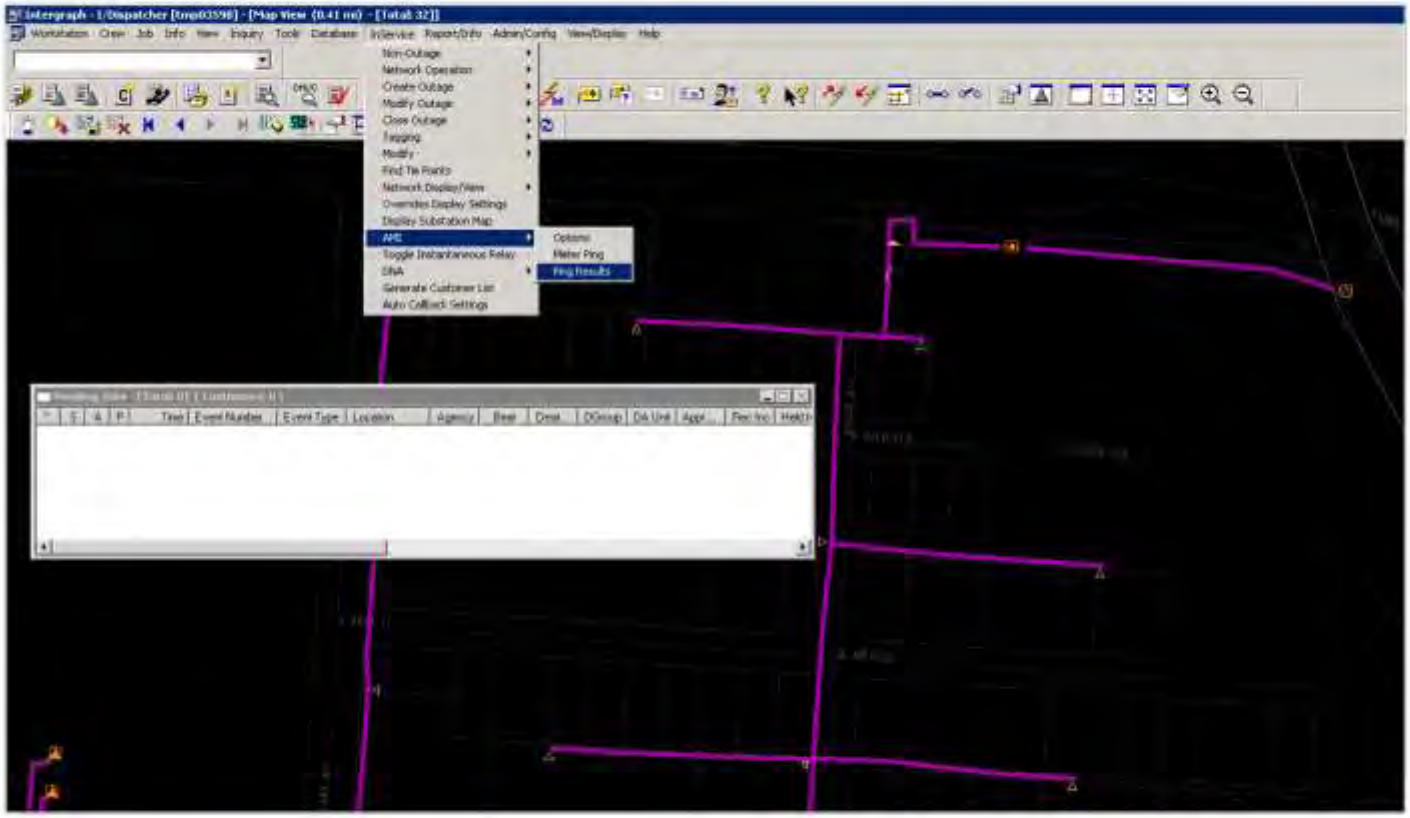
KCP&L energizing life

"Pending Jobs" Window



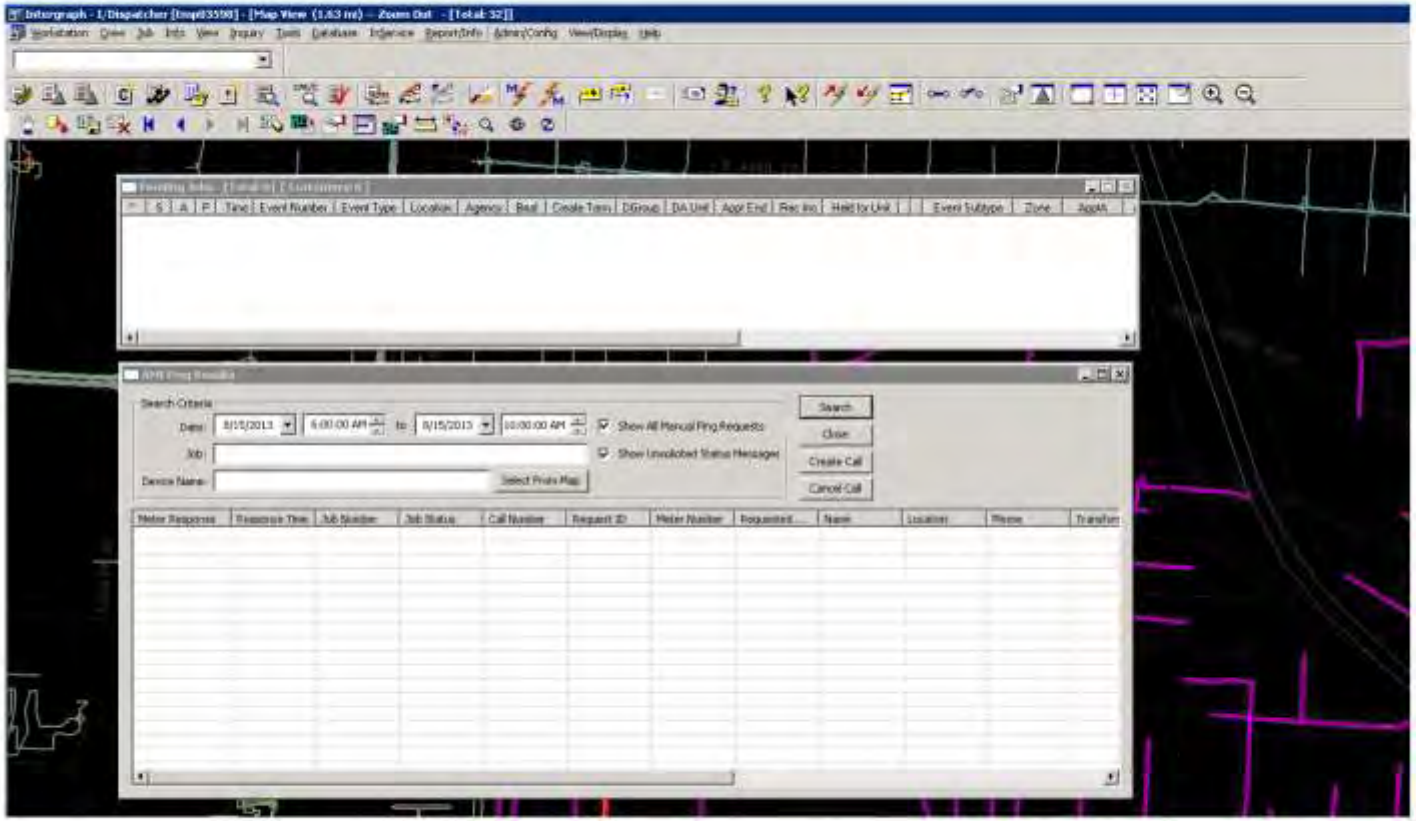
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Open the "AMI Ping Results" Window



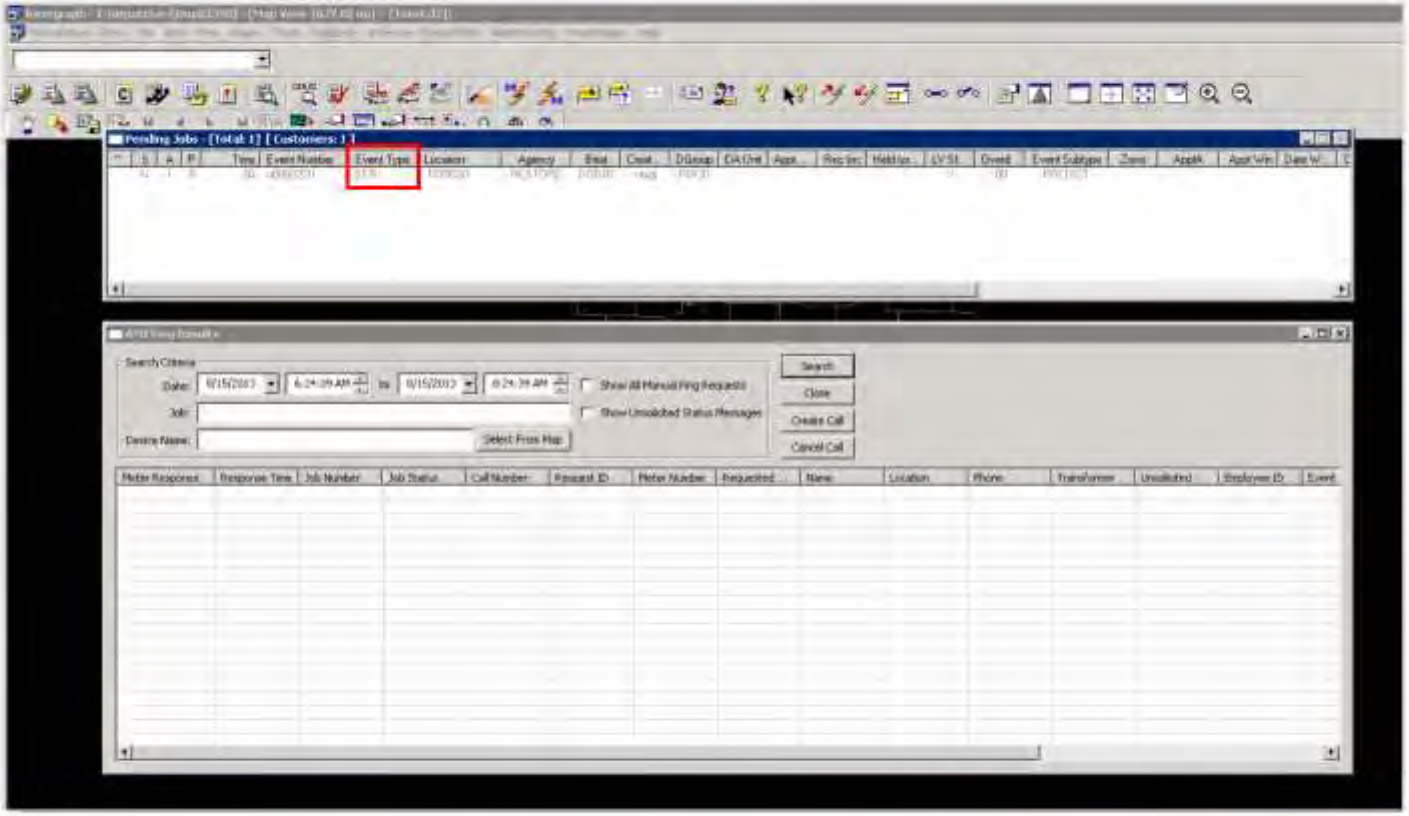
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

"AMI Ping Results" and "Pending Jobs" Window



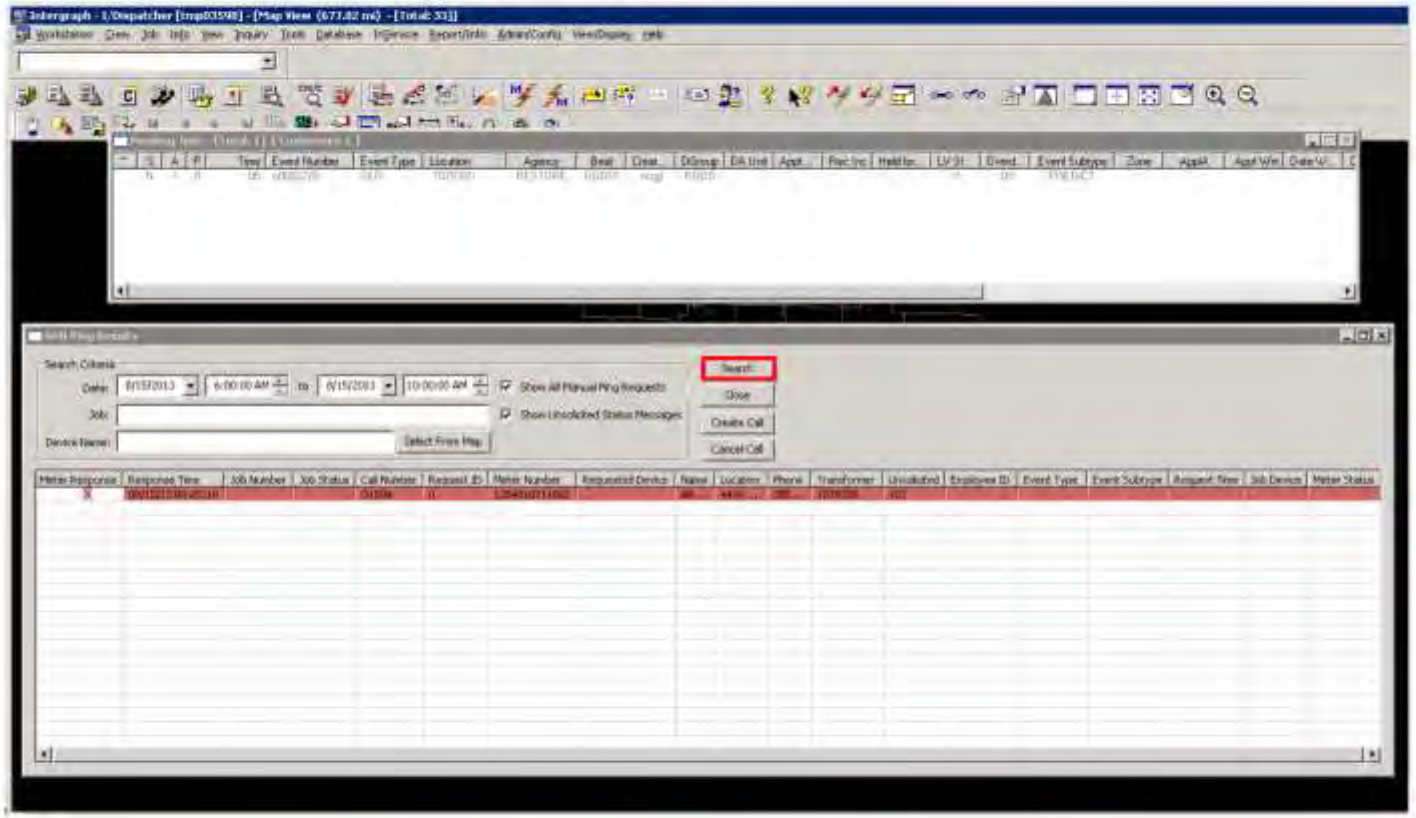
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Service-Level Outage in "Pending Jobs" Window



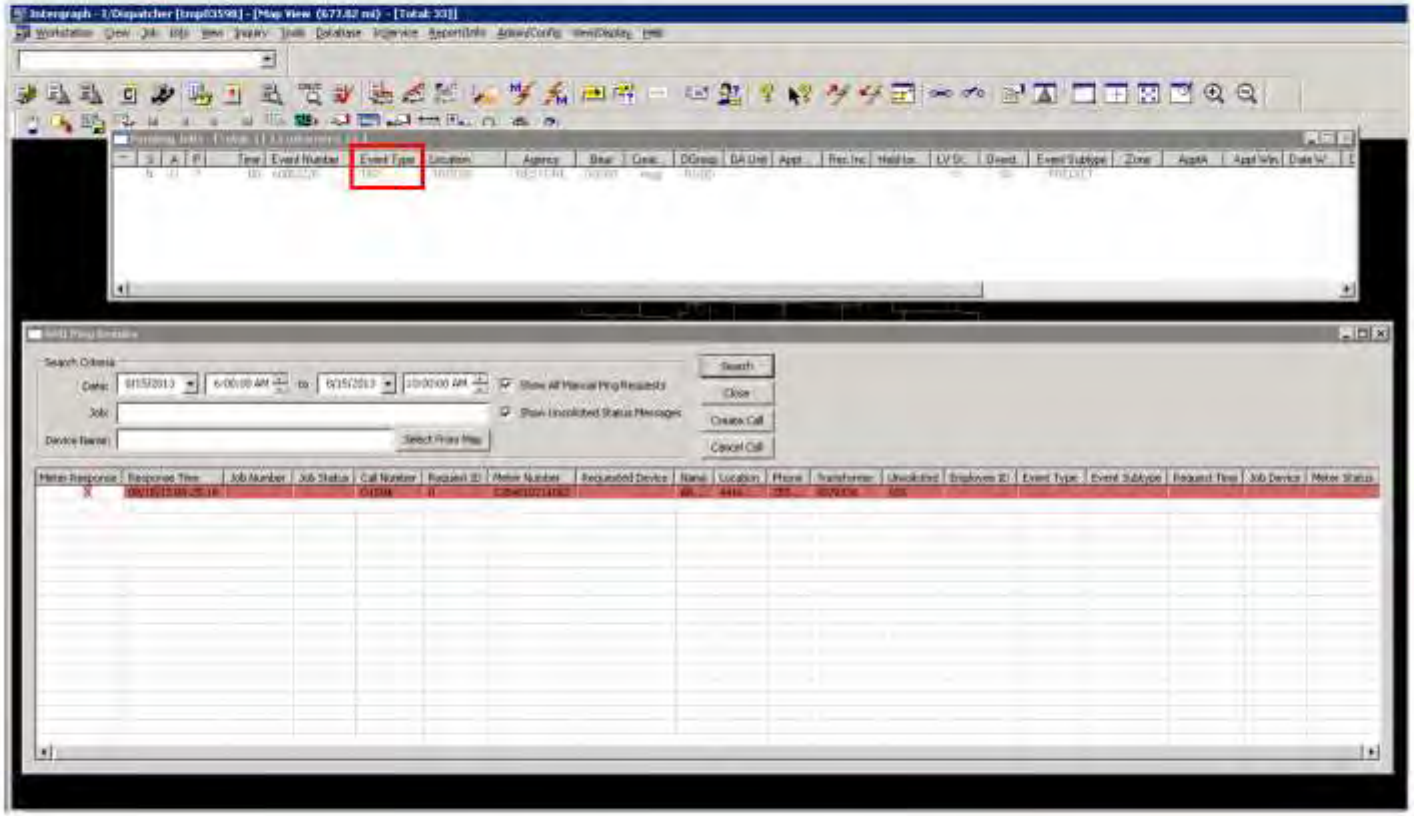
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Search in "AMI Ping Results" for Outage Information



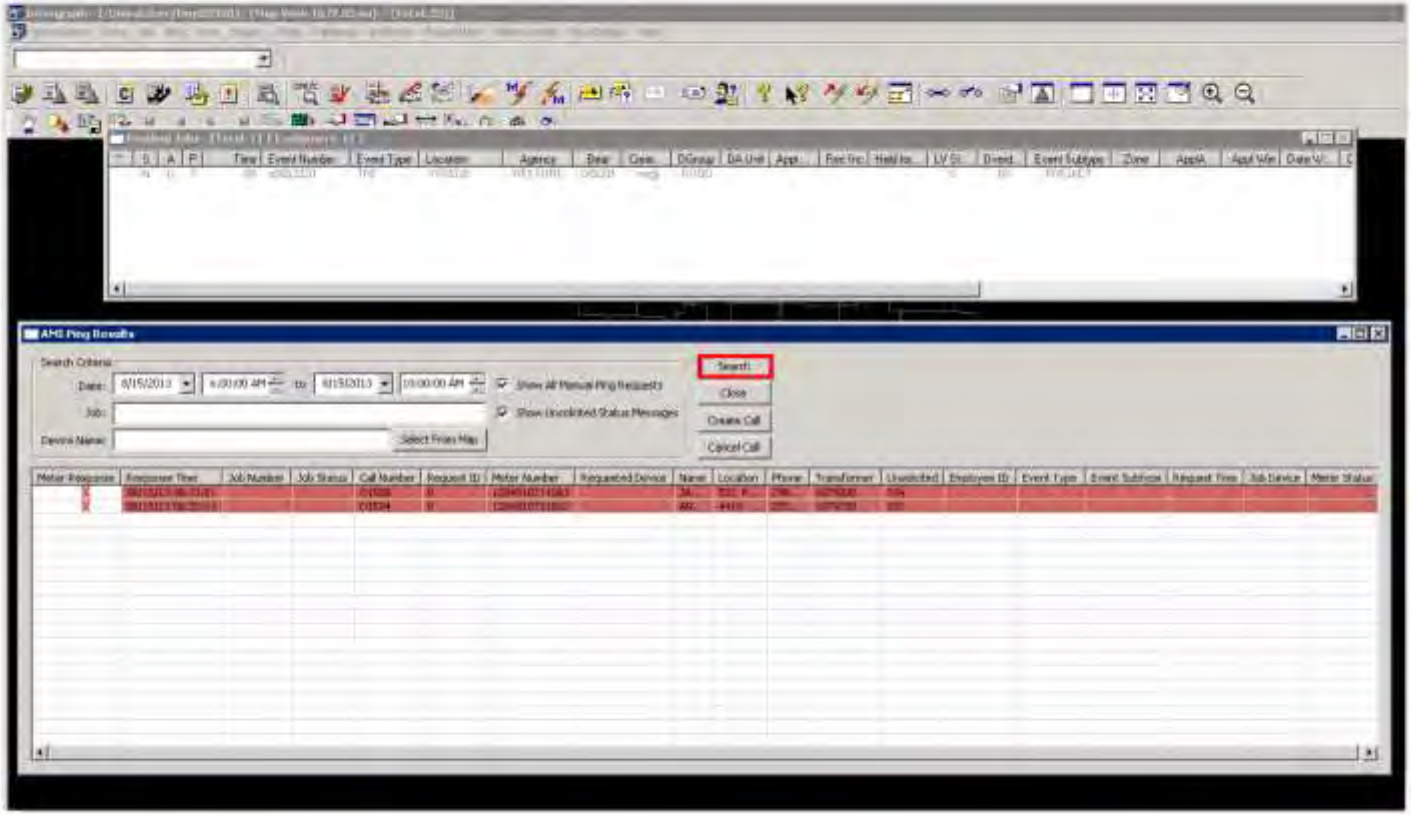
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Transformer-Level Outage in "Pending Jobs" Window



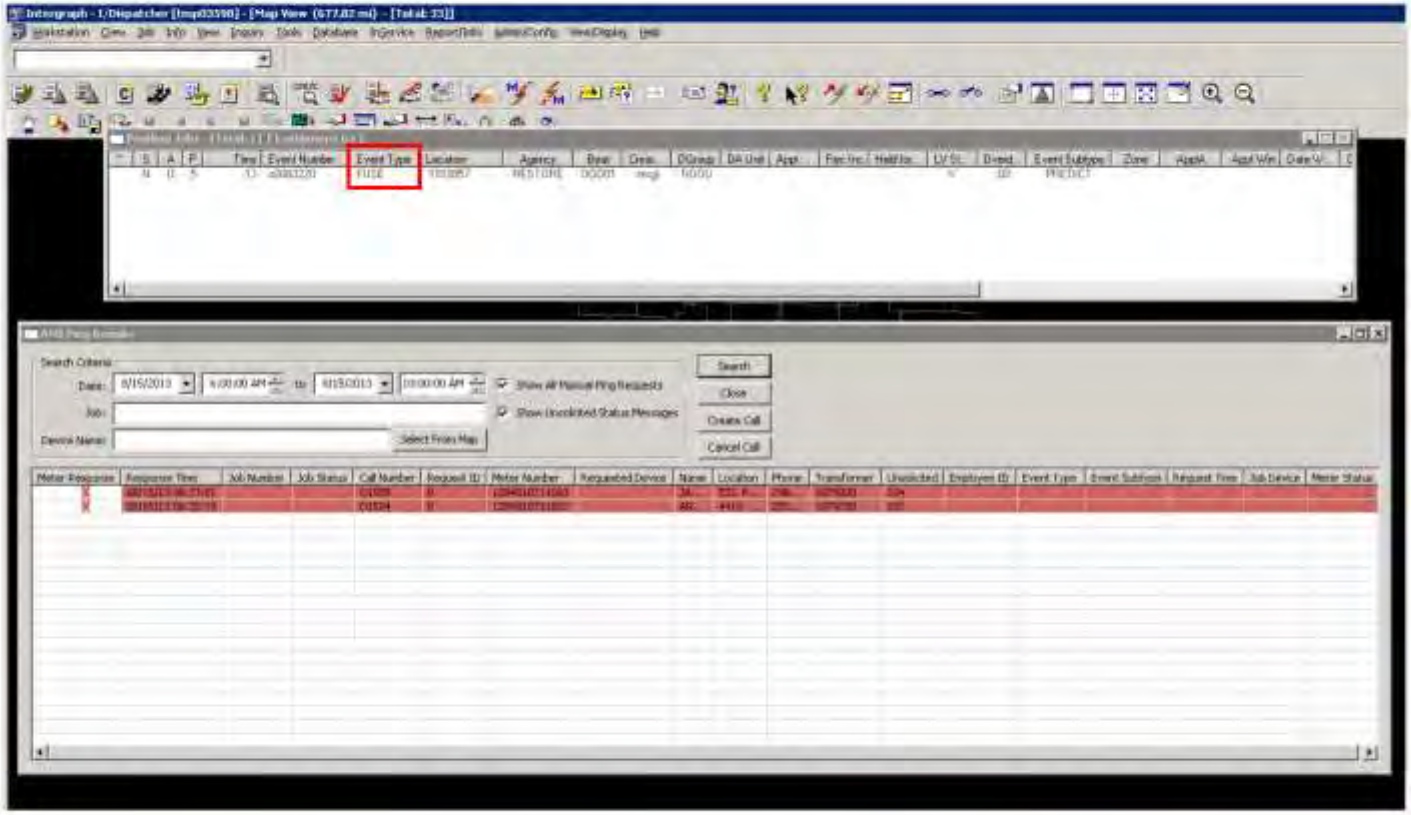
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Search in "AMI Ping Results" for Outage Information



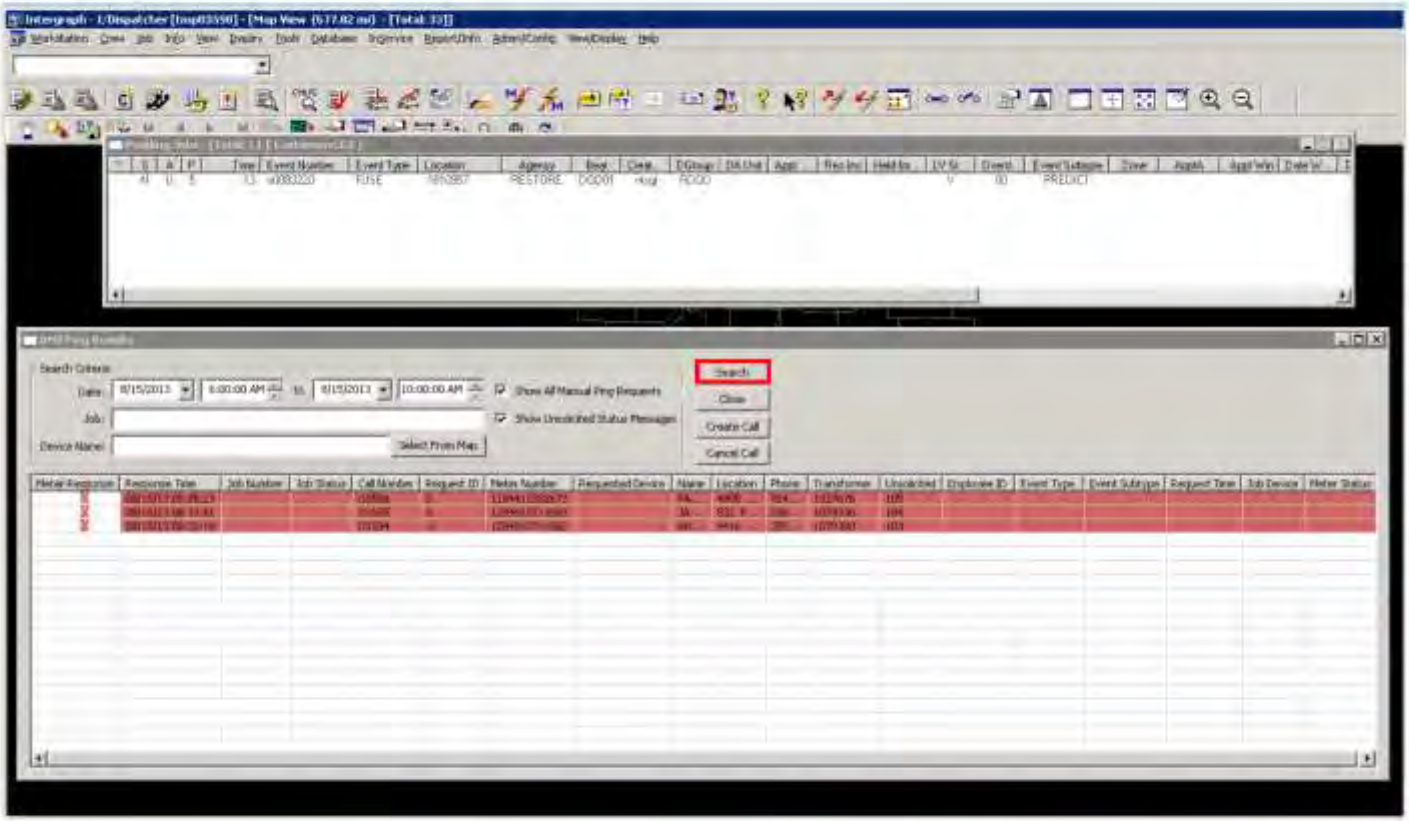
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Fuse-Level Outage in "Pending Jobs" Window



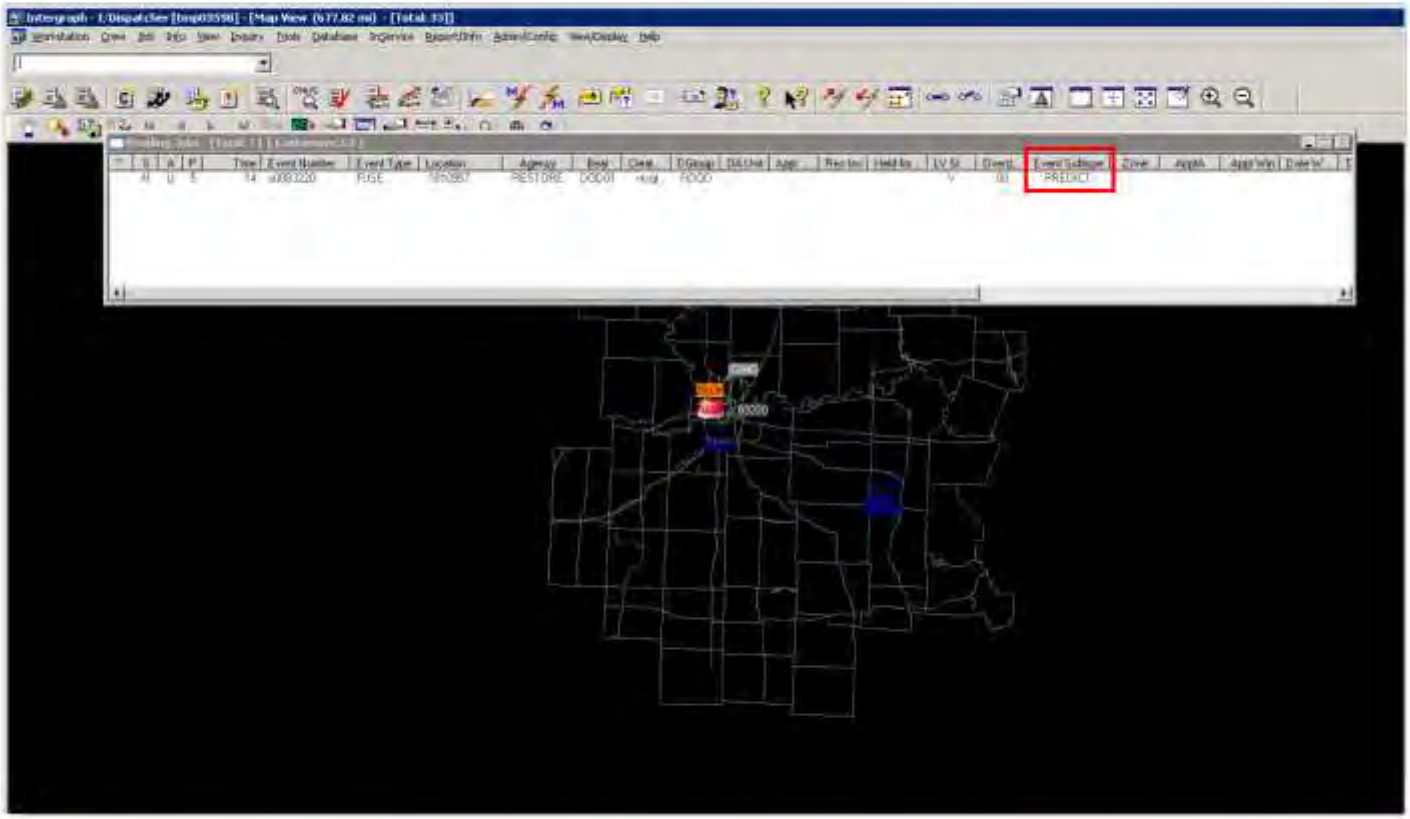
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Search in "AMI Ping Results" for Outage Information



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

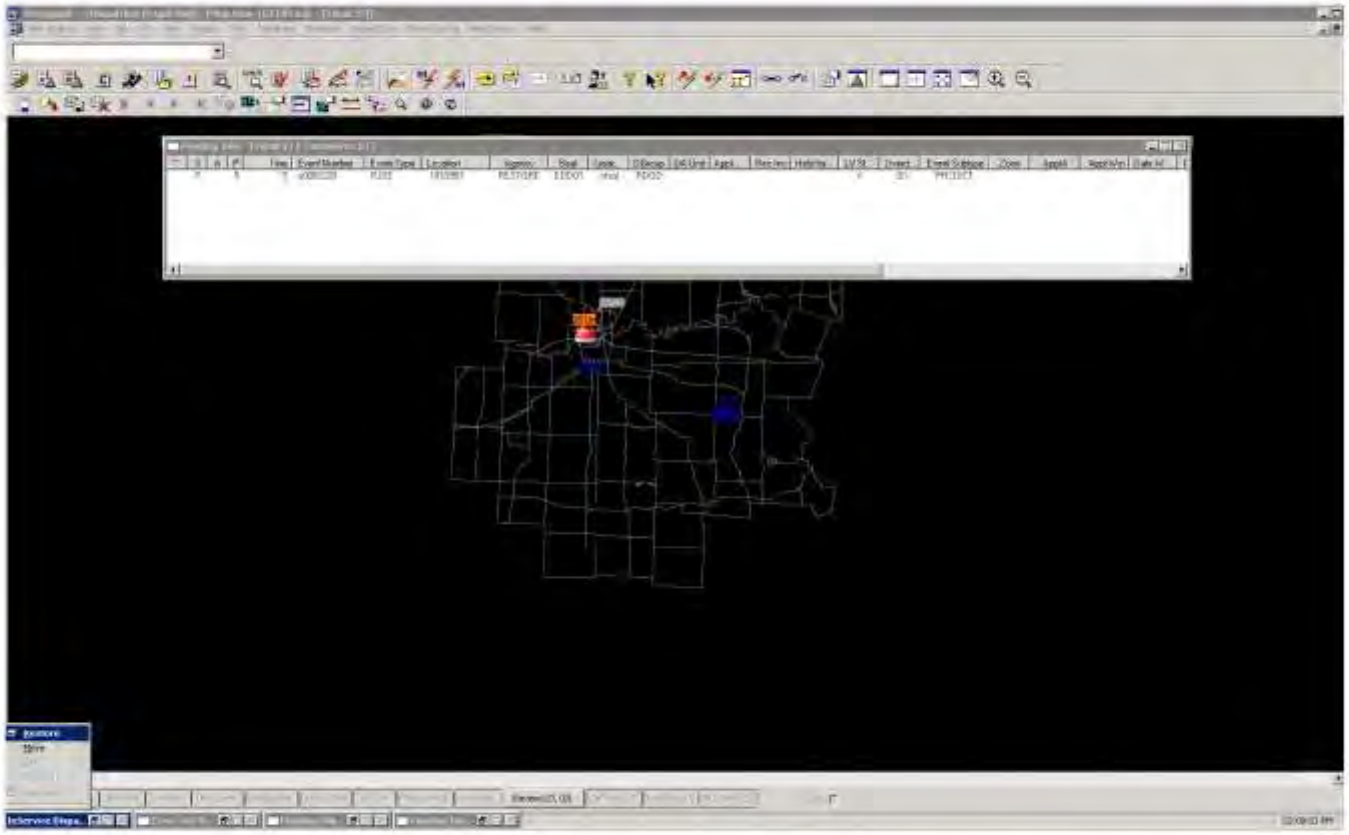
Confirm the Outage



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

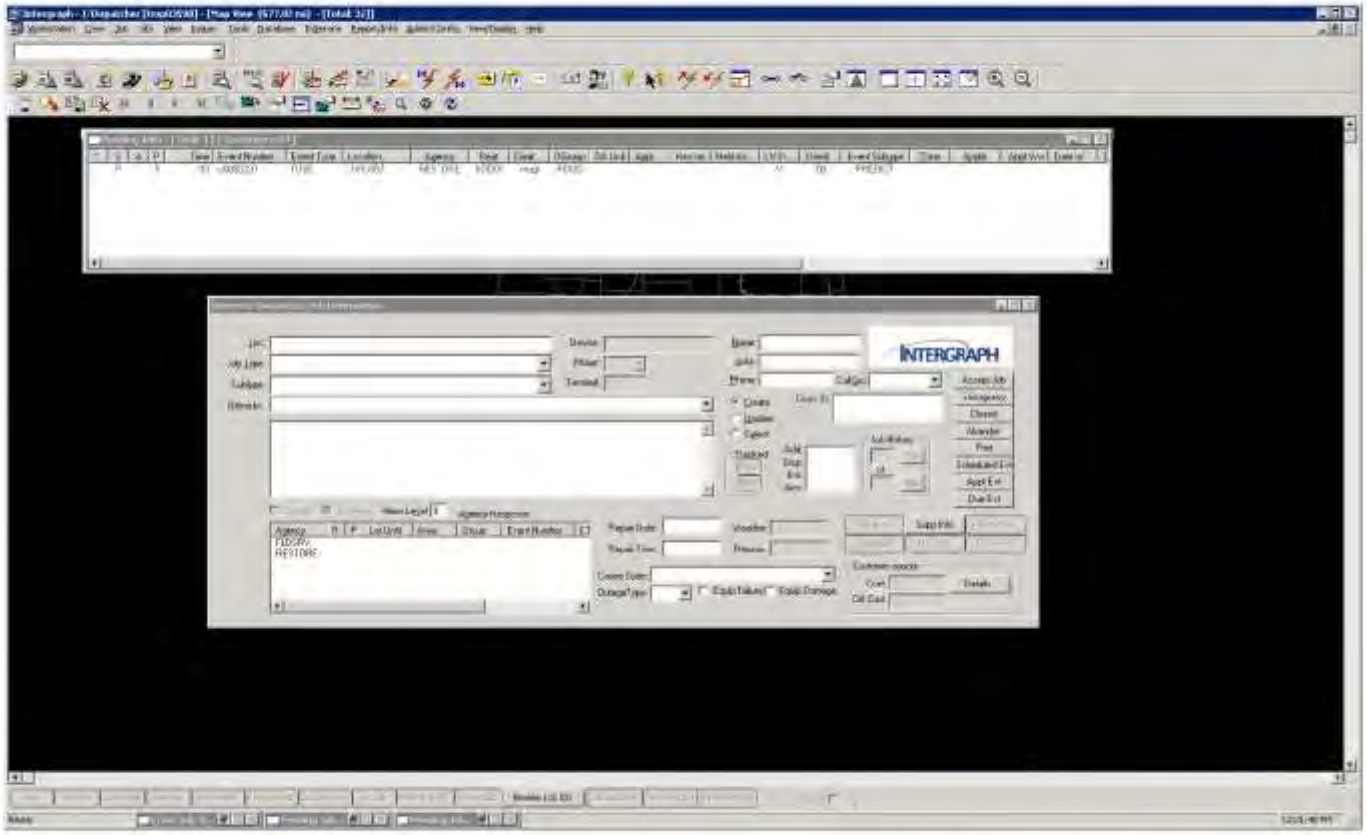
KCP&L energizing life

Restore "InService Dispatcher Job Information" Window



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

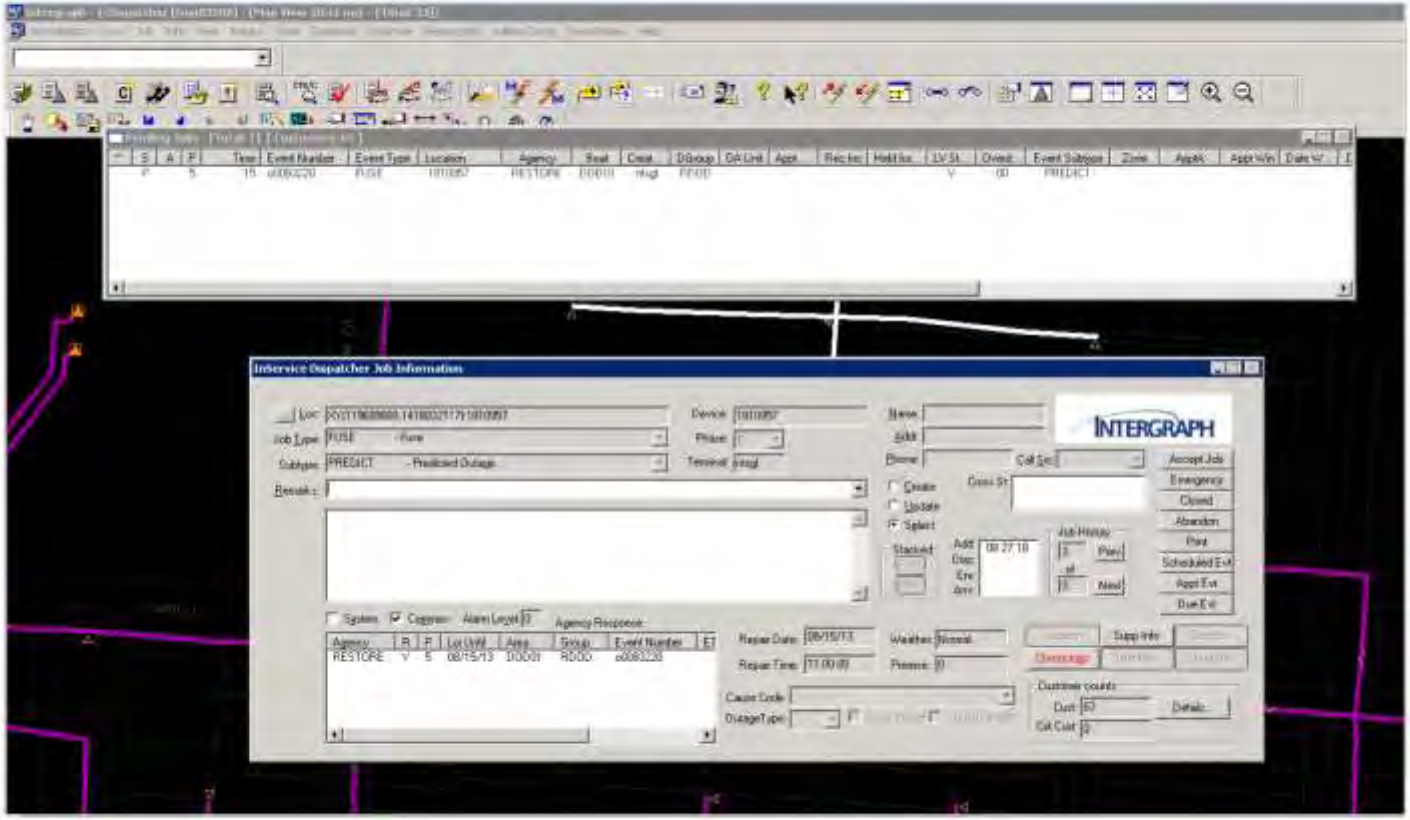
Select the Job in "Pending Jobs" Window



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

KCP&L energizing life

Fields in "InService Dispatcher Job Information" Window

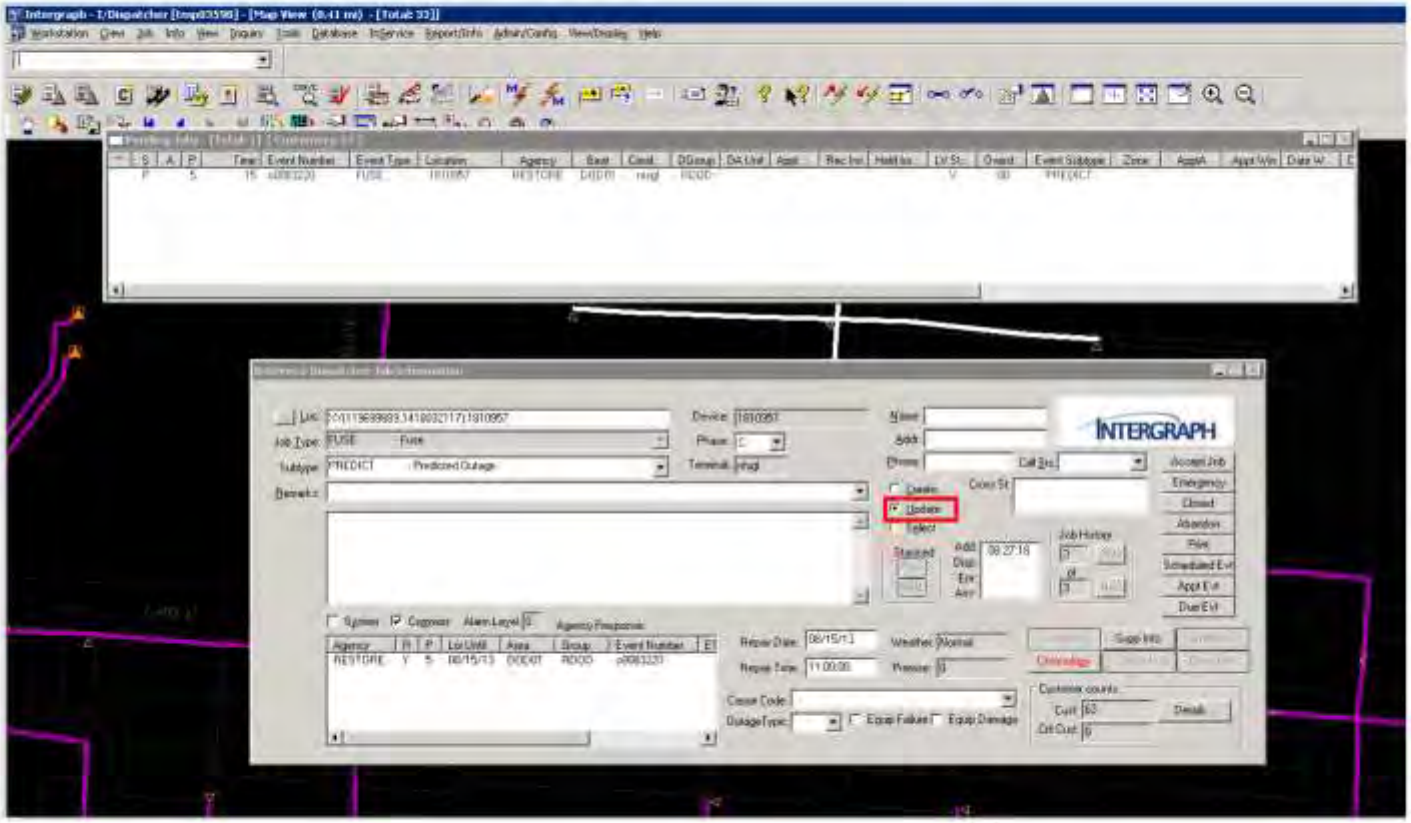


▪17

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

KCP&L energizing life

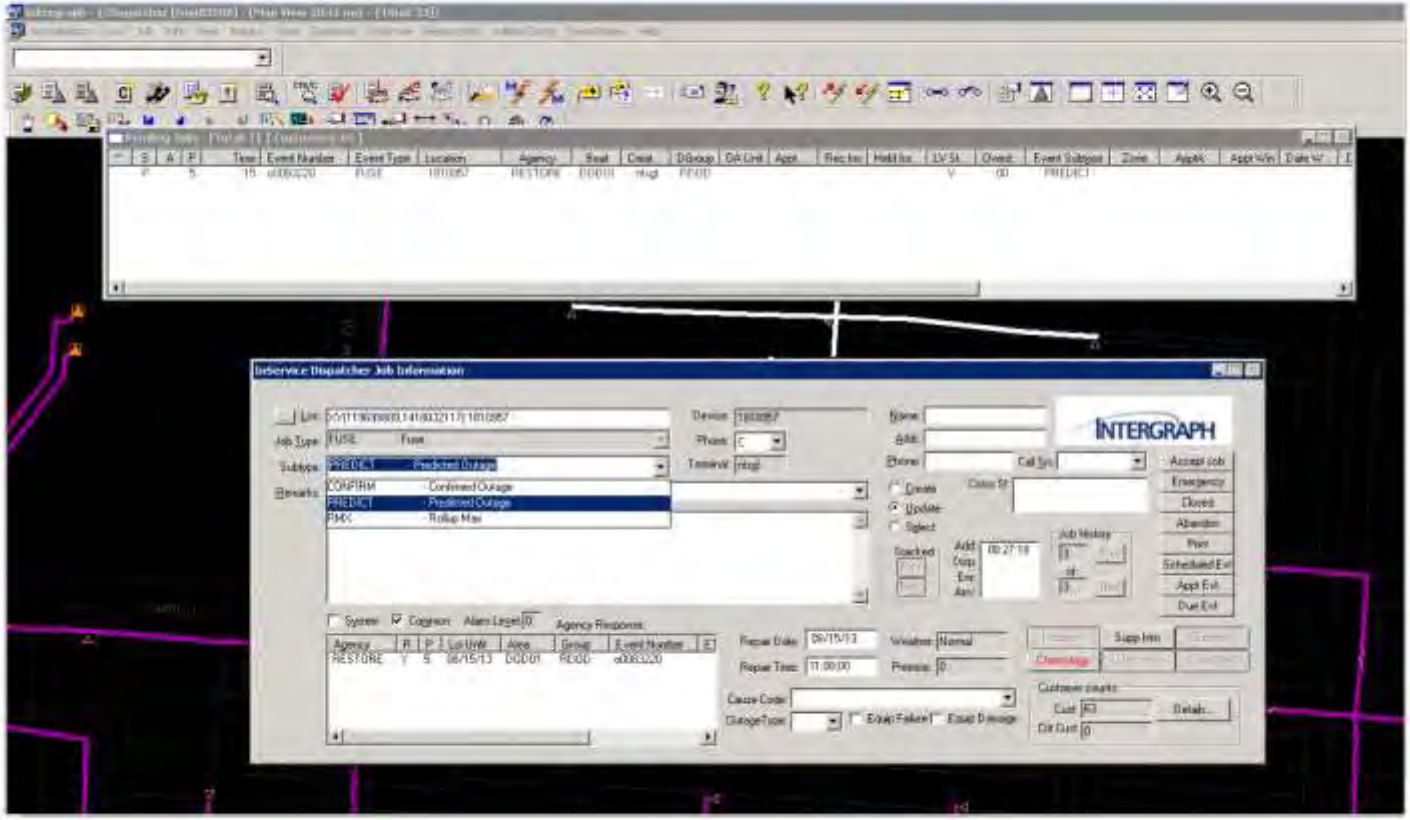
Select "Update" to Confirm the Outage



▪18

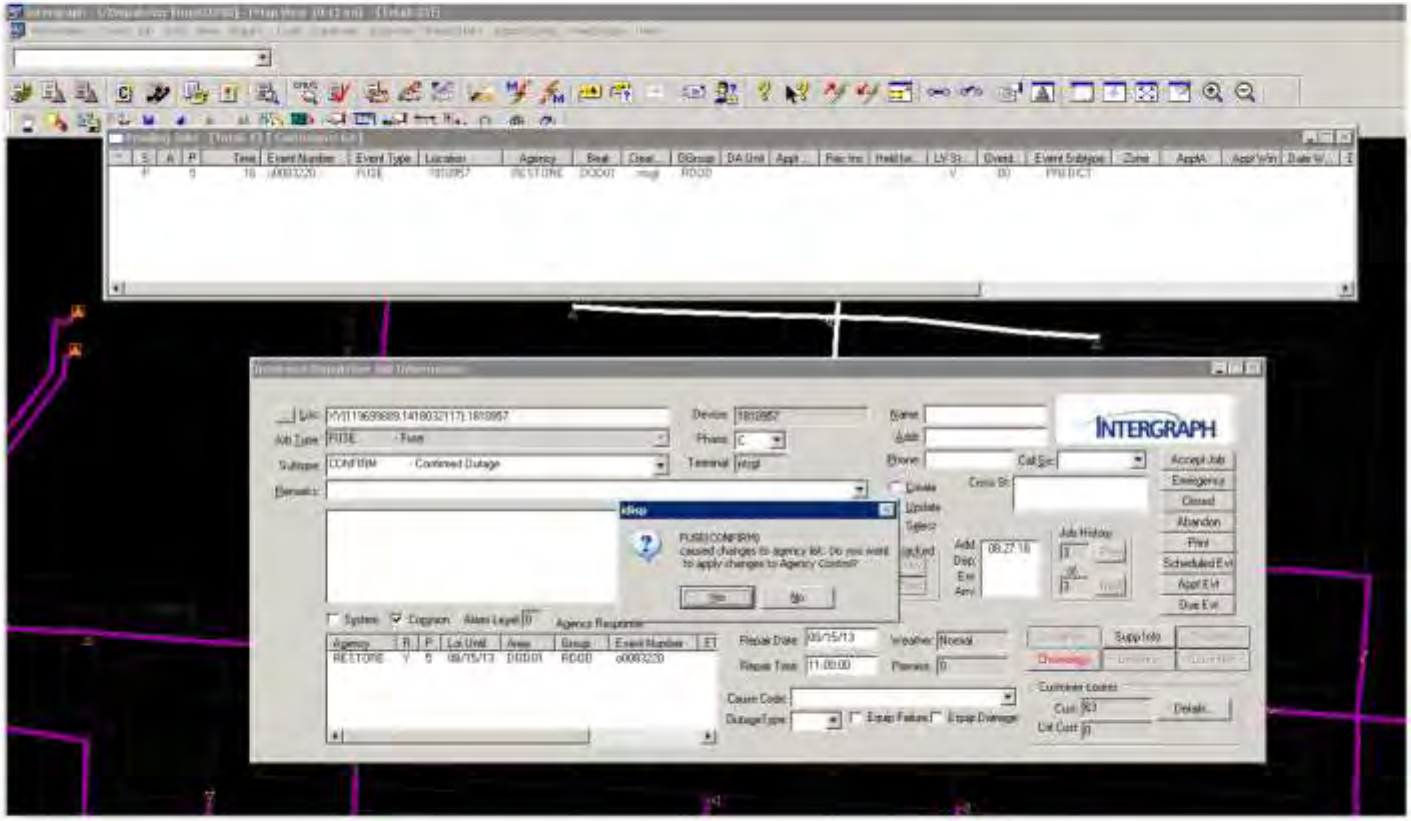
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Update Outage from "PREDICT" to "CONFIRM"



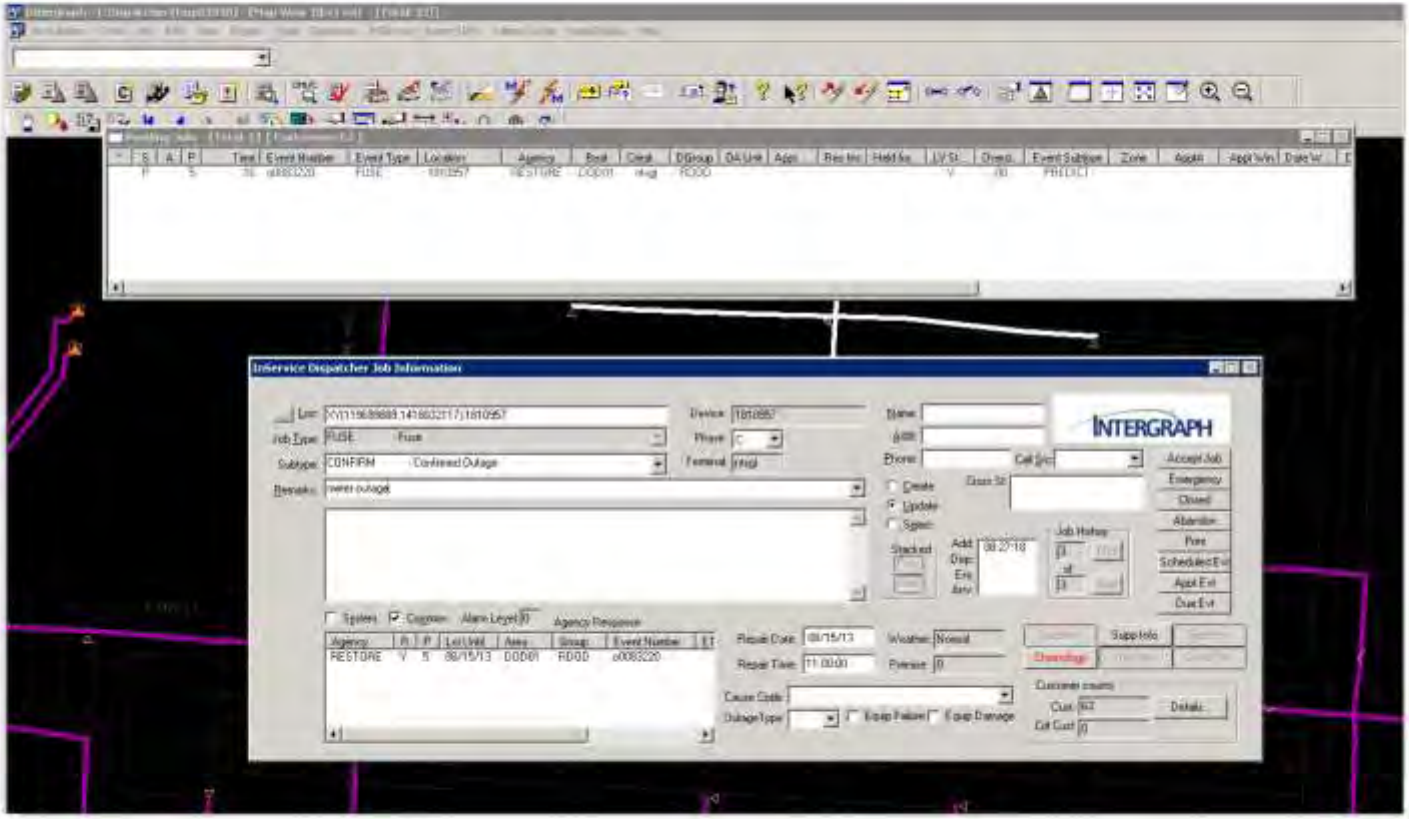
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Confirm the Outage



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

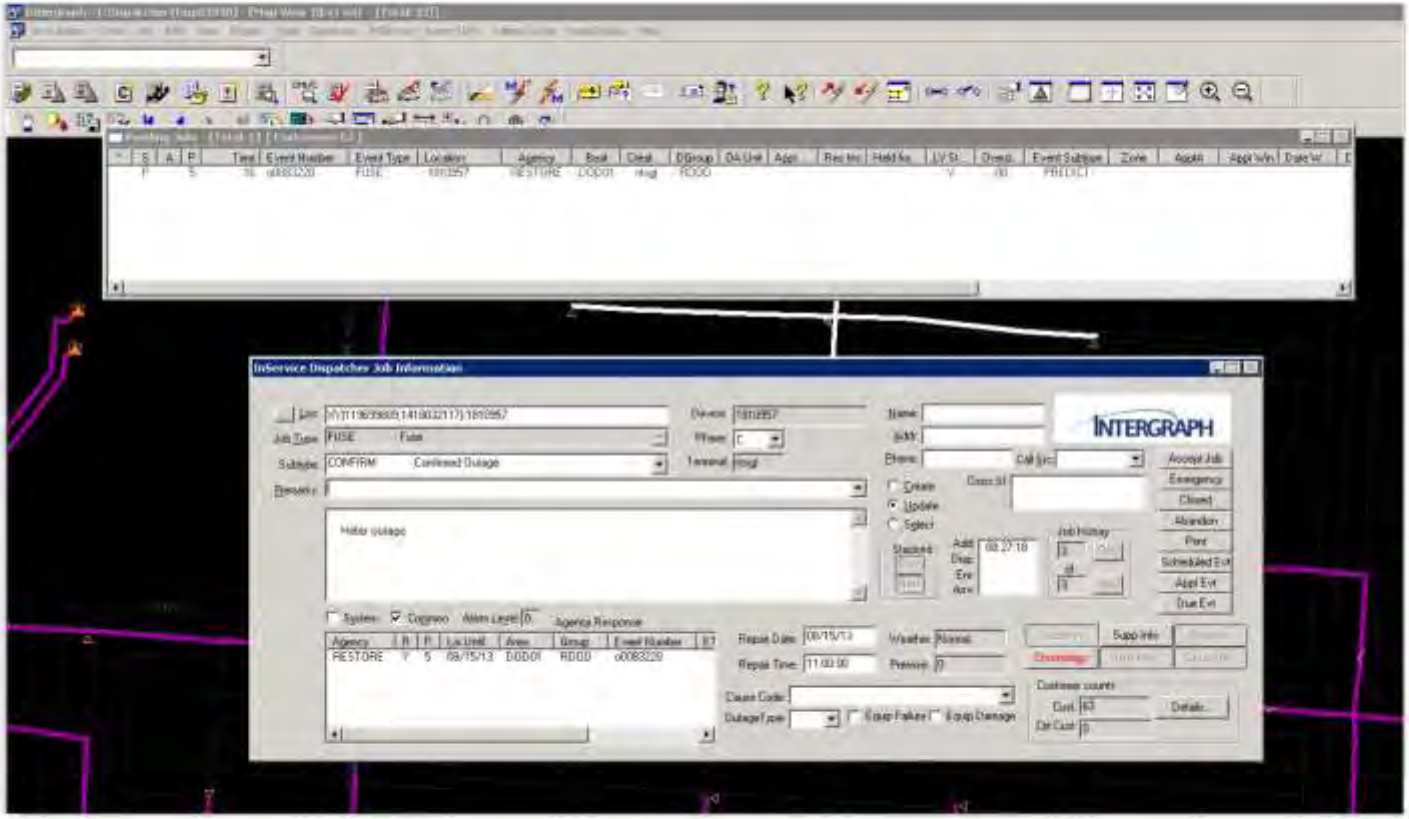
Enter Remarks



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

KCP&L energizing life

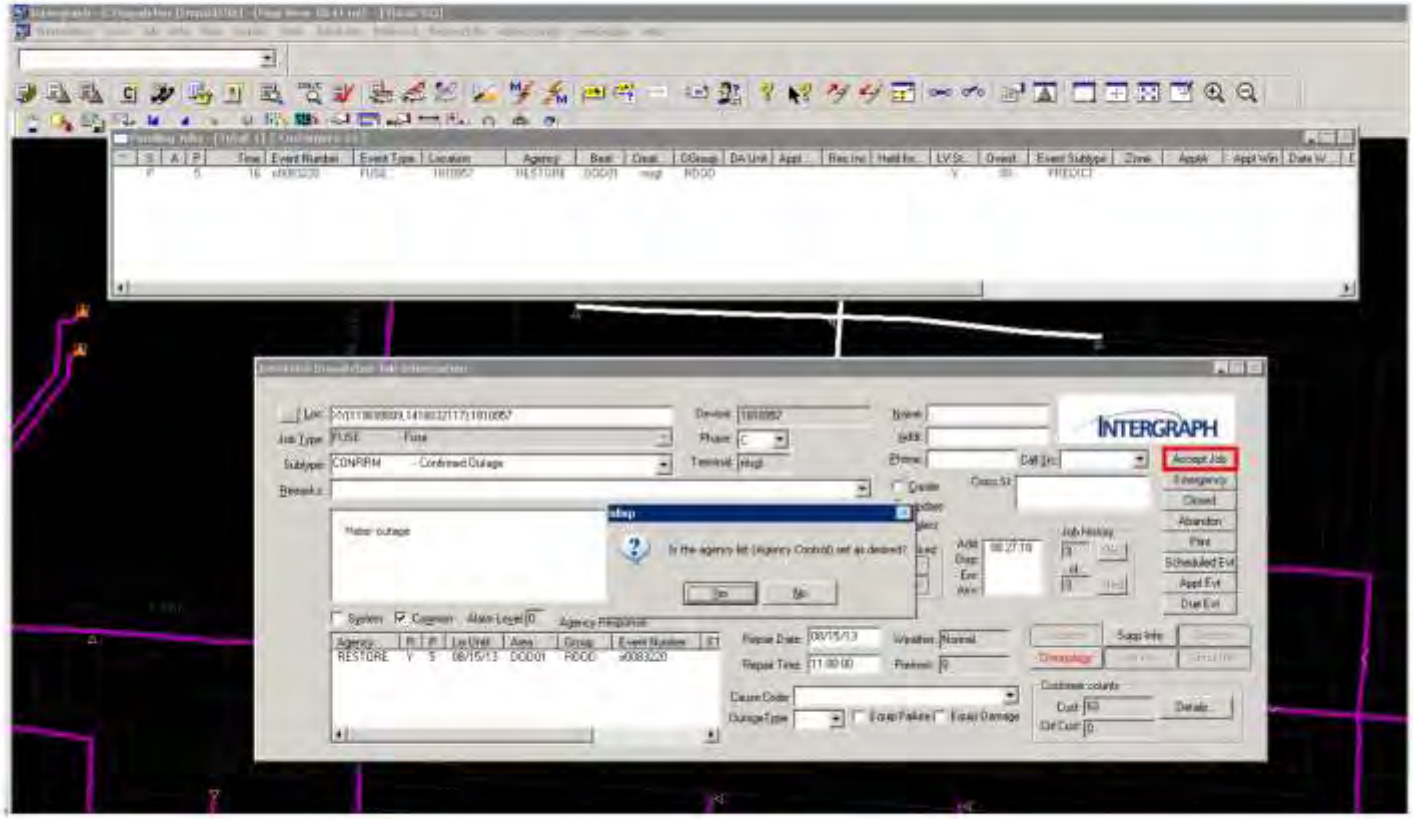
Outage Confirmed



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

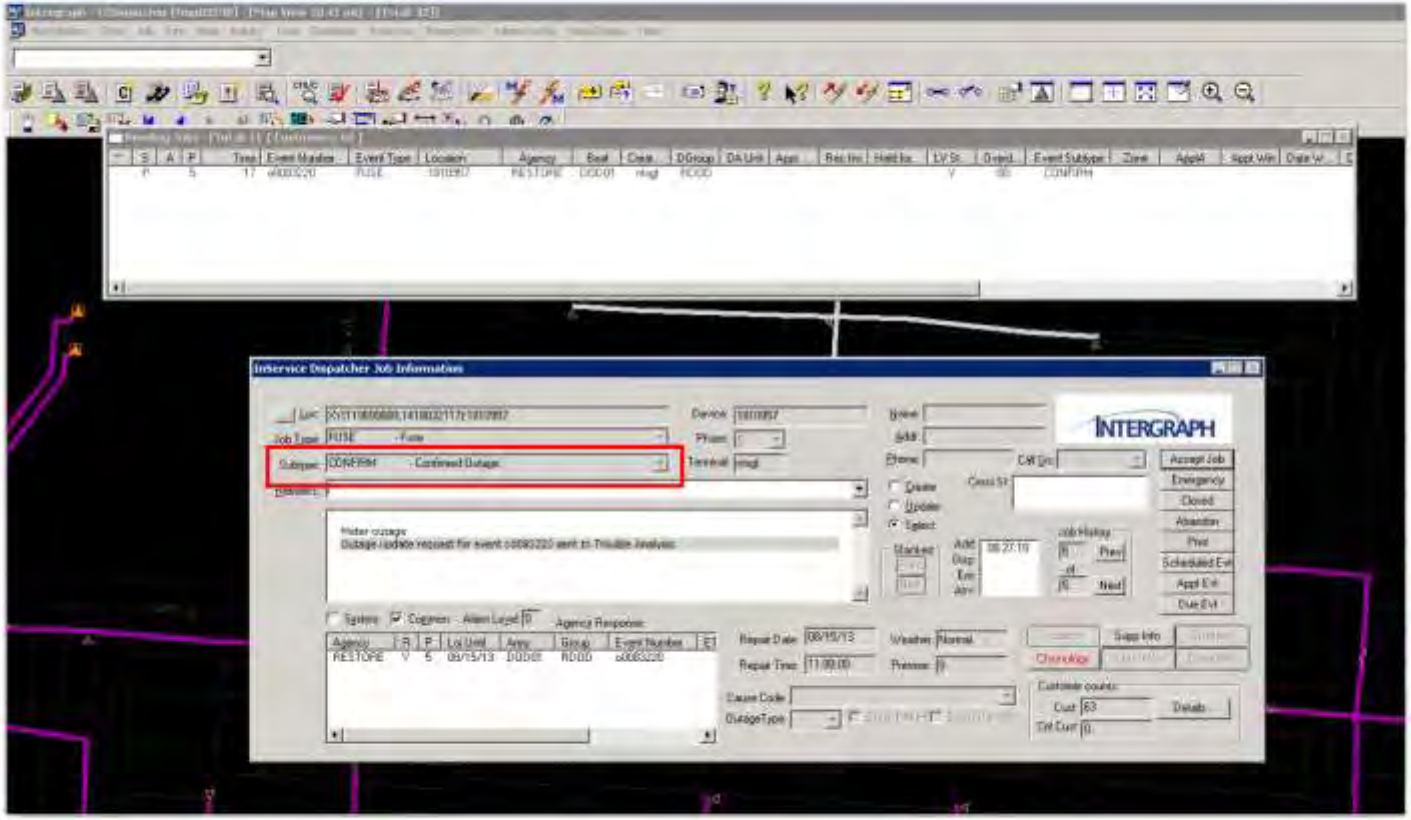
KCP&L energizing life

Click "Accept Job"



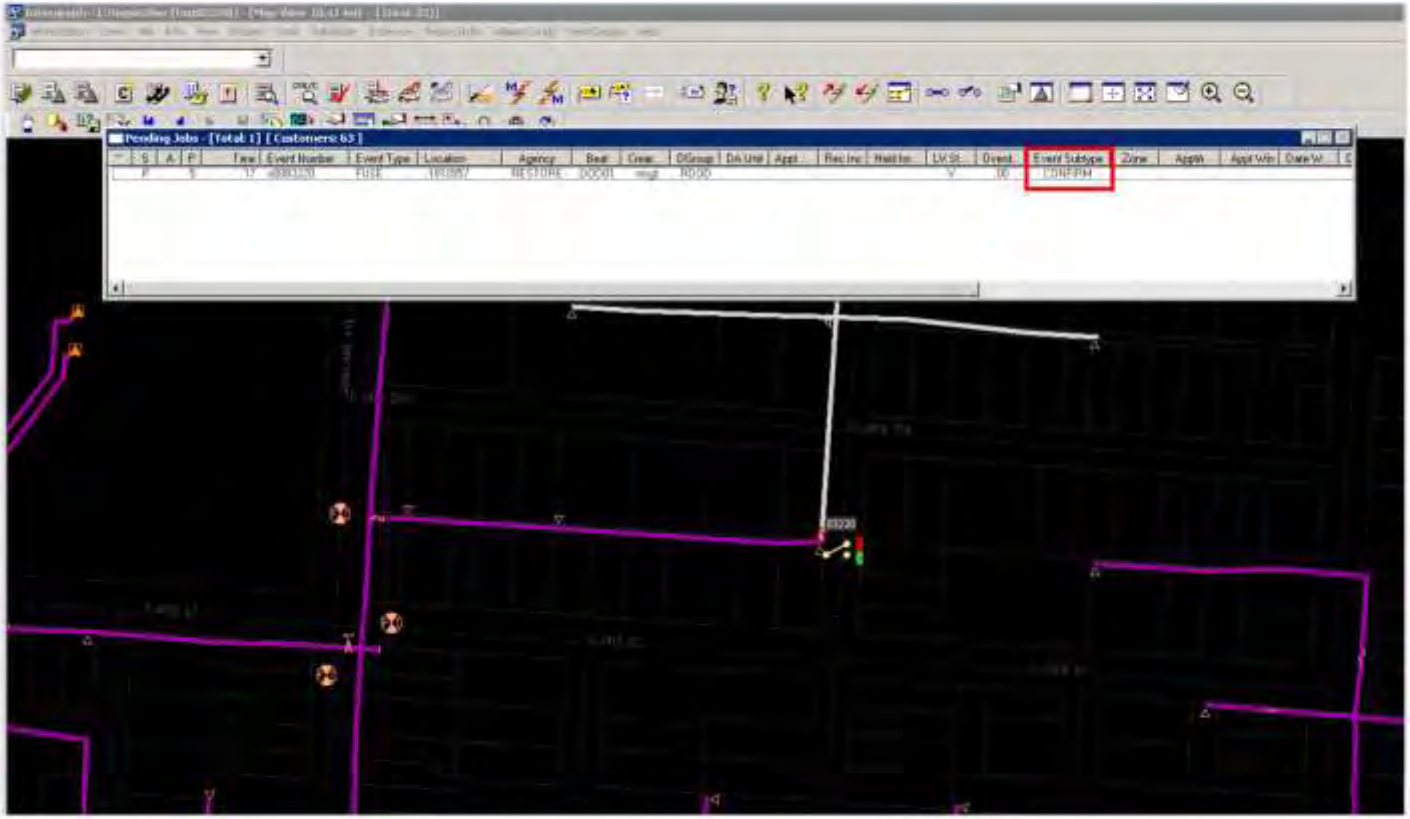
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Job is Accepted and Outage is Confirmed



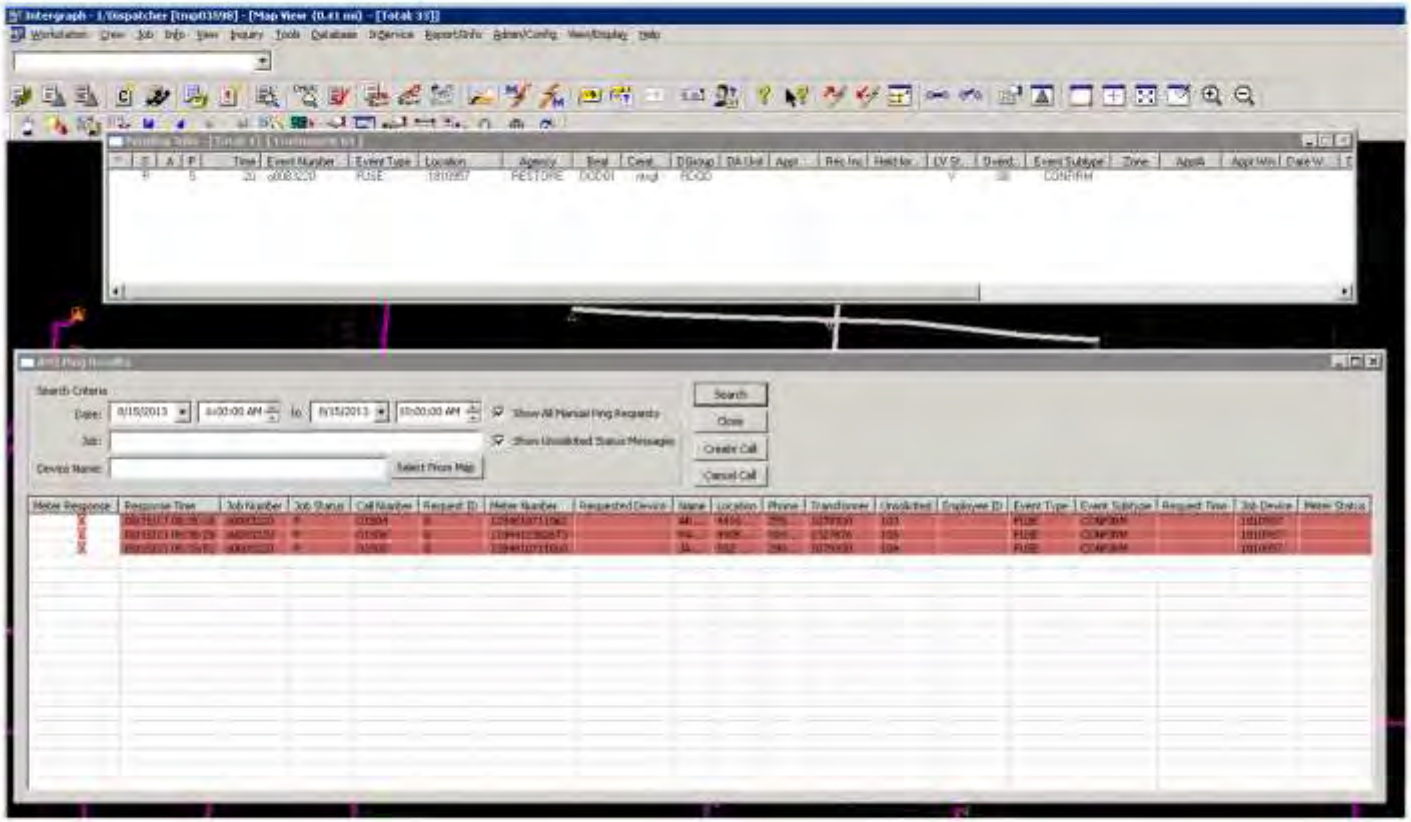
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Event Subtype updated to "CONFIRM"



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

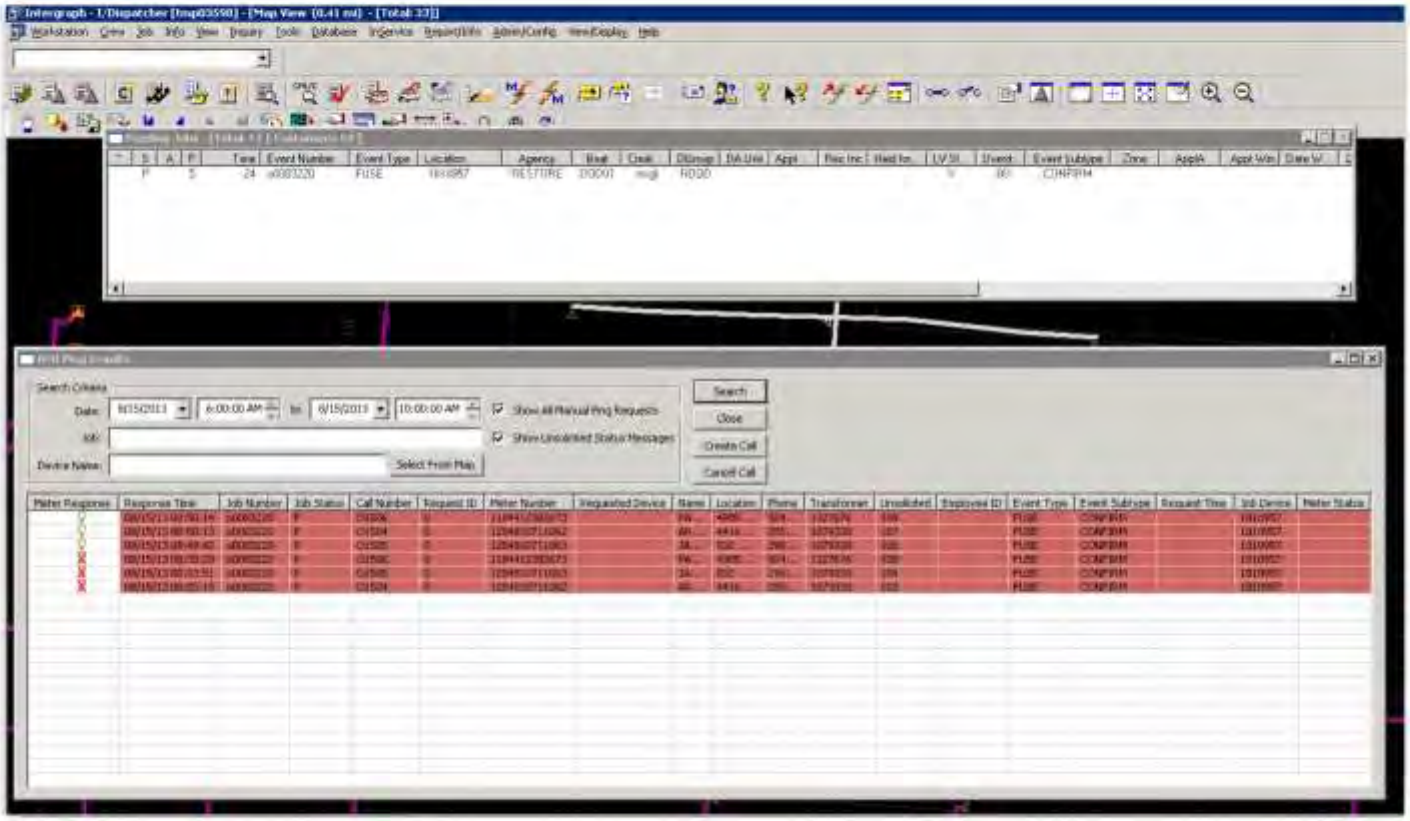
Fields in "AMI Ping Results" after Outage is Confirmed



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

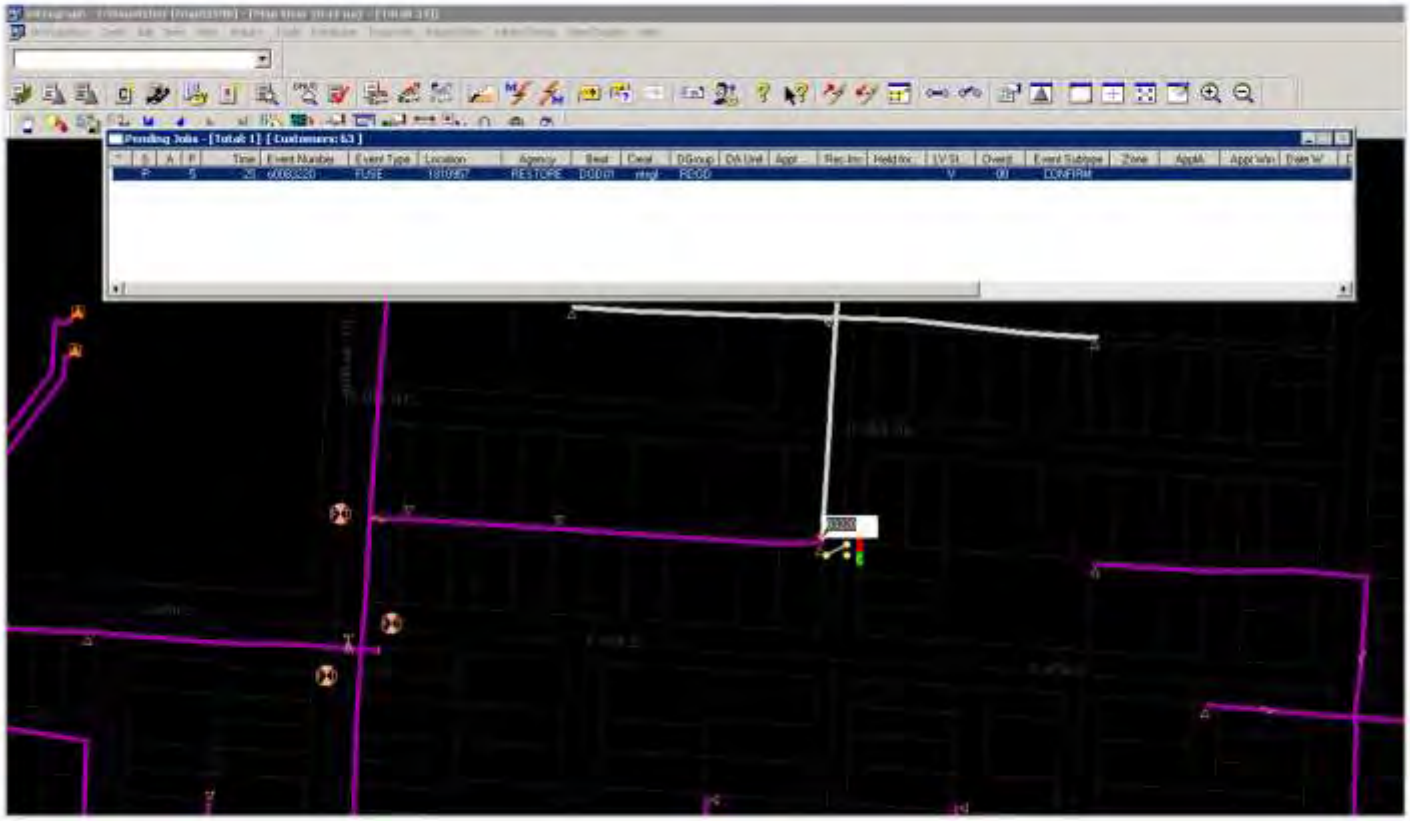
KCP&L energizing life

Search in "AMI Ping Results" for Restoration Information



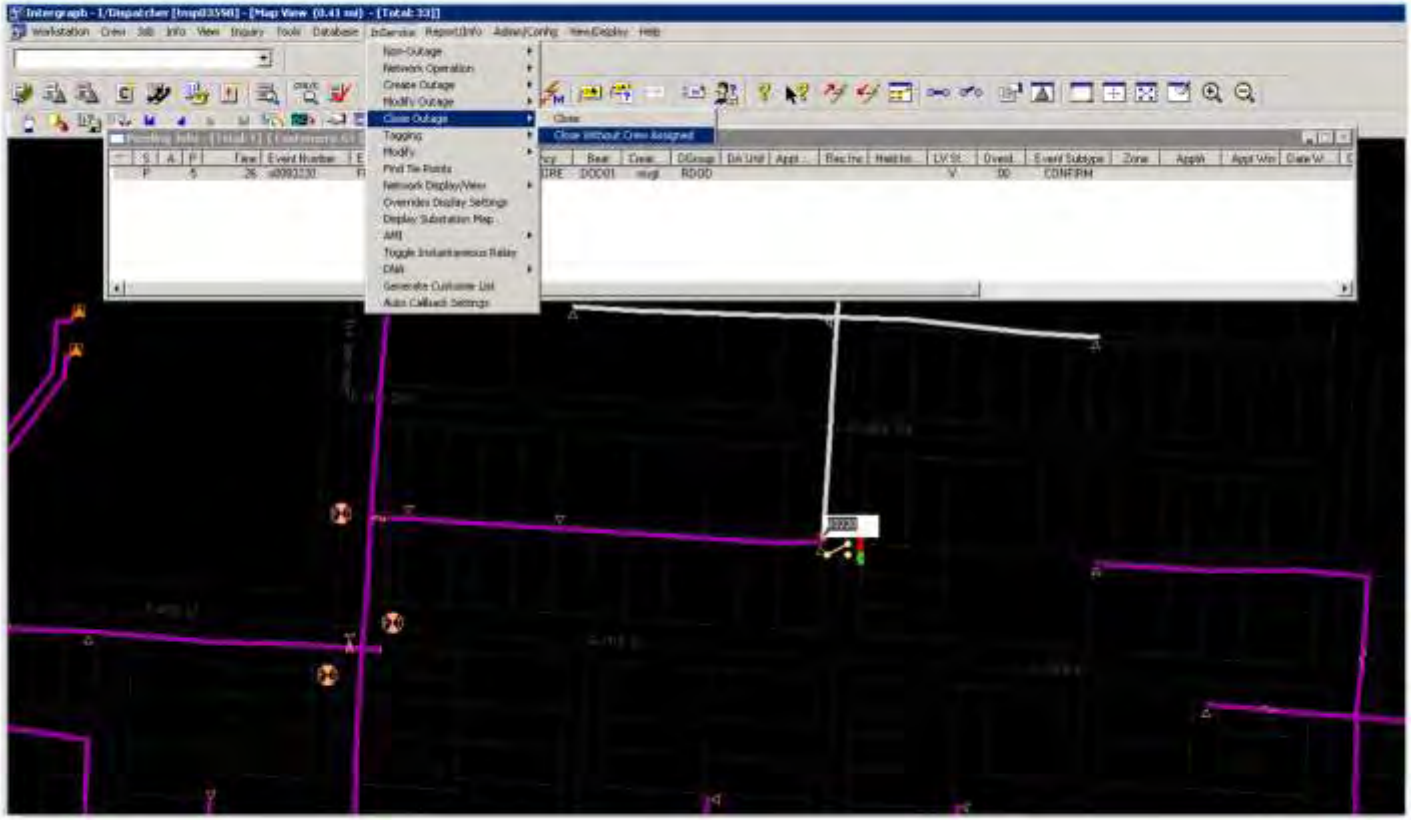
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Select the Job in "Pending Jobs" to View Location on Map



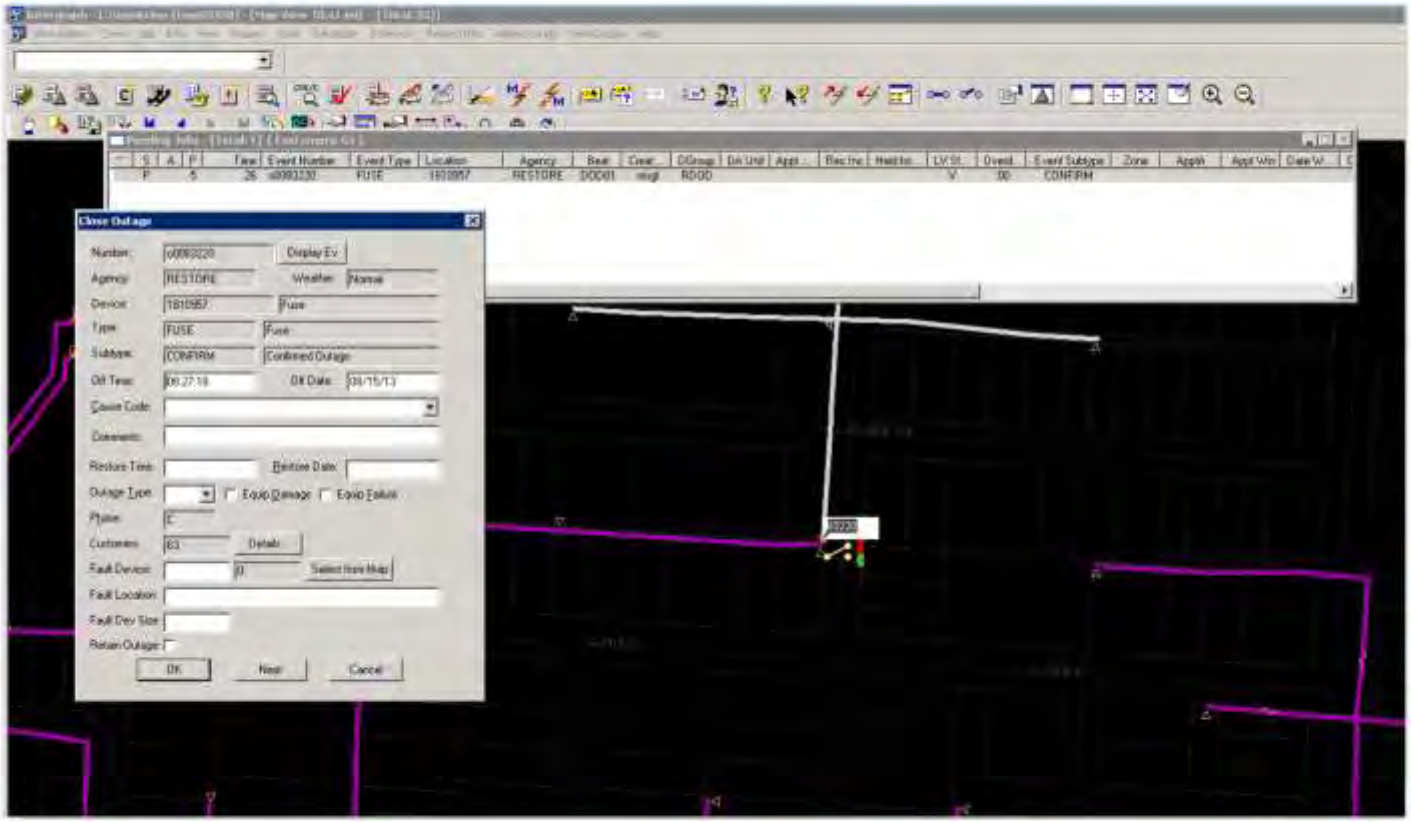
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Open the "Close Outage" Window



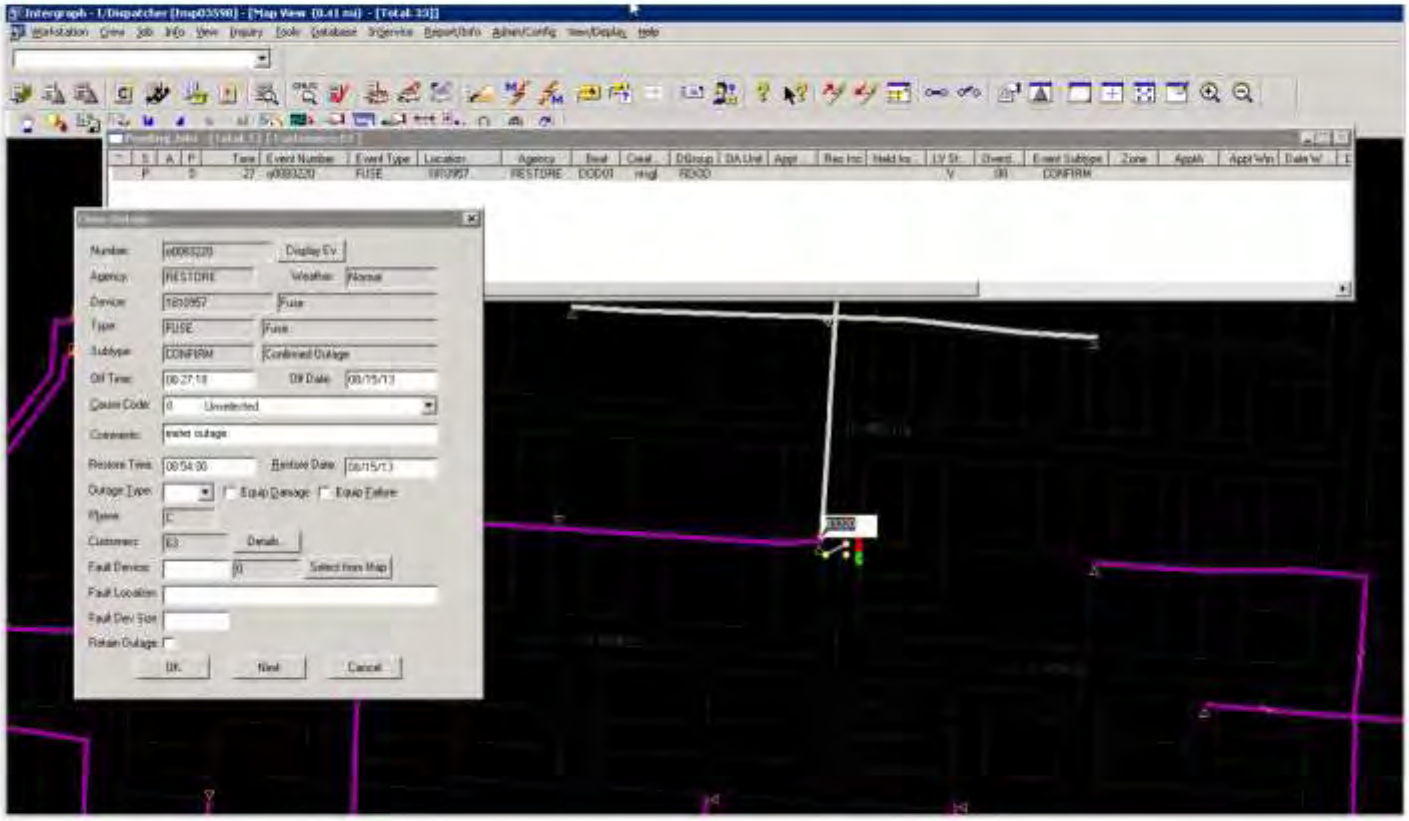
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Fields in "Close Outage" Window



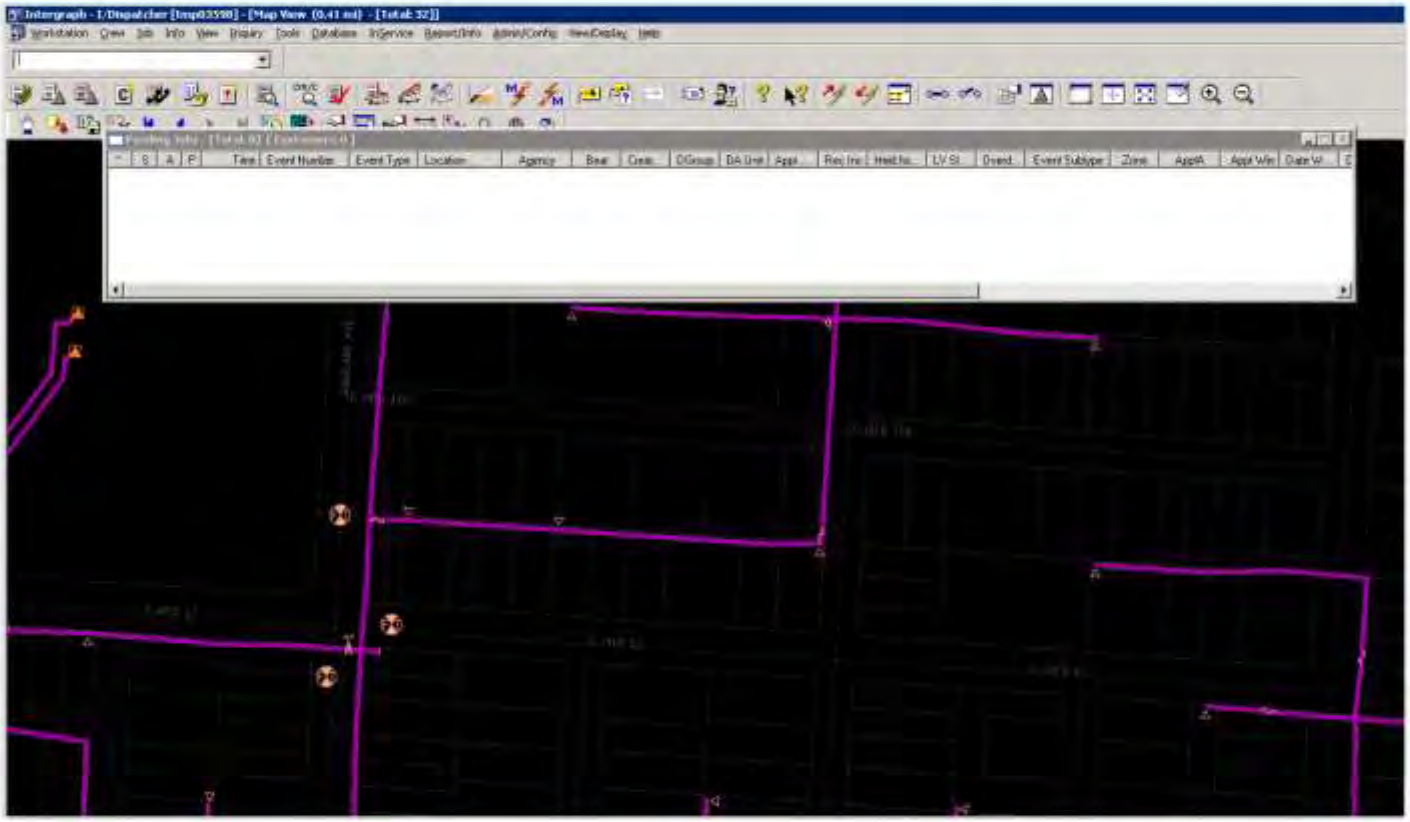
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Enter Information in "Close Outage" Window

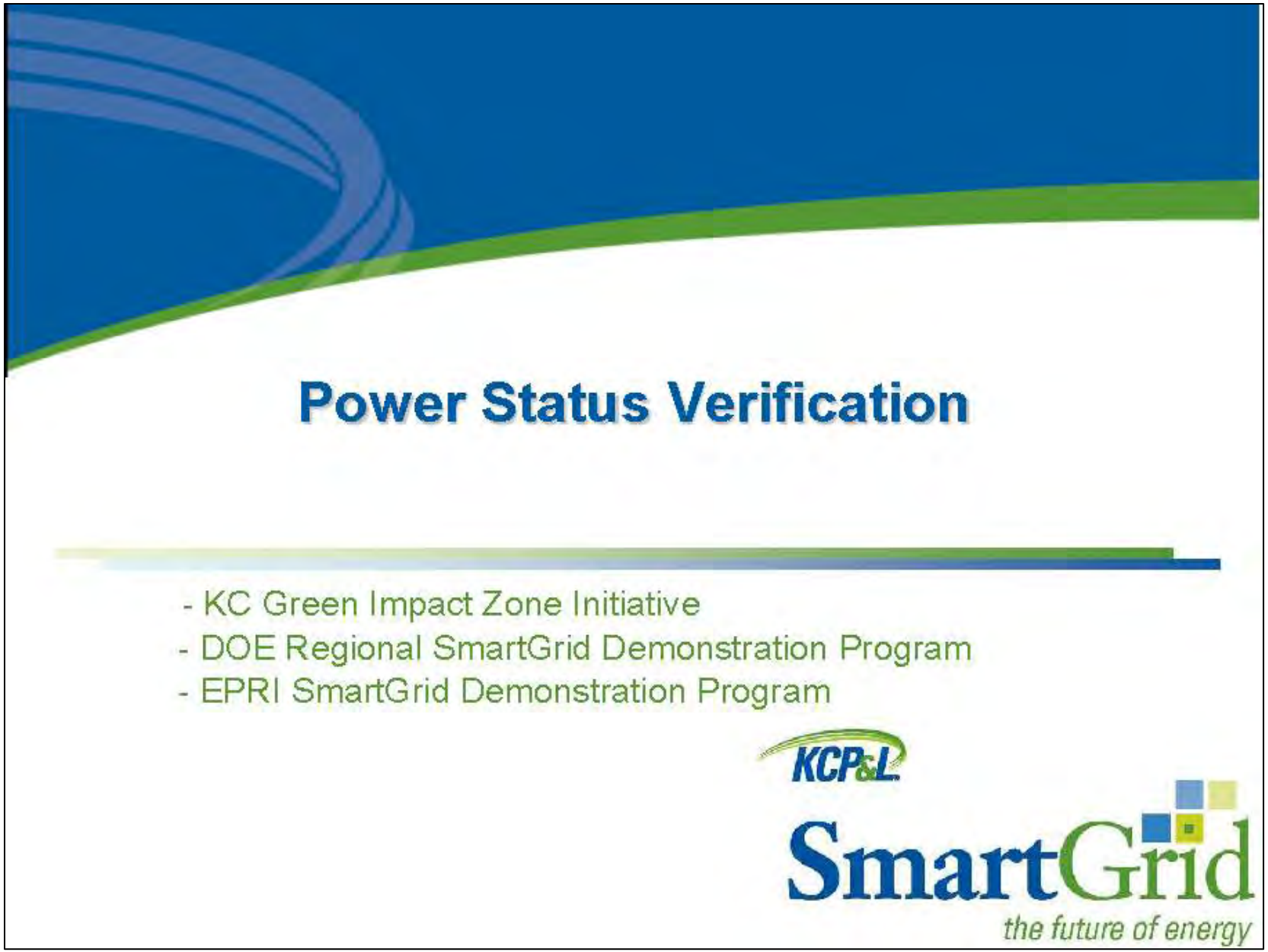


This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

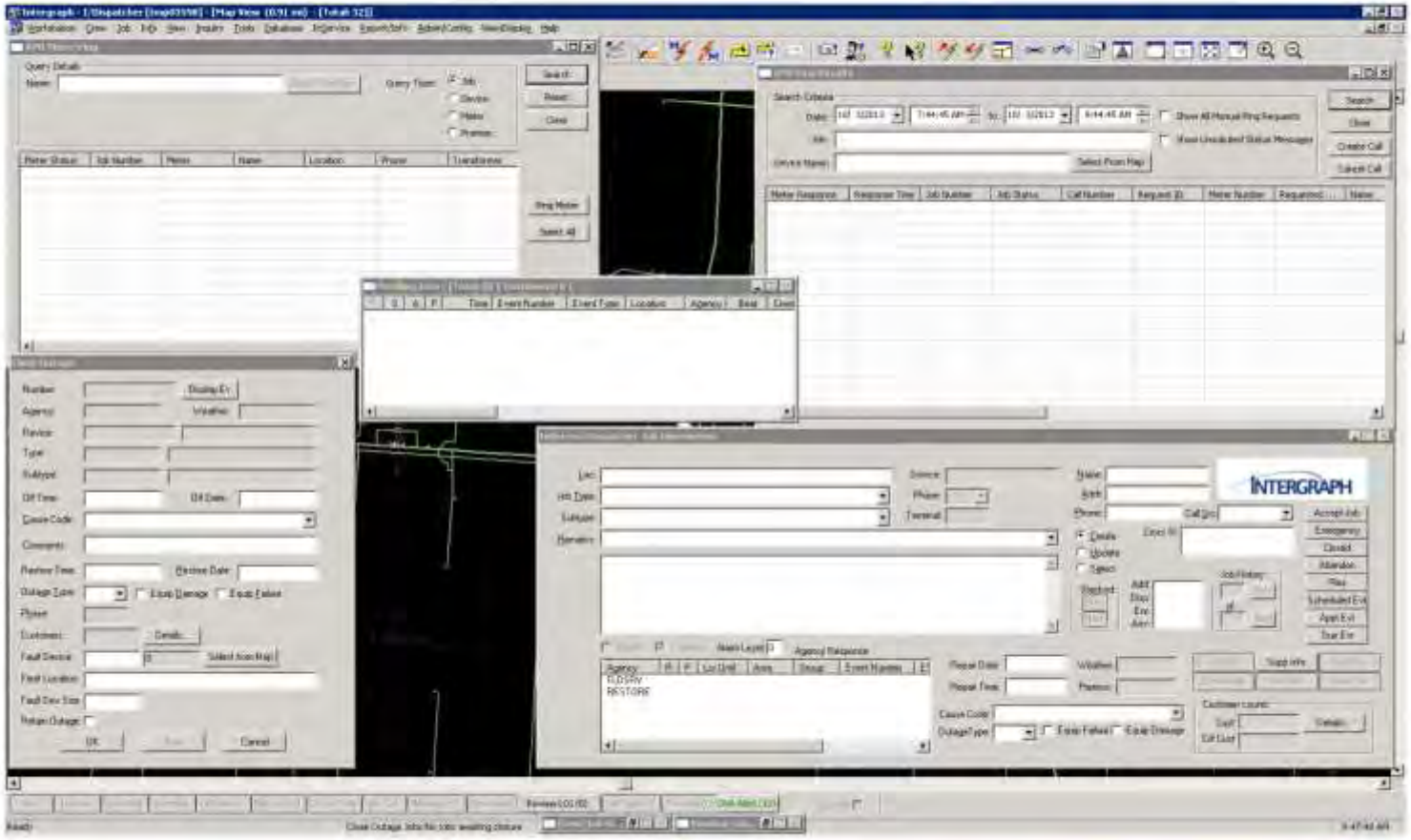
Outage Job is Closed



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

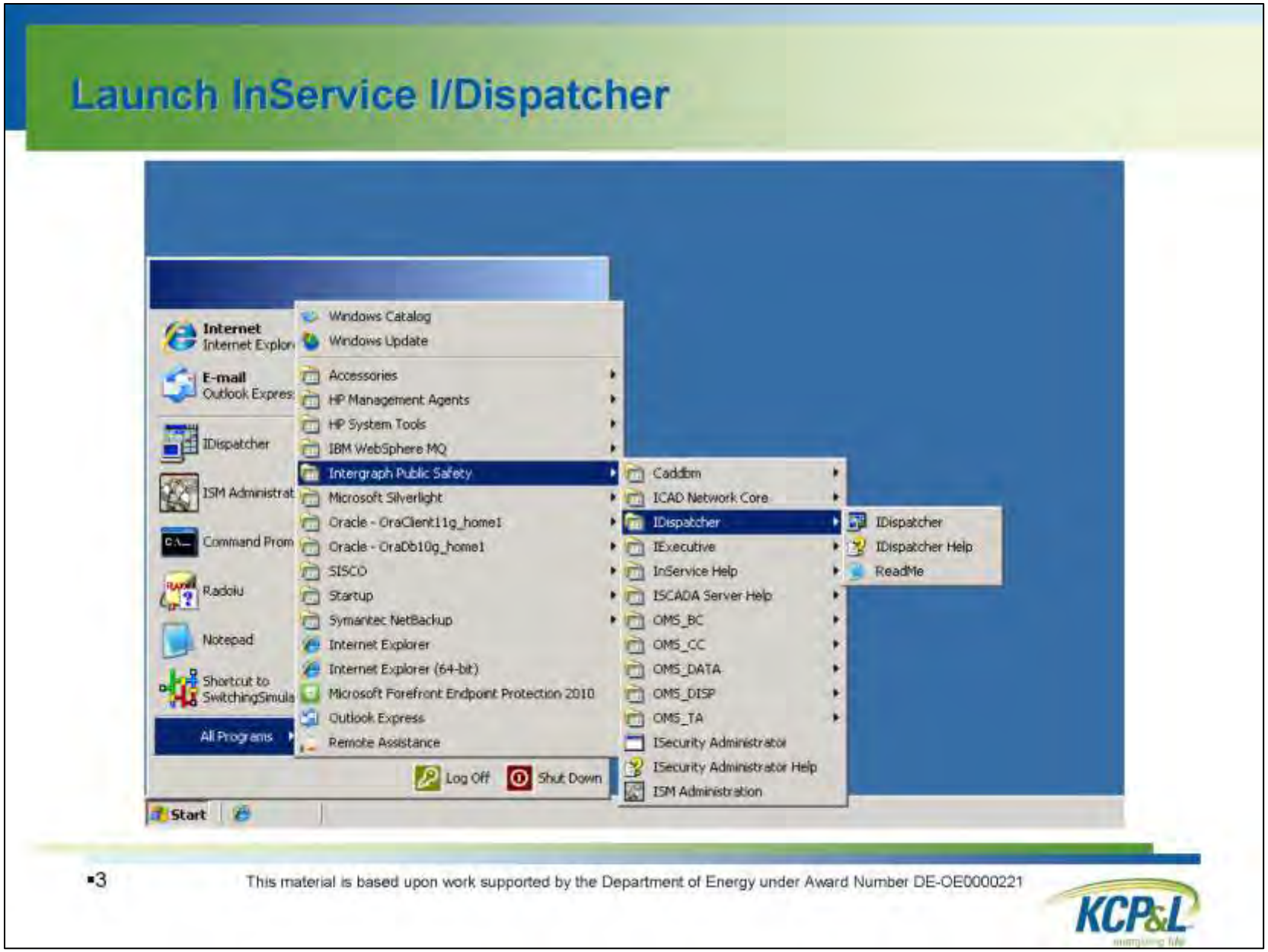

Power Status Verification
- KC Green Impact Zone Initiative
- DOE Regional SmartGrid Demonstration Program
- EPRI SmartGrid Demonstration Program
KCP&L
SmartGrid
the future of energy

Windows Used for Power Status Verification

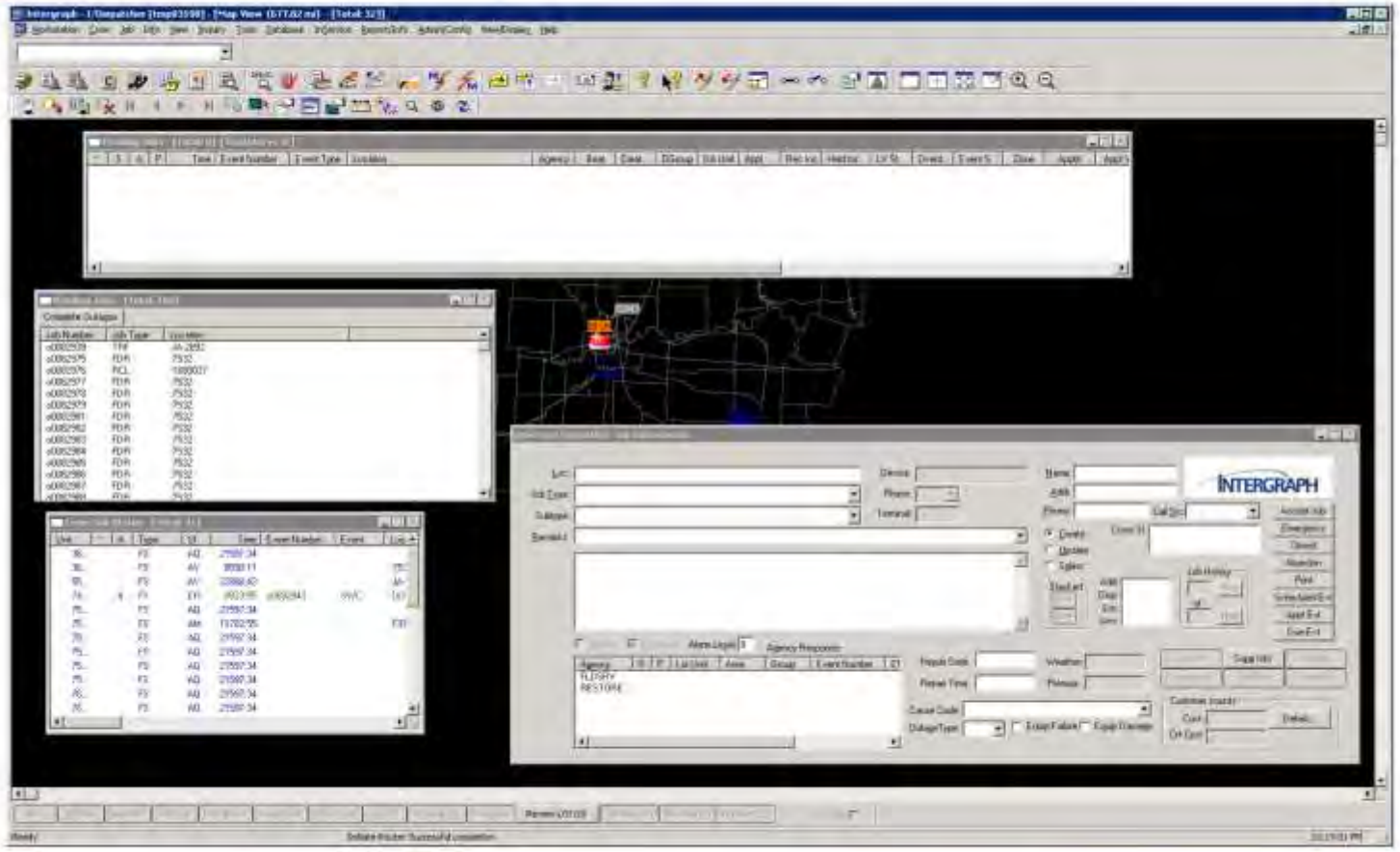


This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

KCP&L energizing life


Launch InService I/Dispatcher
Internet
E-mail
IDispatcher
ISM Administrat
Command Prom
Radoiu
Notepad
Shortcut to SwitchingSimula
All Programs
Windows Catalog
Windows Update
Accessories
HP Management Agents
HP System Tools
IBM WebSphere MQ
Intergraph Public Safety
Microsoft Silverlight
Oracle - OraClient11g_home1
Oracle - OraDb10g_home1
SISCO
Startup
Symantec NetBackup
Internet Explorer
Internet Explorer (64-bit)
Microsoft Forefront Endpoint Protection 2010
Outlook Express
Remote Assistance
Log Off
Shut Down
Start
Caddbm
ICAD Network Core
IDispatcher
IExecutive
InService Help
ISCADA Server Help
OMS_BC
OMS_CC
OMS_DATA
OMS_DISP
OMS_TA
ISecurity Administrator
ISecurity Administrator Help
ISM Administration
IDispatcher
IDispatcher Help
ReadMe
3
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

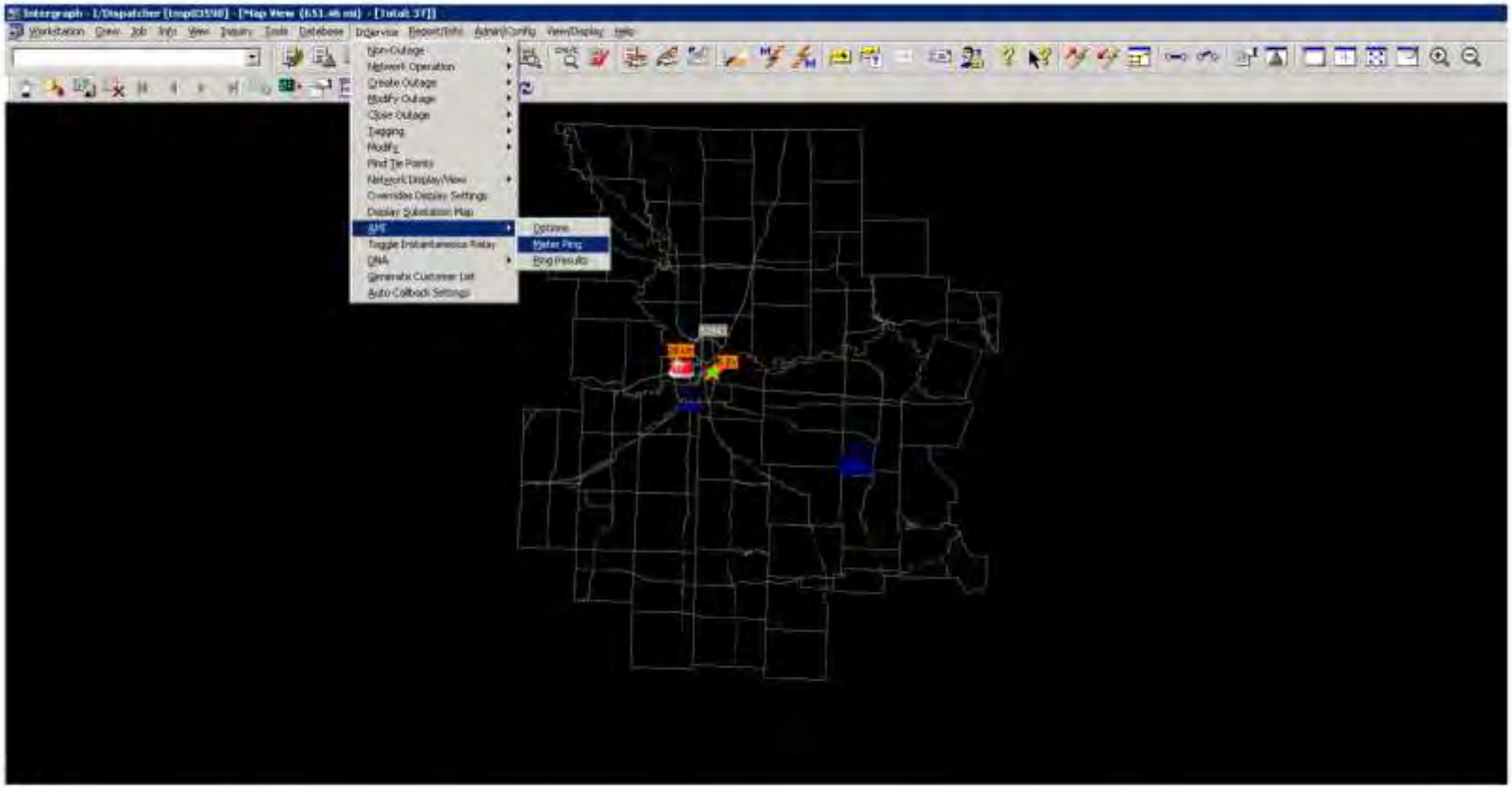
InService I/Dispatcher Main Screen



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

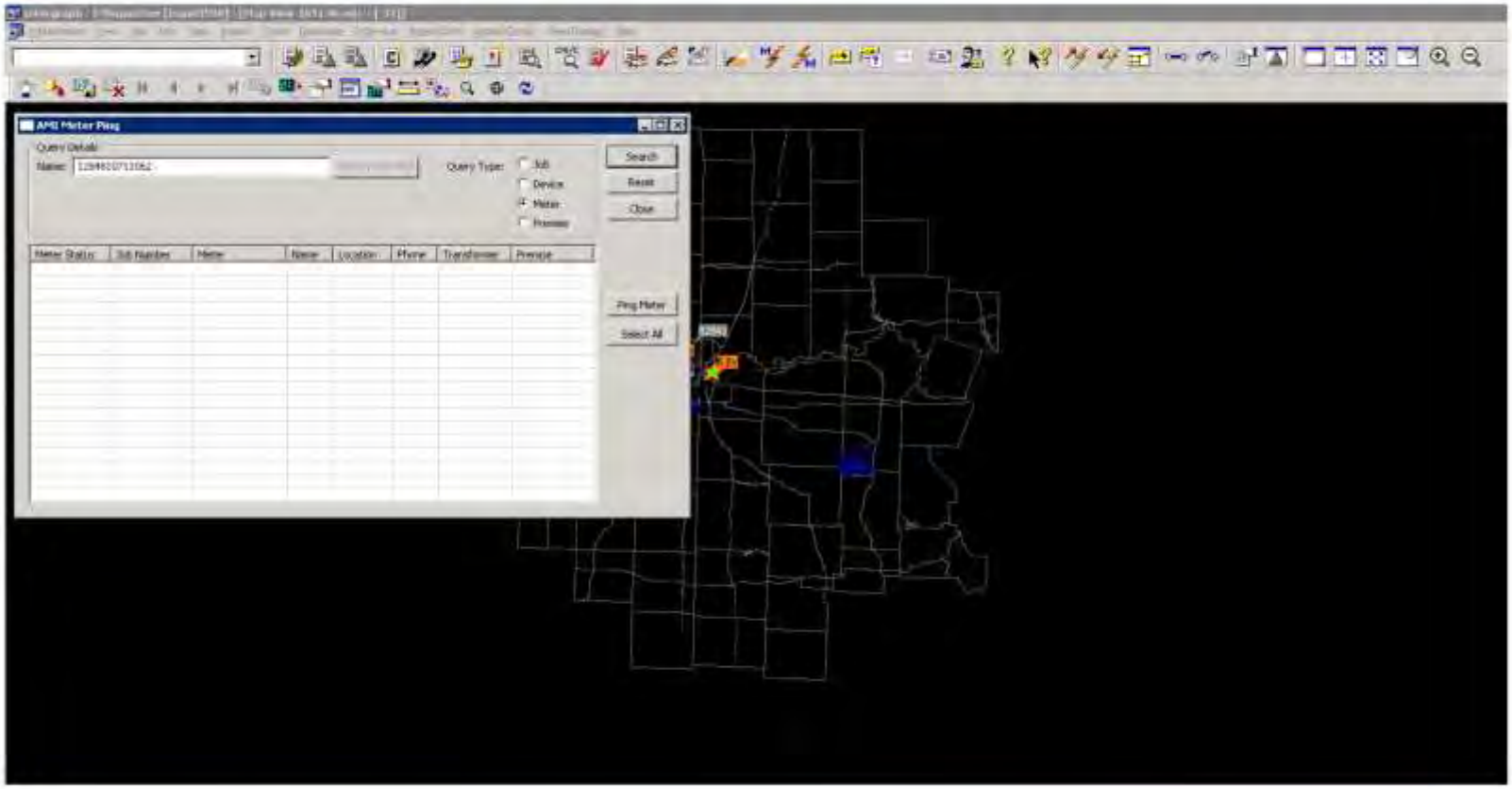
KCP&L energizing life

Open "AMI Meter Ping" to send Power Status Verification



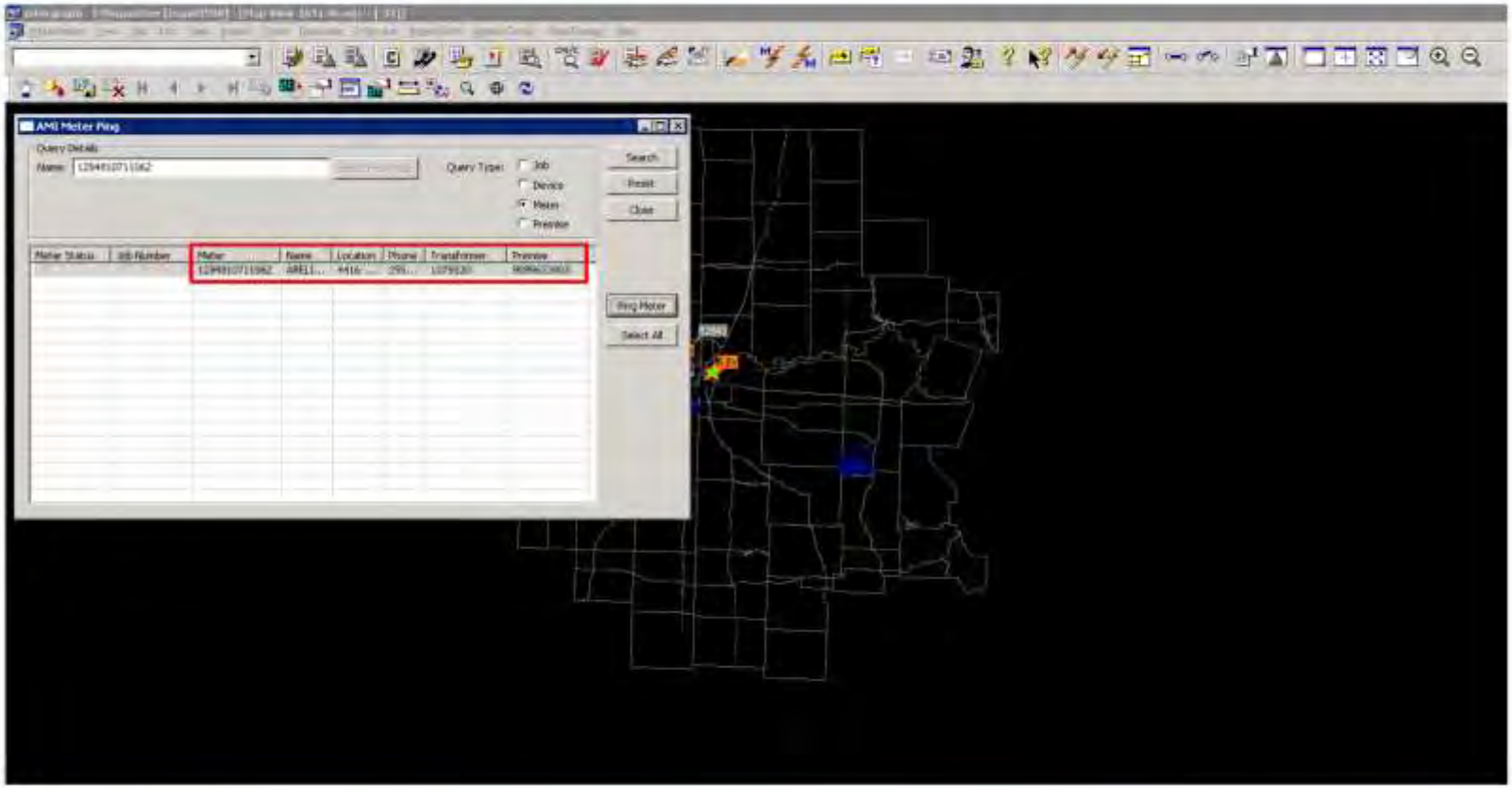
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Scenario #1: Meter is "Powered On"



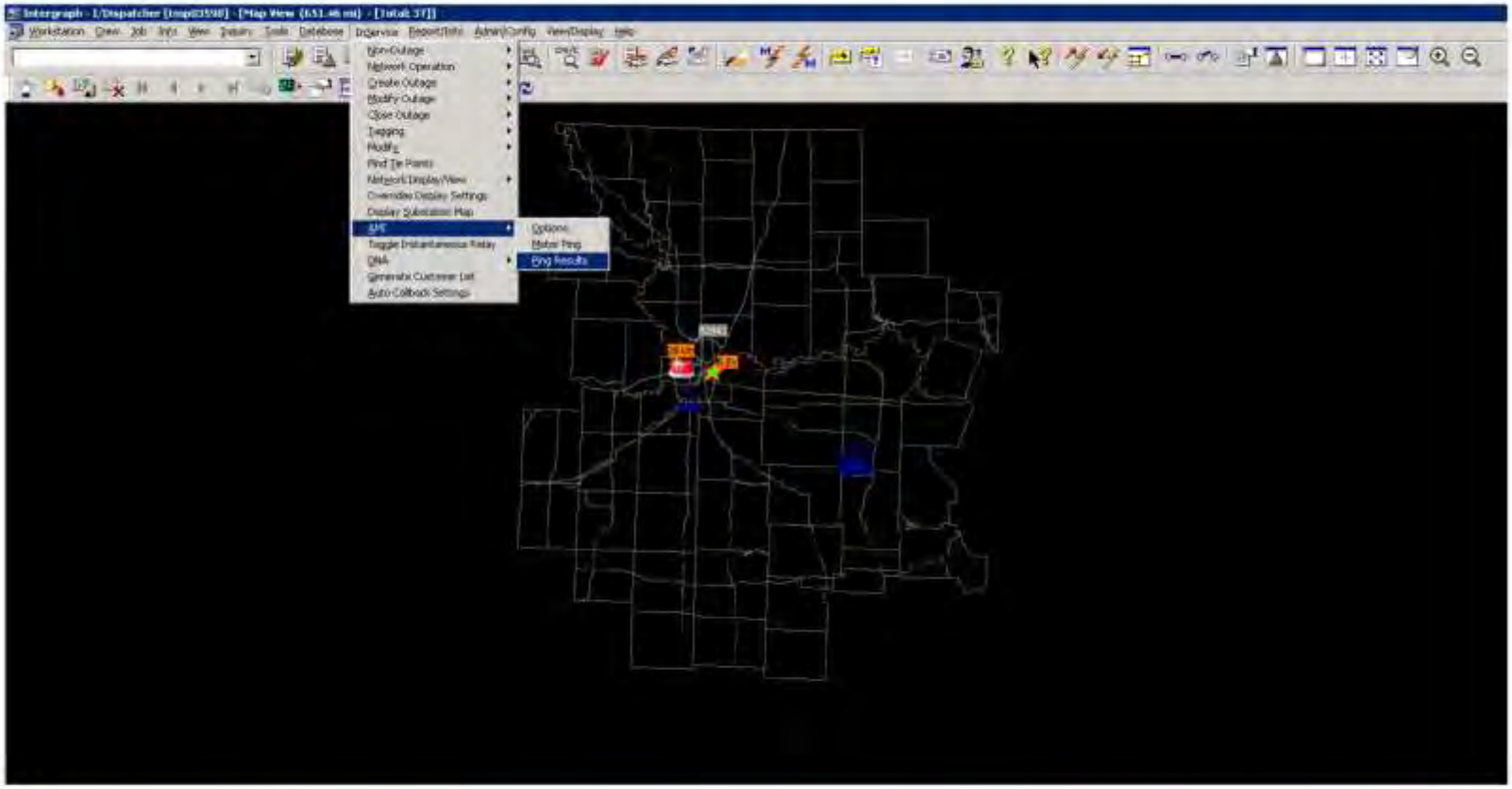
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Send Meter Ping Request



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

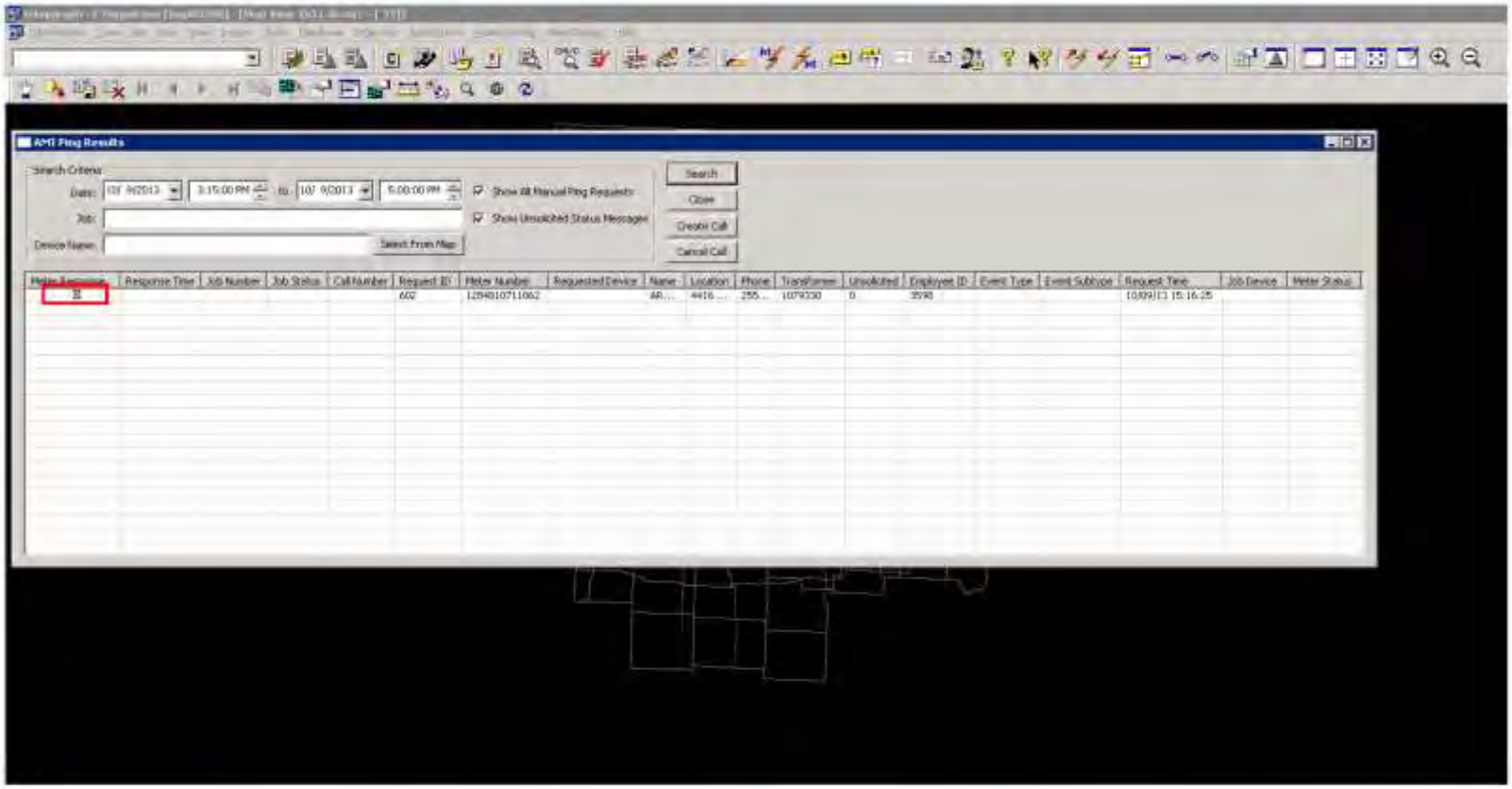
Open AMI Ping Results



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

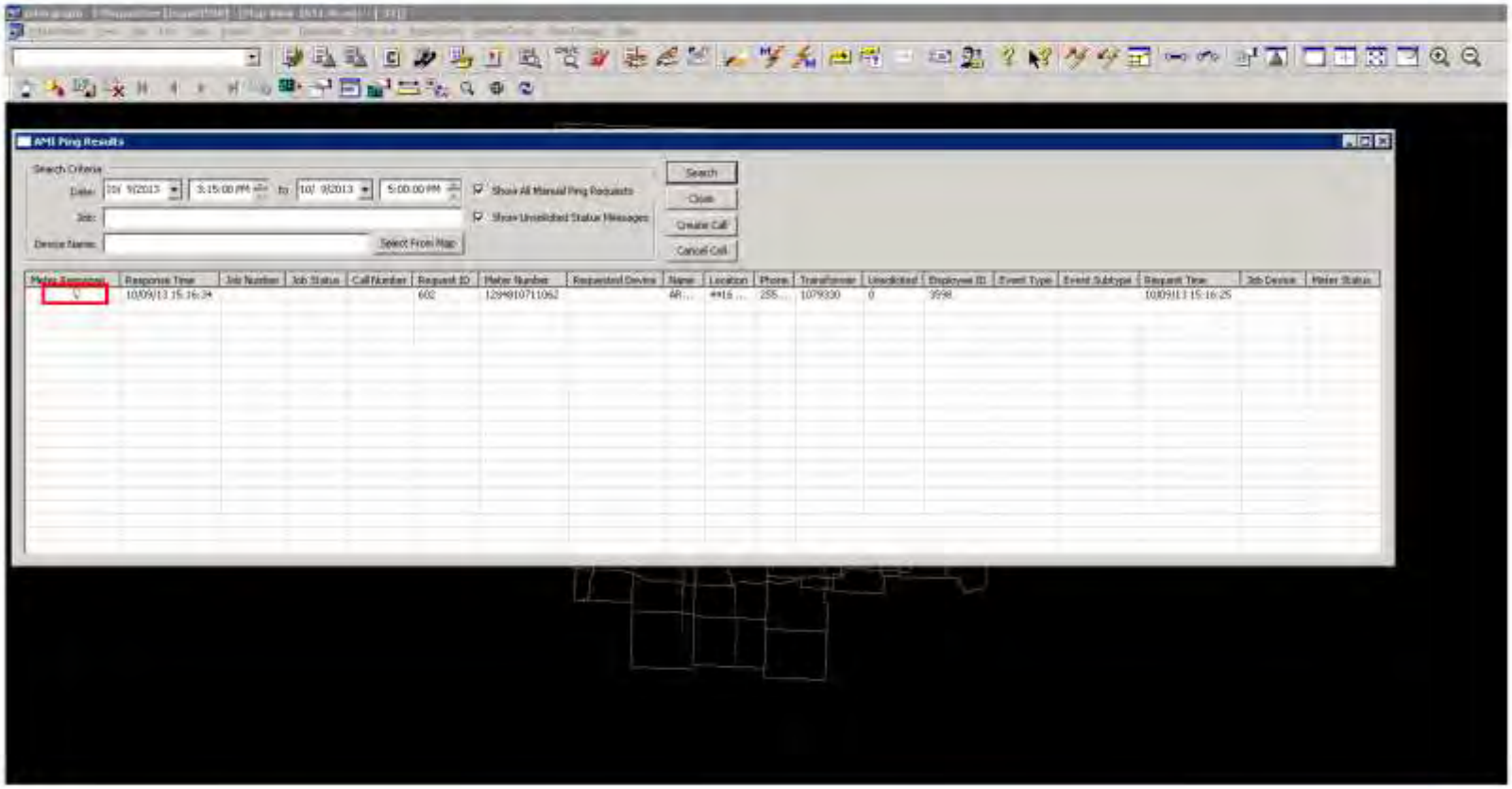
KCP&L energizing life

Meter Ping Request in "AMI Ping Results"



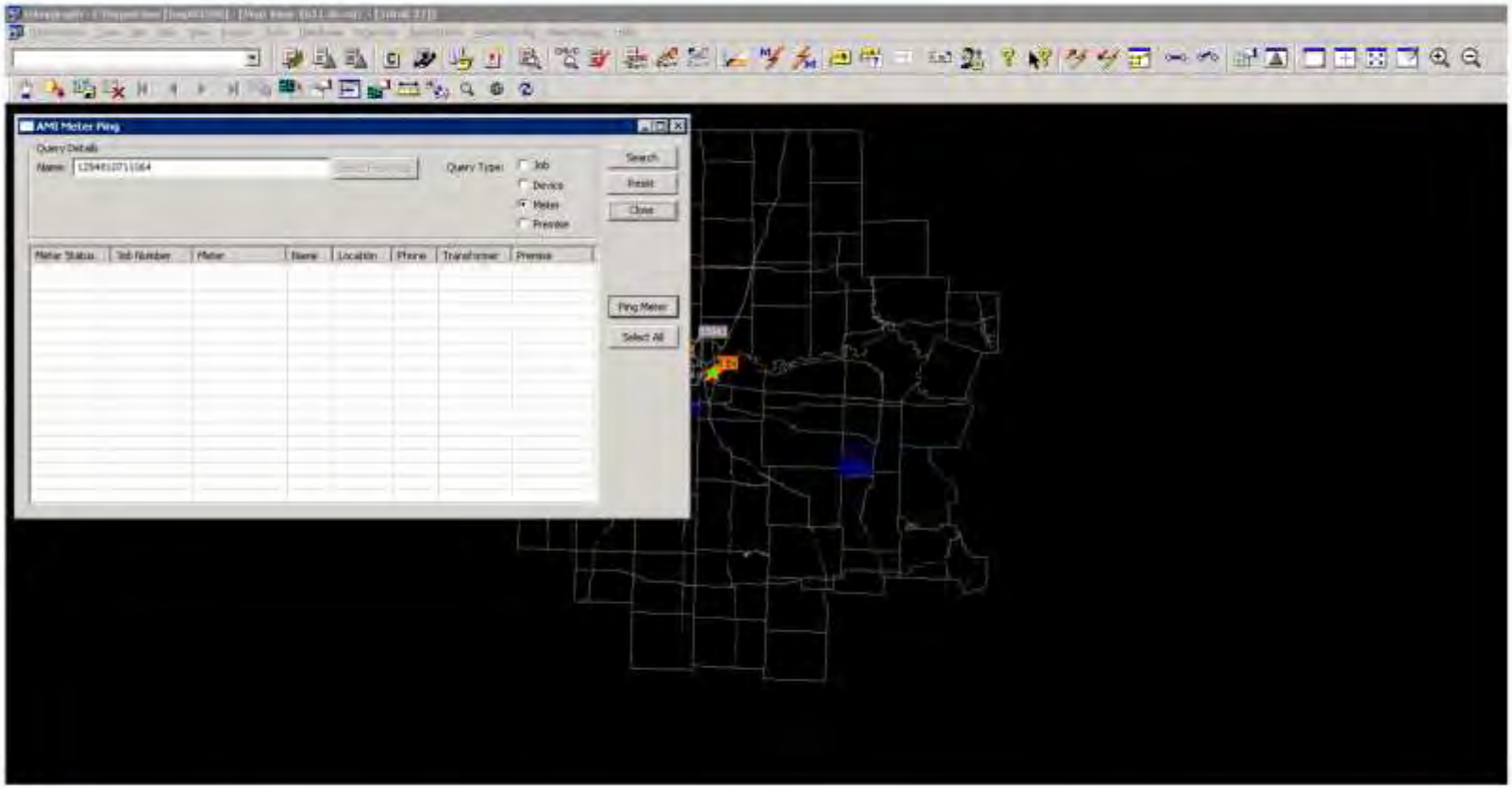
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Received Meter Ping Response



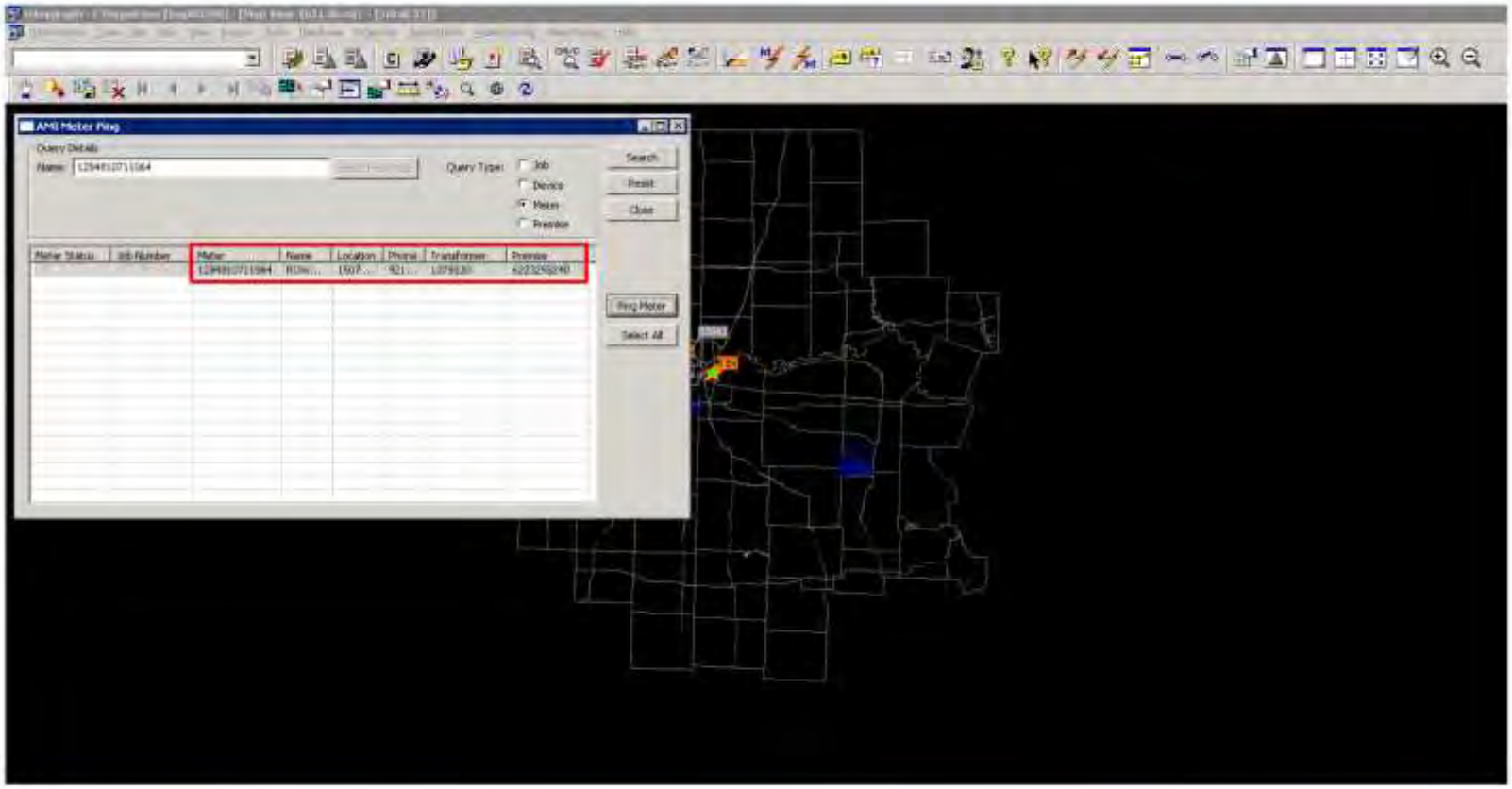
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Scenario #2: Meter is "Powered Off"



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

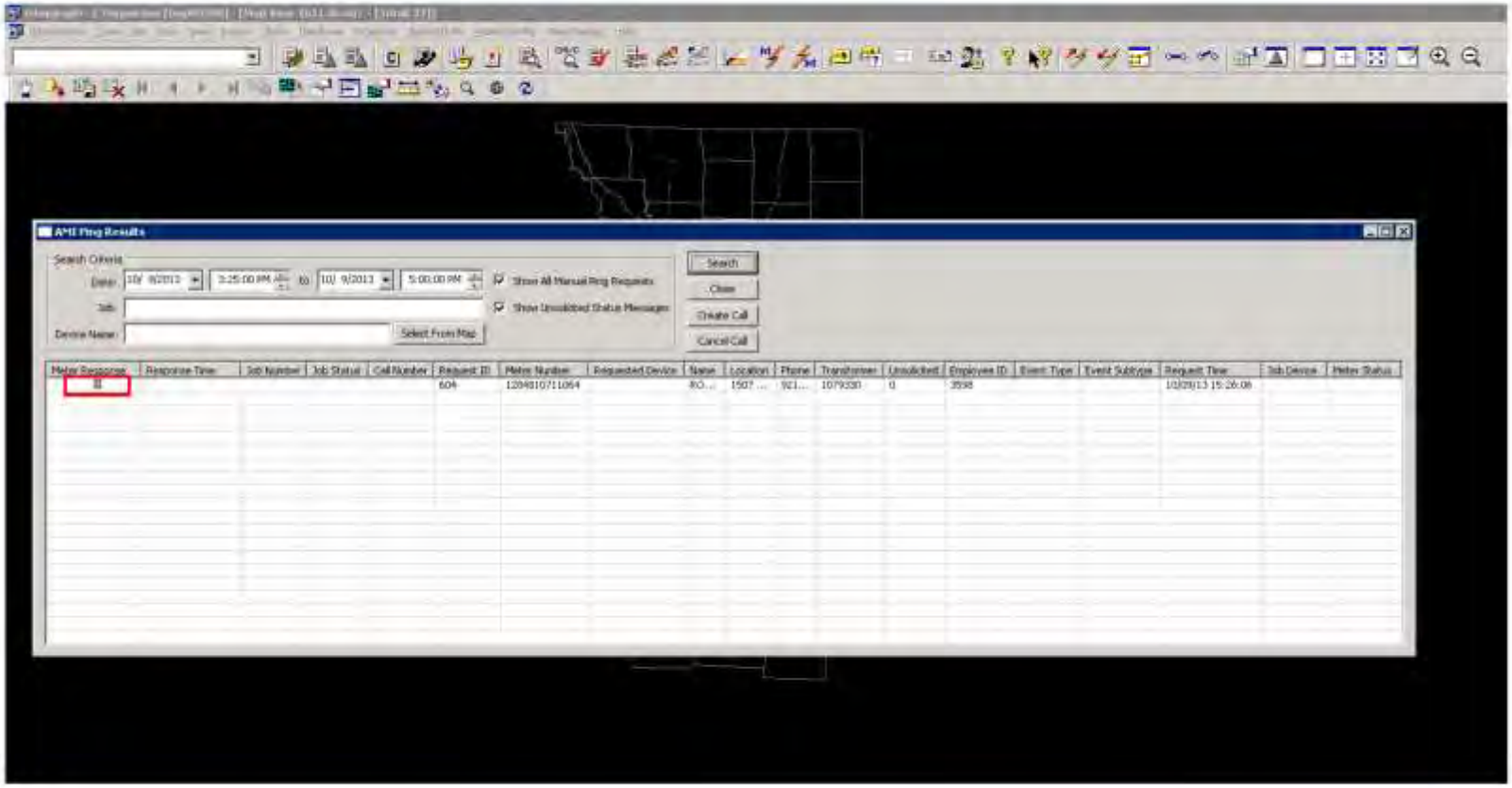
Send Meter Ping Request



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

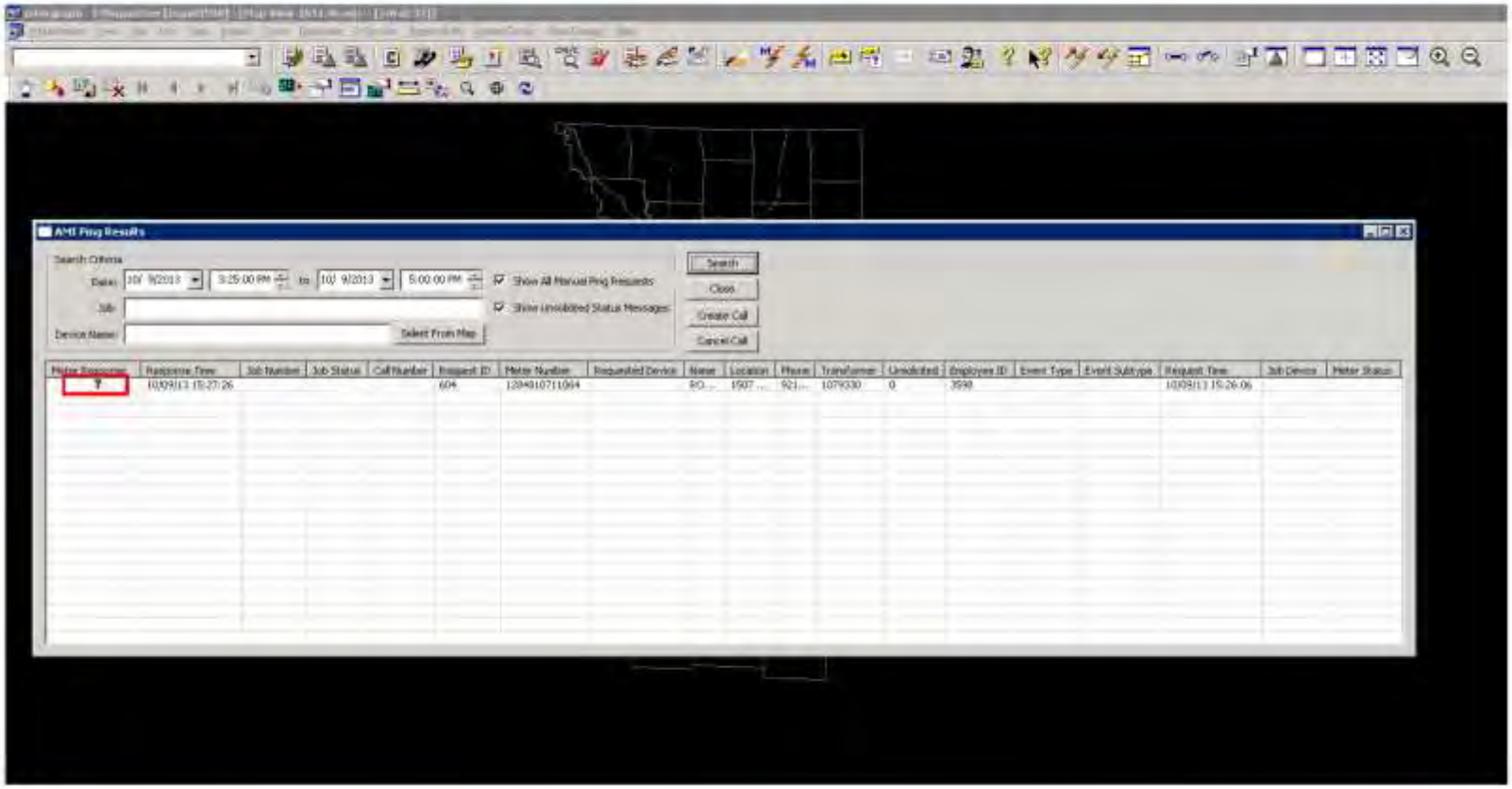
KCP&L energizing life

Meter Ping Request in "AMI Ping Results"



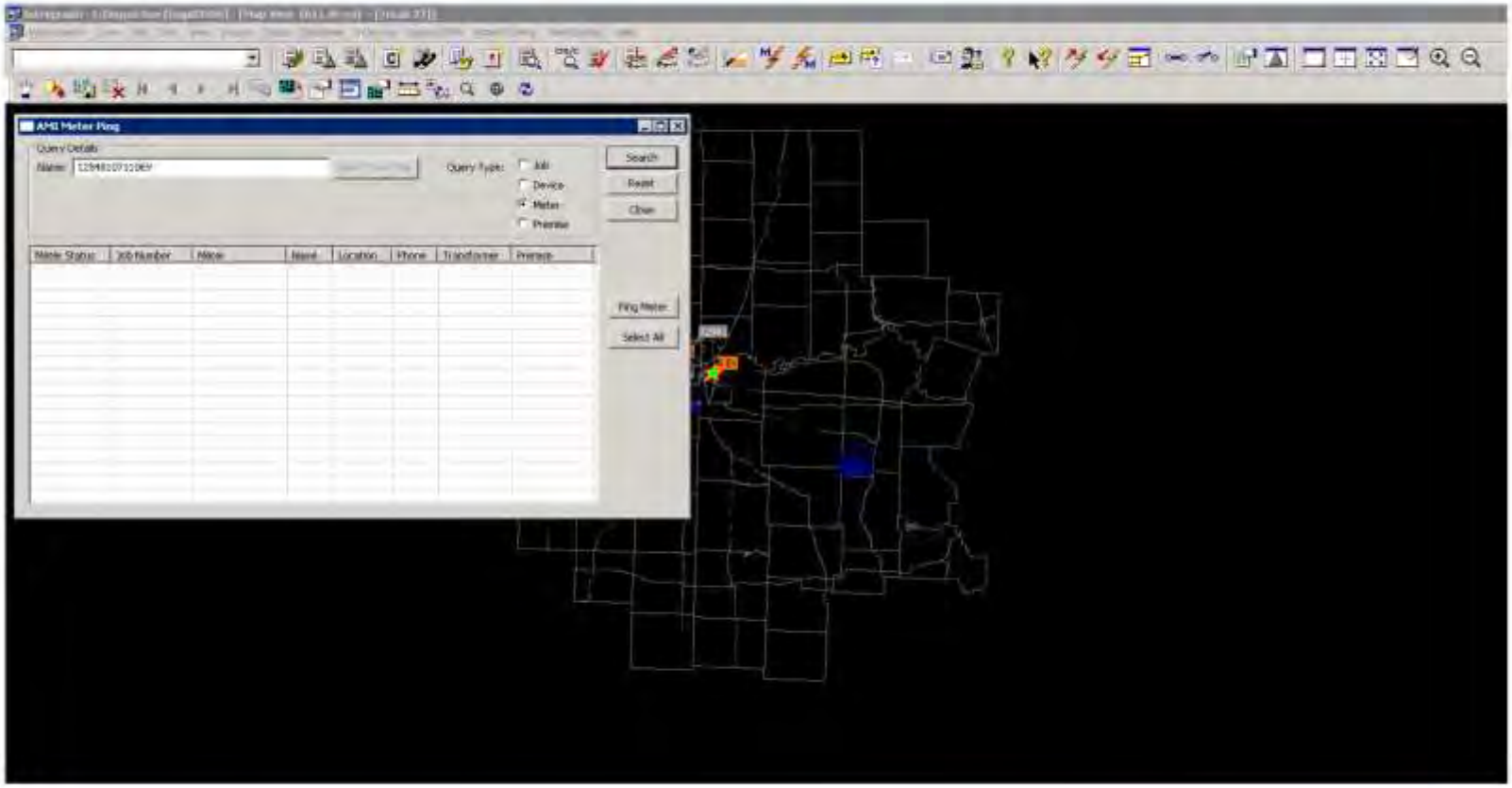
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Received Meter Ping Response



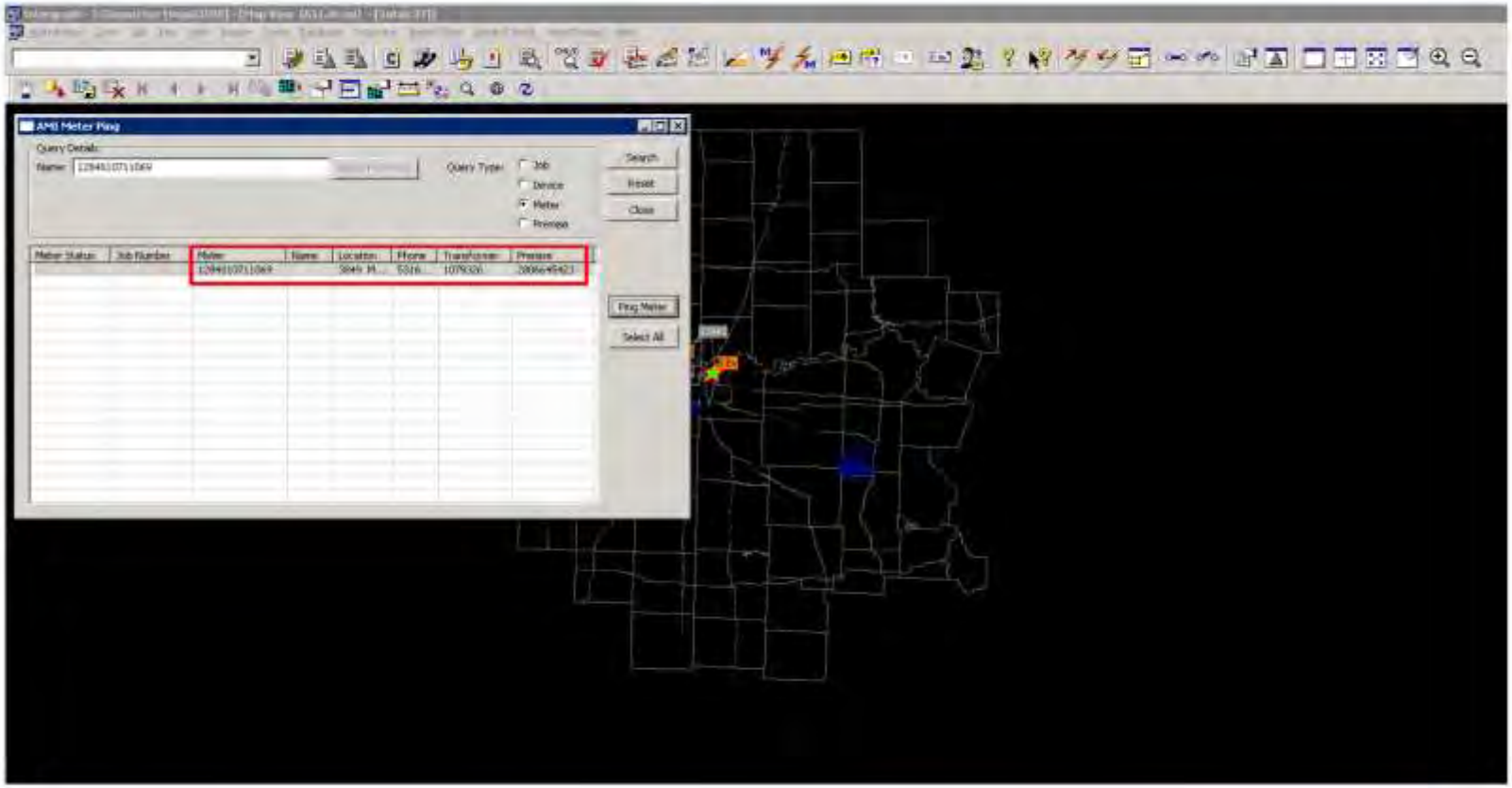
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Scenario #3: Meter is "De-energized" in CIS



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

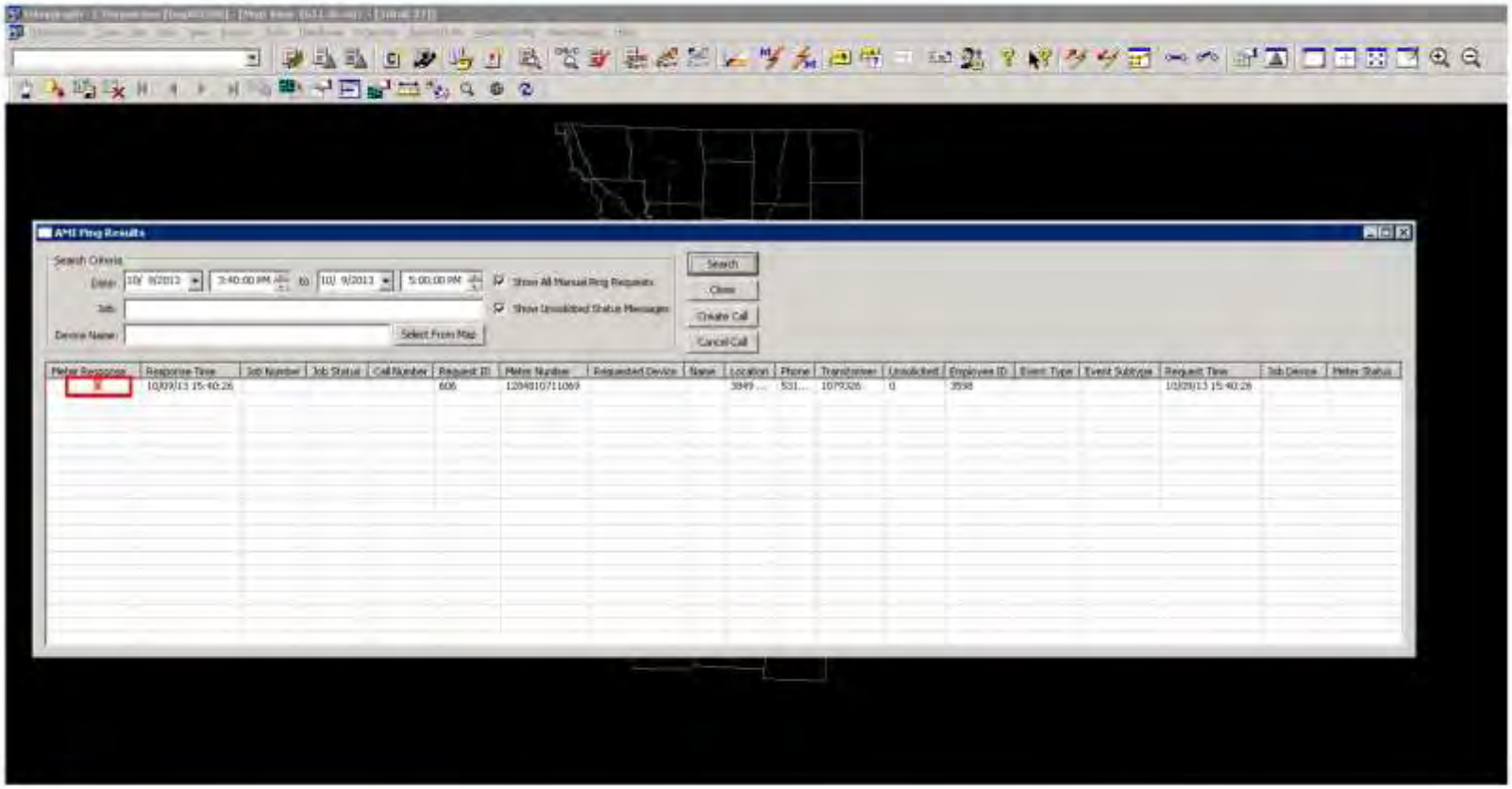
Send Meter Ping Request



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

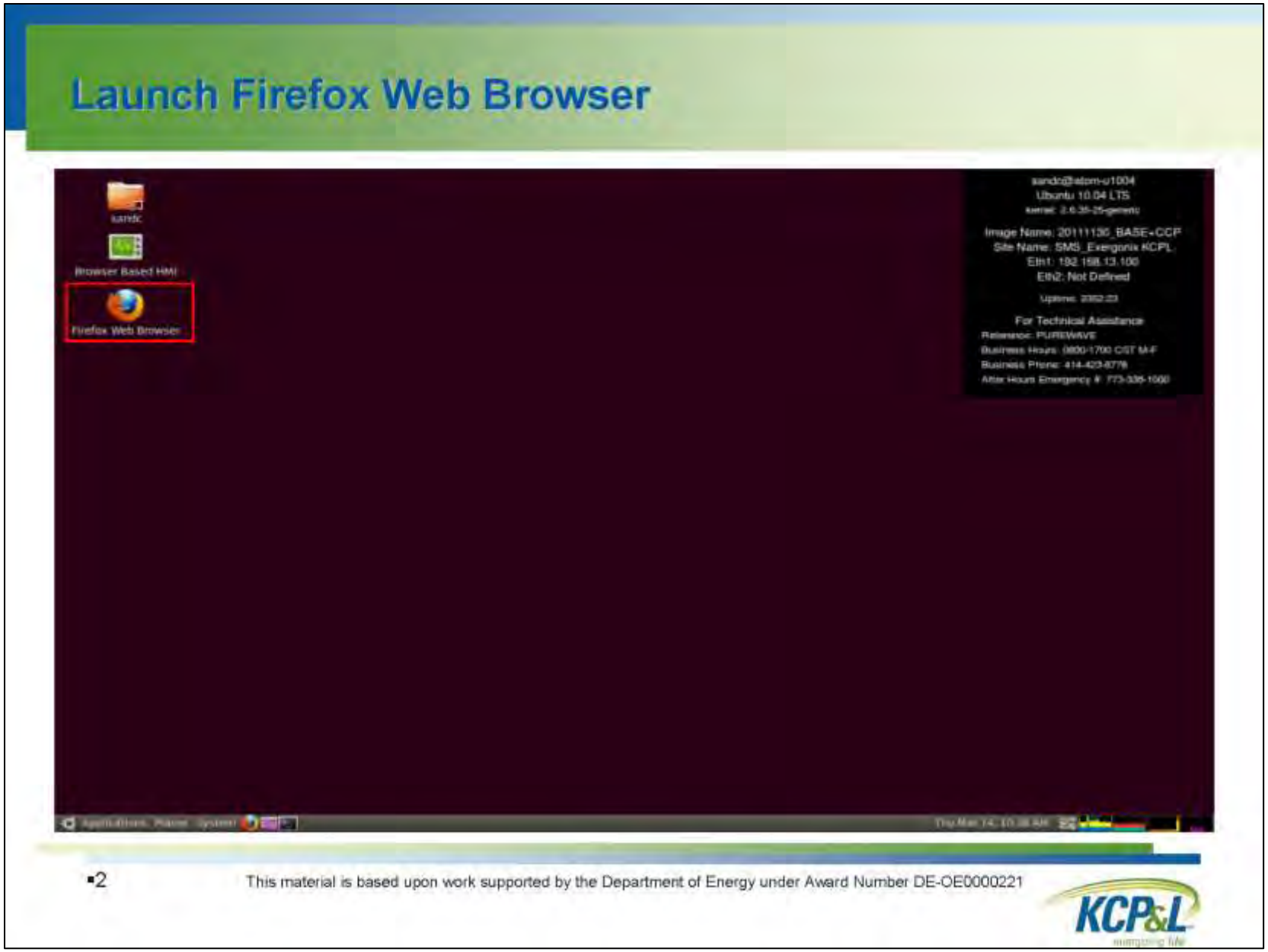
KCP&L energizing life

Meter Ping Request/Response in "AMI Ping Results"

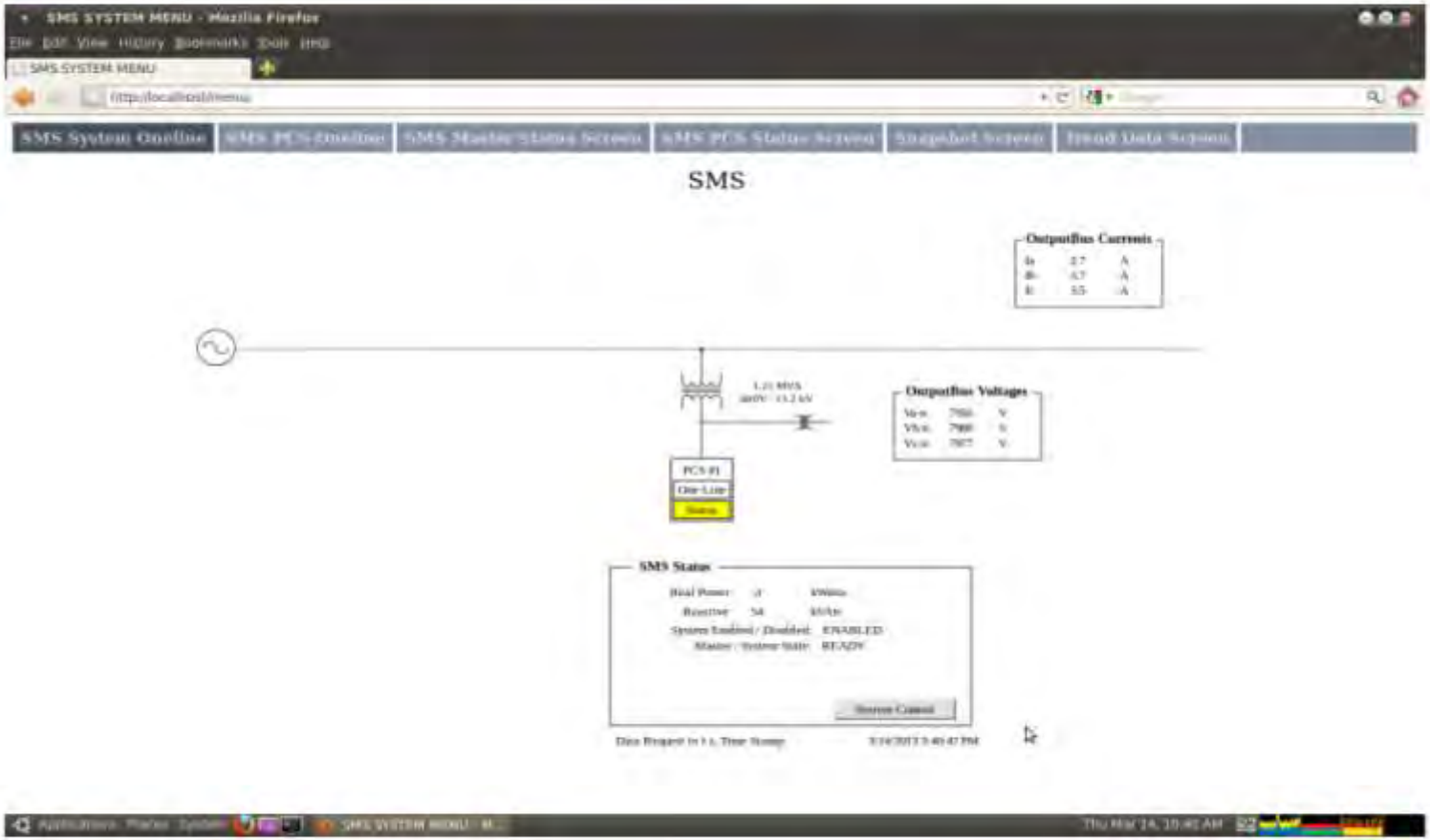


This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221


Battery Operation: Local Control
- KC Green Impact Zone Initiative
- DOE Regional SmartGrid Demonstration Program
- EPRI SmartGrid Demonstration Program
KCP&L
SmartGrid
the future of energy

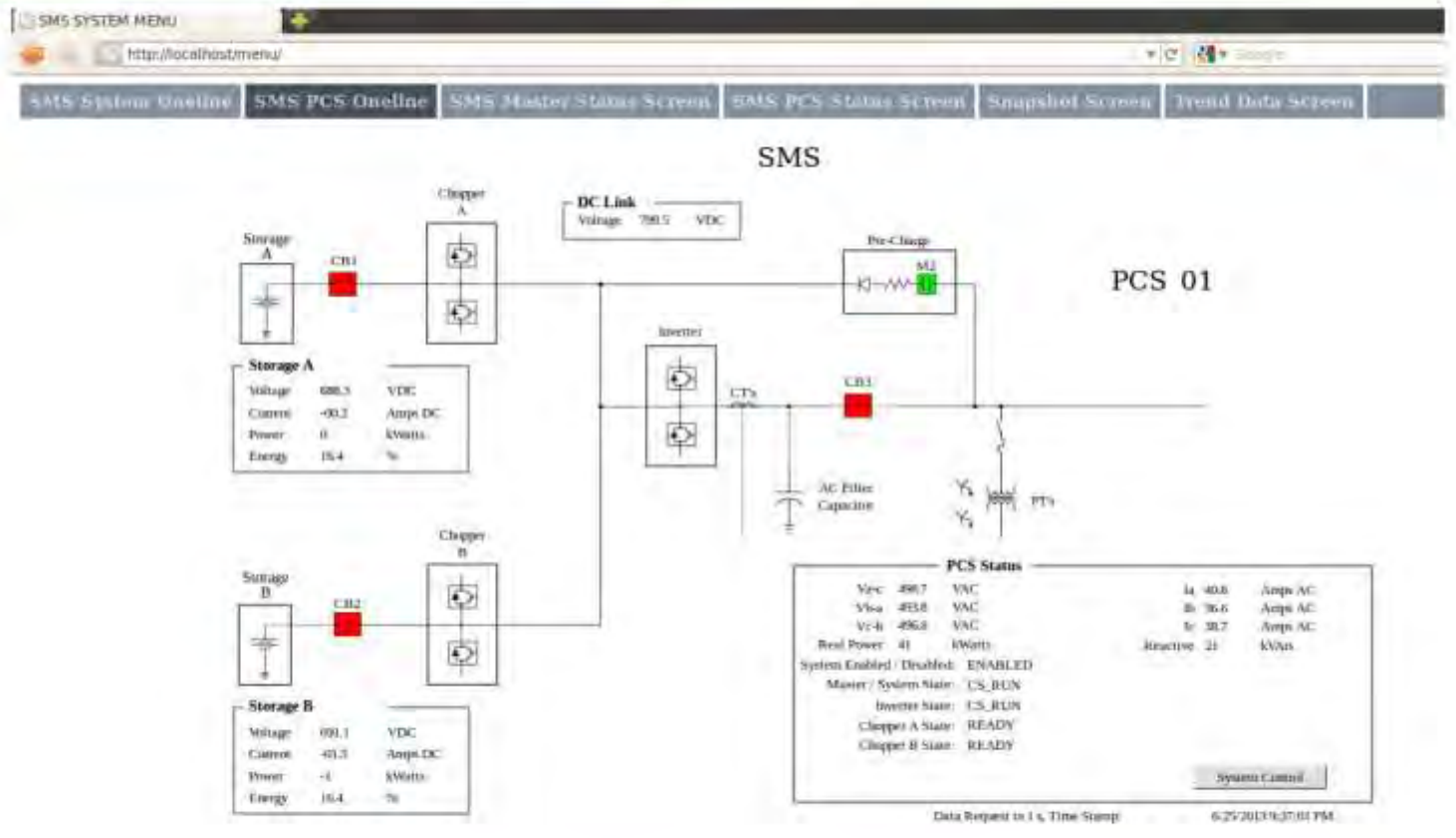

Launch Firefox Web Browser
sandc
Browser Based HMI
Firefox Web Browser
Ubuntu 10.04 LTS
For Technical Assistance
▪2
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

SMS System Menu Main Screen

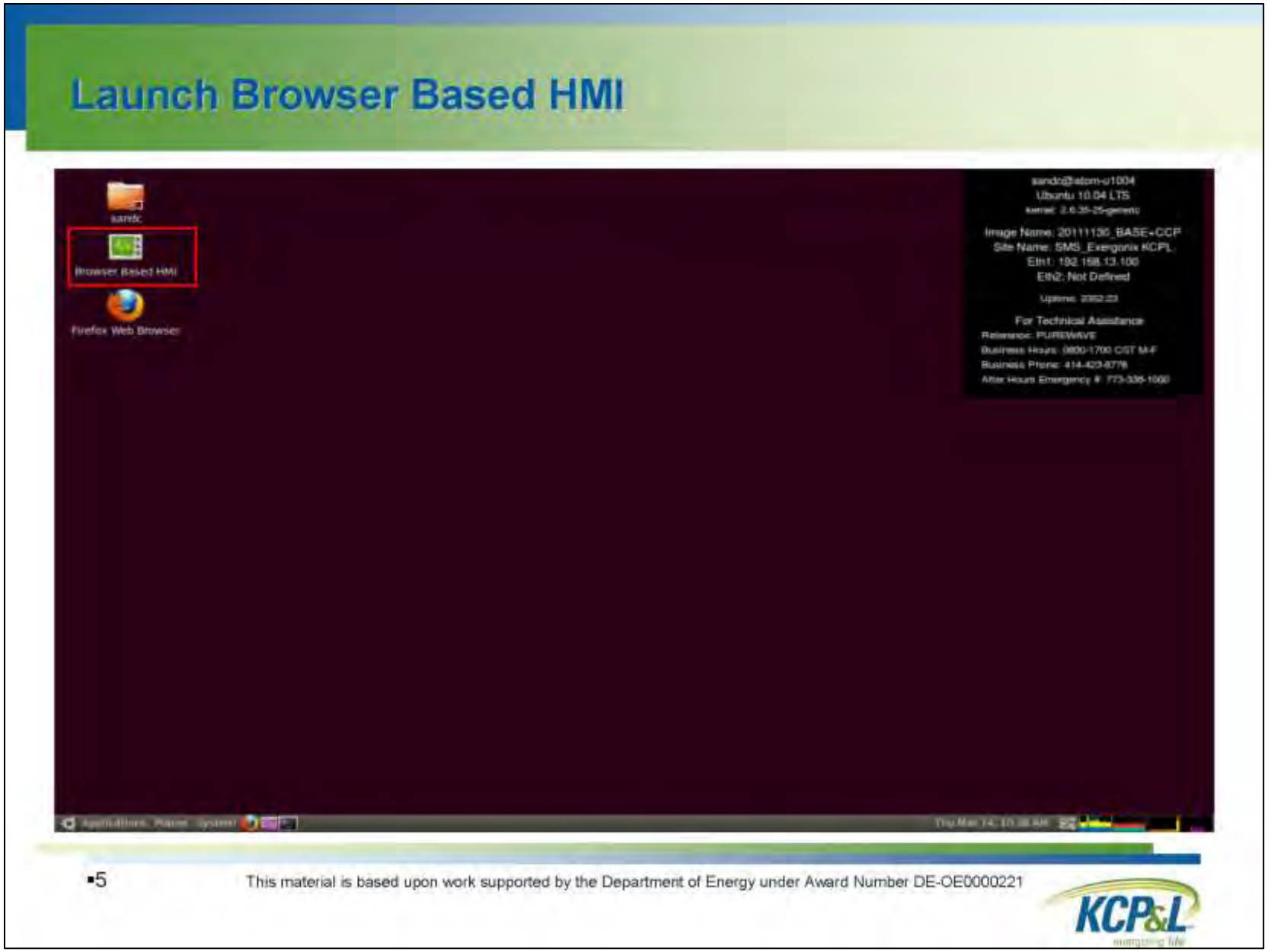


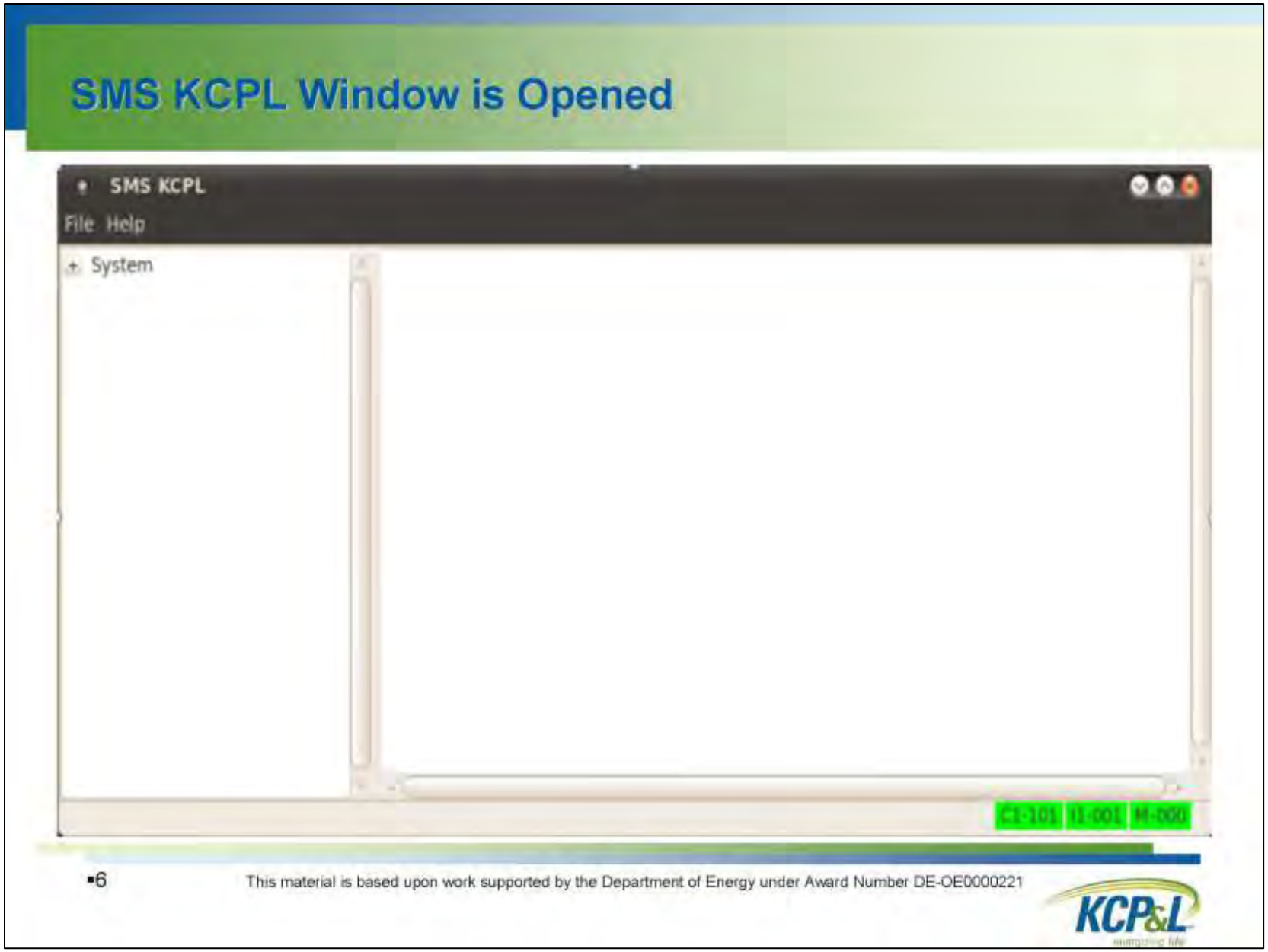
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

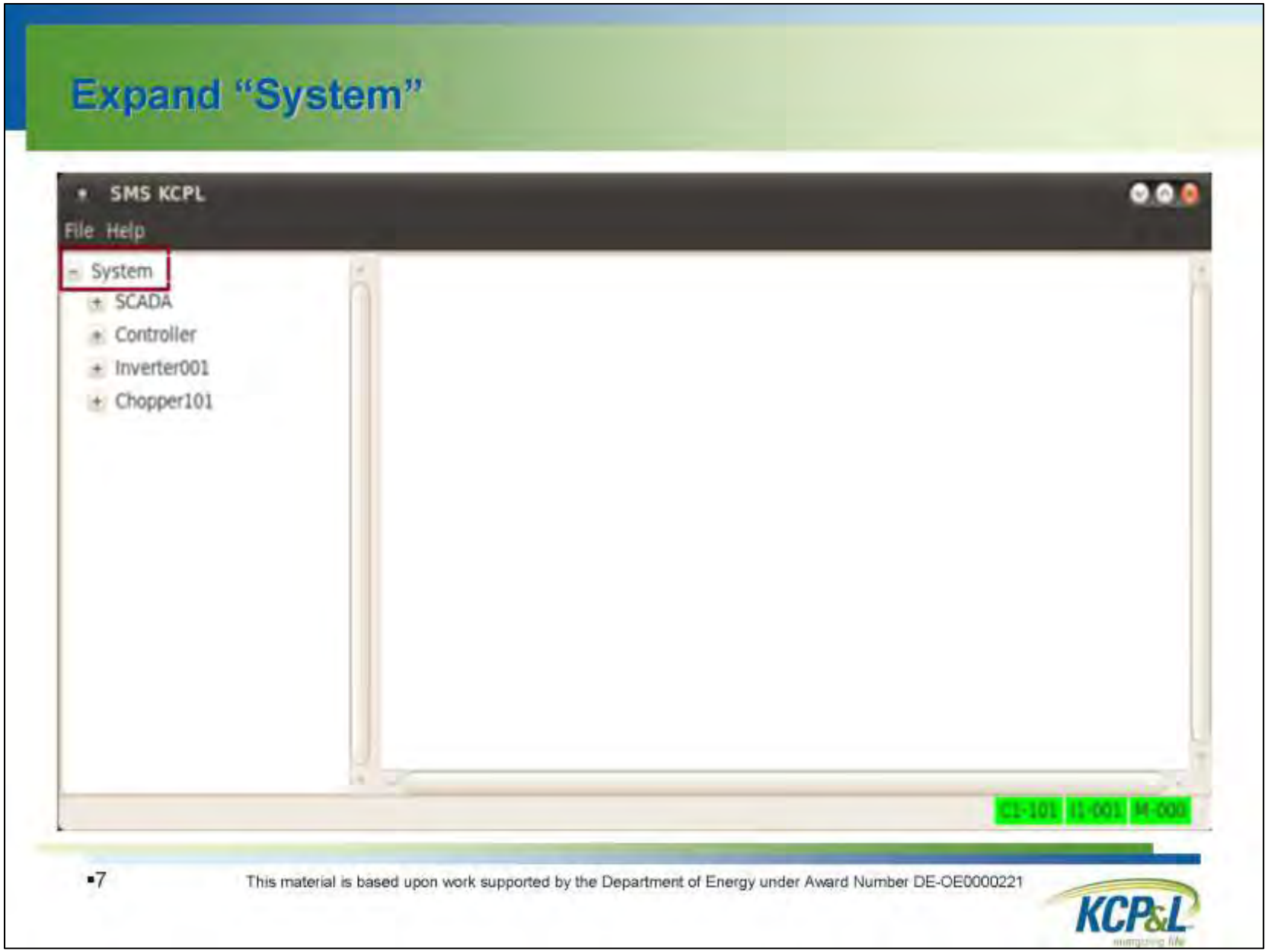
Open SMS PCS Oneline

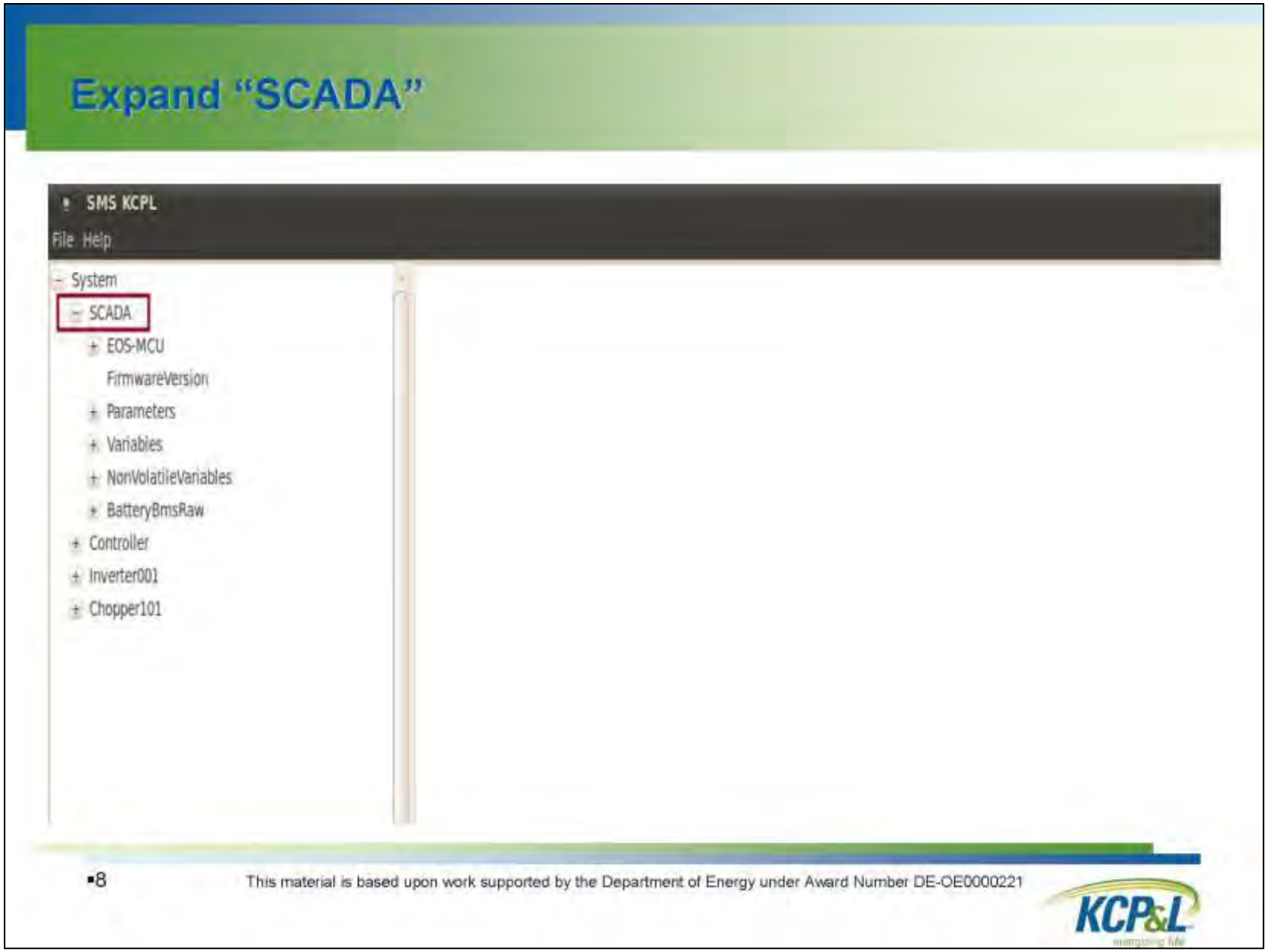


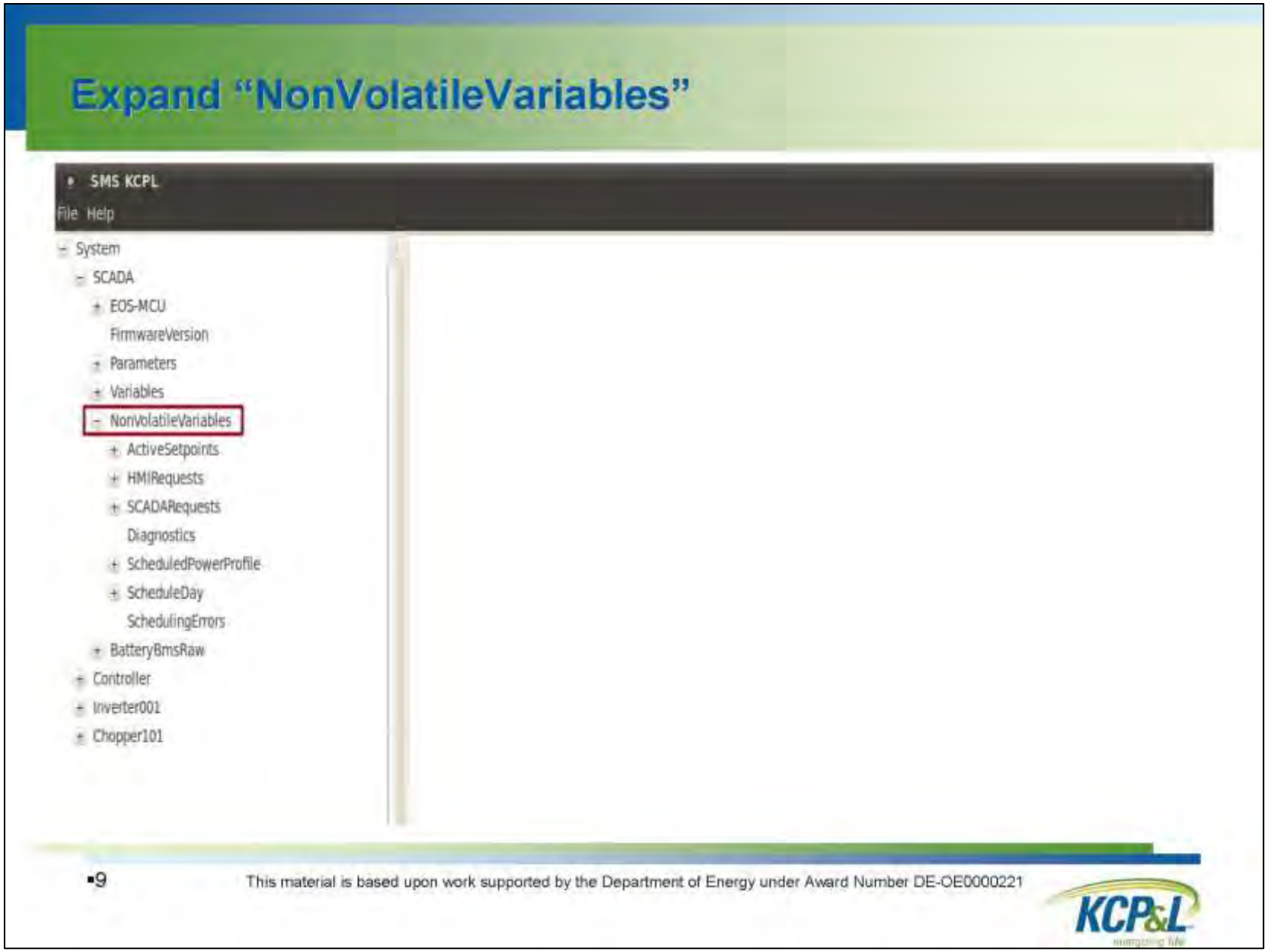
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

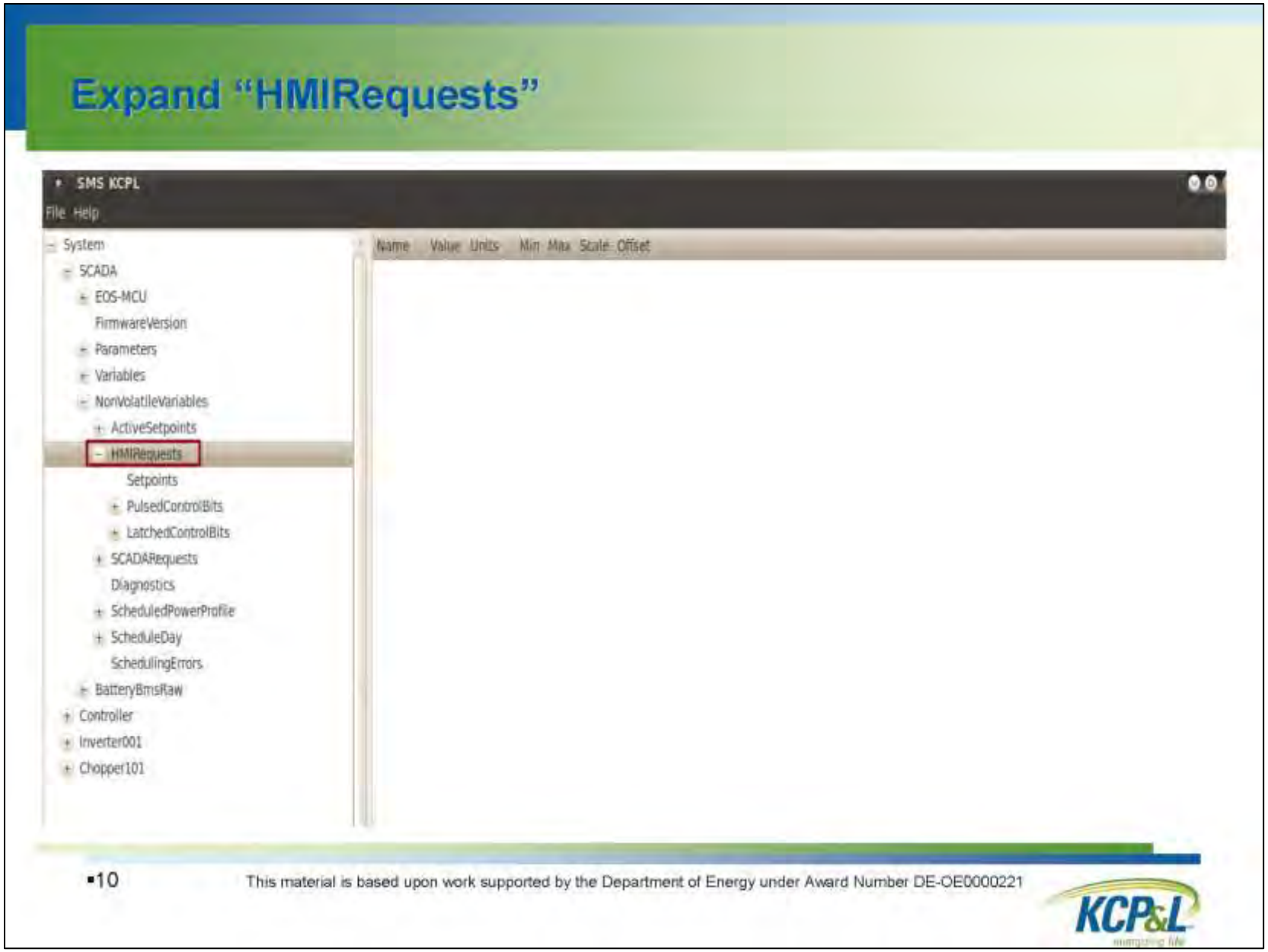

Launch Browser Based HMI
sandc
Browser Based HMI
Firefox Web Browser
Ubuntu 10.04 LTS
Image Name: 20111130_BASE+CCF
Site Name: SMS_Exergonix KCPL
Eth1: 192.168.13.100
Eth2: Not Defined
For Technical Assistance
5
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L
energizing life

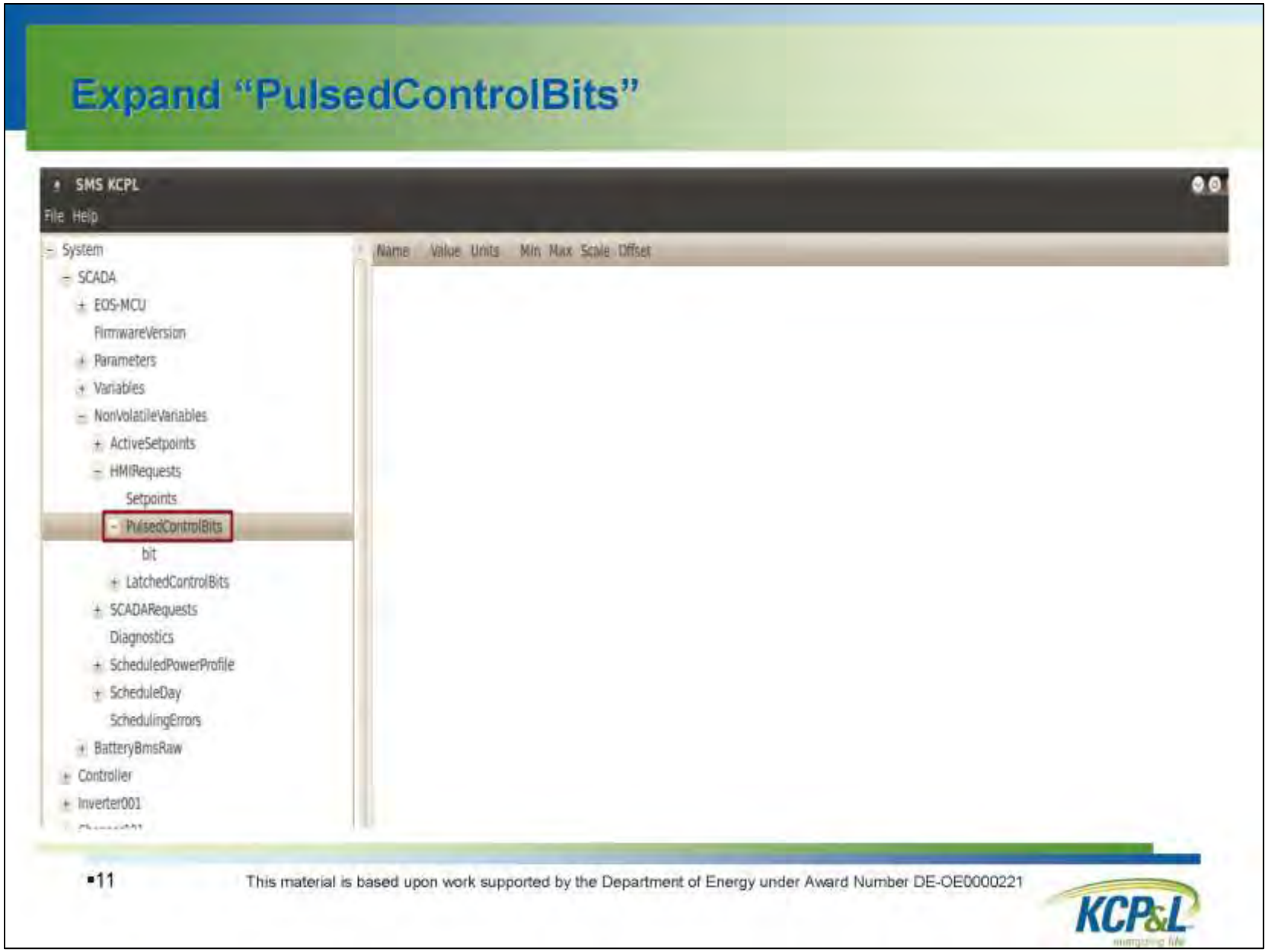

SMS KCPL Window is Opened
SMS KCPL
File Help
System
C1-101
I1-001
M-000
6
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

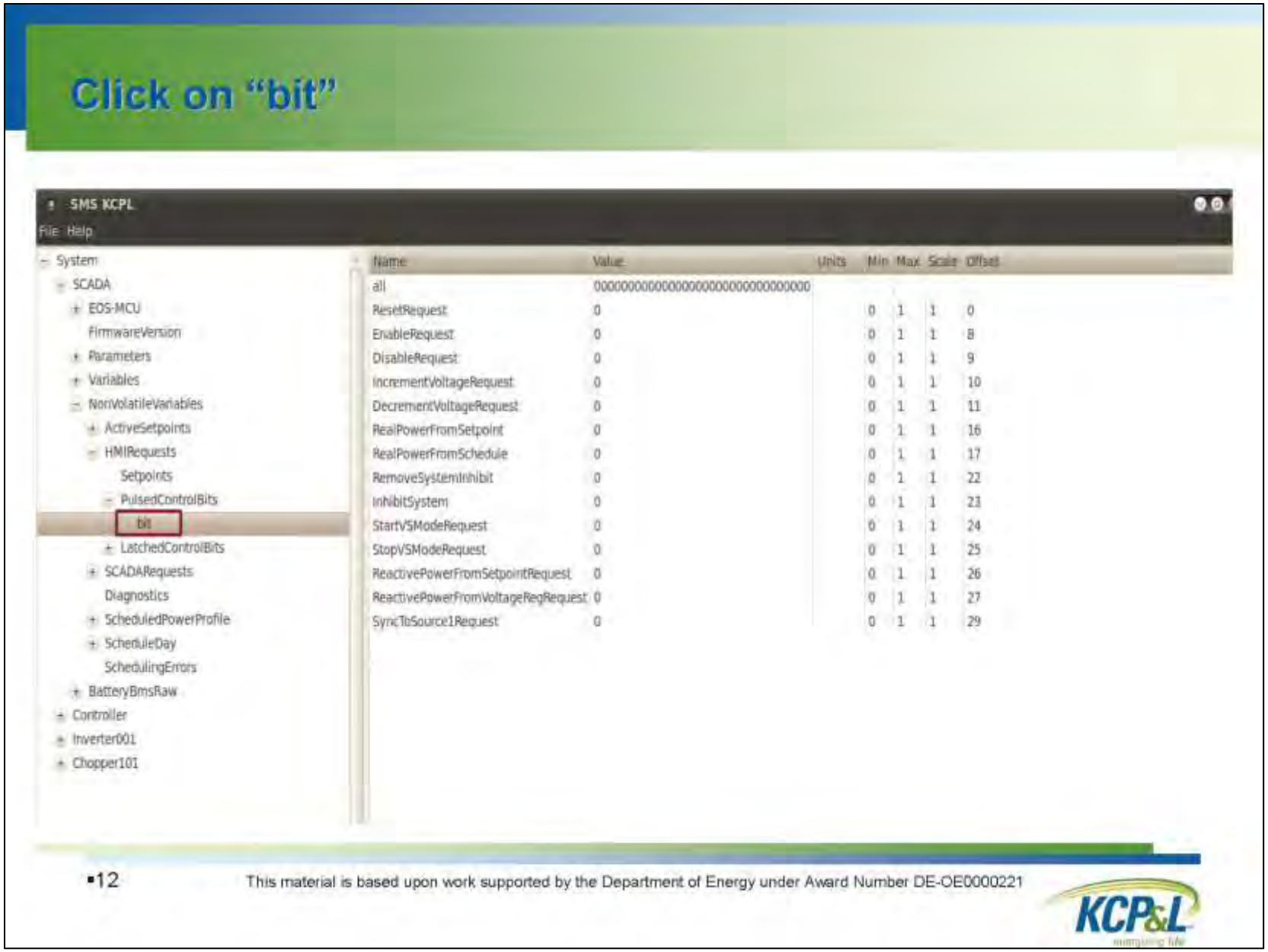

Expand "System"
SMS KCPL
File Help
System
SCADA
Controller
Inverter001
Chopper101
7
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L


Expand "SCADA"
SMS KCPL
File Help
System
SCADA
EOS-MCU
FirmwareVersion
Parameters
Variables
NonVolatileVariables
BatteryBmsRaw
Controller
Inverter001
Chopper101
8
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

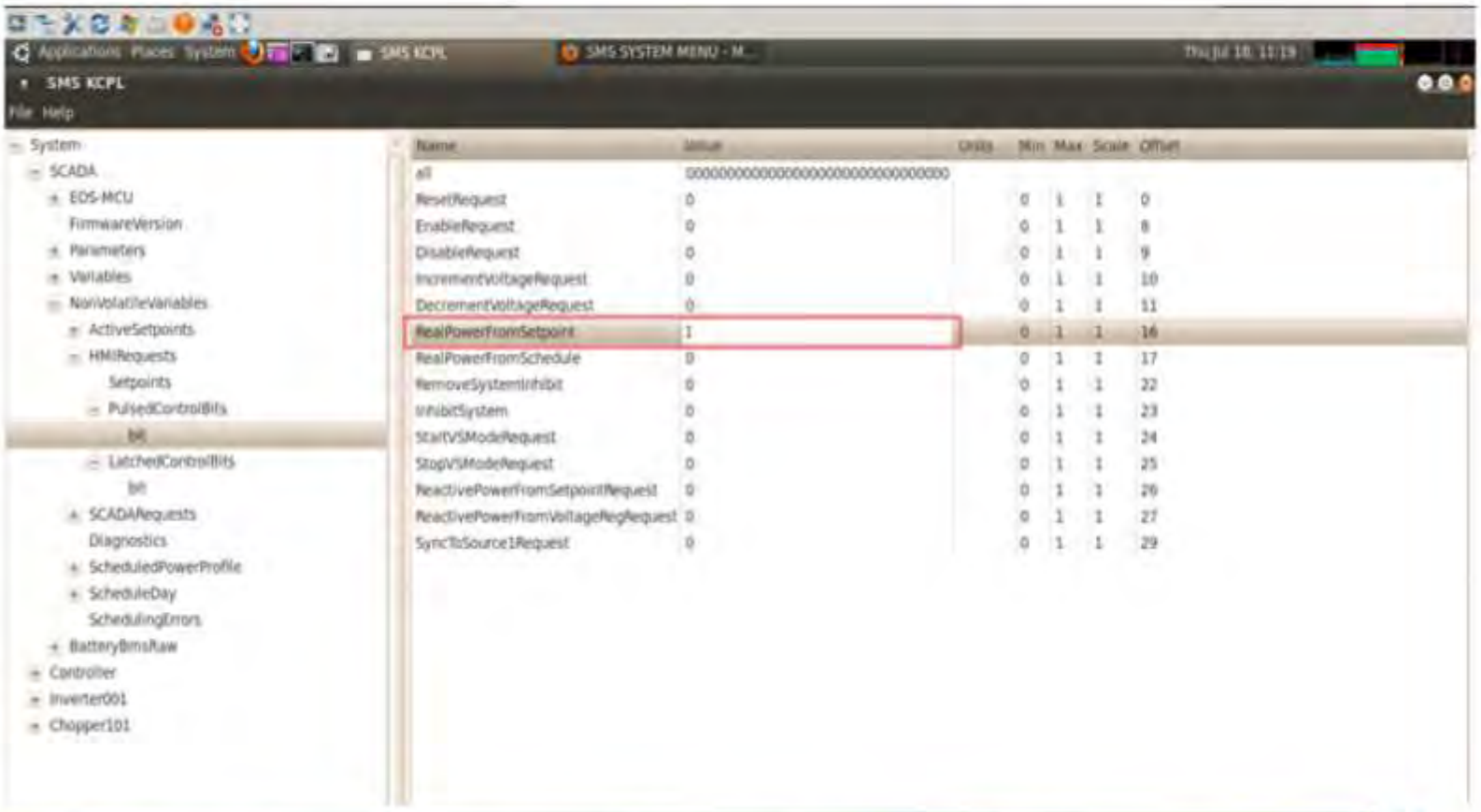

Expand "NonVolatileVariables"
SMS KCPL
File Help
System
SCADA
EOS-MCU
FirmwareVersion
Parameters
Variables
NonVolatileVariables
ActiveSetpoints
HMIRequests
SCADARequests
Diagnostics
ScheduledPowerProfile
ScheduleDay
SchedulingErrors
BatteryBmsRaw
Controller
Inverter001
Chopper101
9
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L


Expand "HMIRequests"
SMS KCPL
File Help
System
SCADA
EOS-MCU
FirmwareVersion
Parameters
Variables
NonVolatileVariables
ActiveSetpoints
HMIRequests
Setpoints
PulsedControlBits
LatchedControlBits
SCADARequests
Diagnostics
ScheduledPowerProfile
ScheduleDay
SchedulingErrors
BatteryBmsRaw
Controller
Inverter001
Chopper101
Name Value Units Min Max Scale Offset
10
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

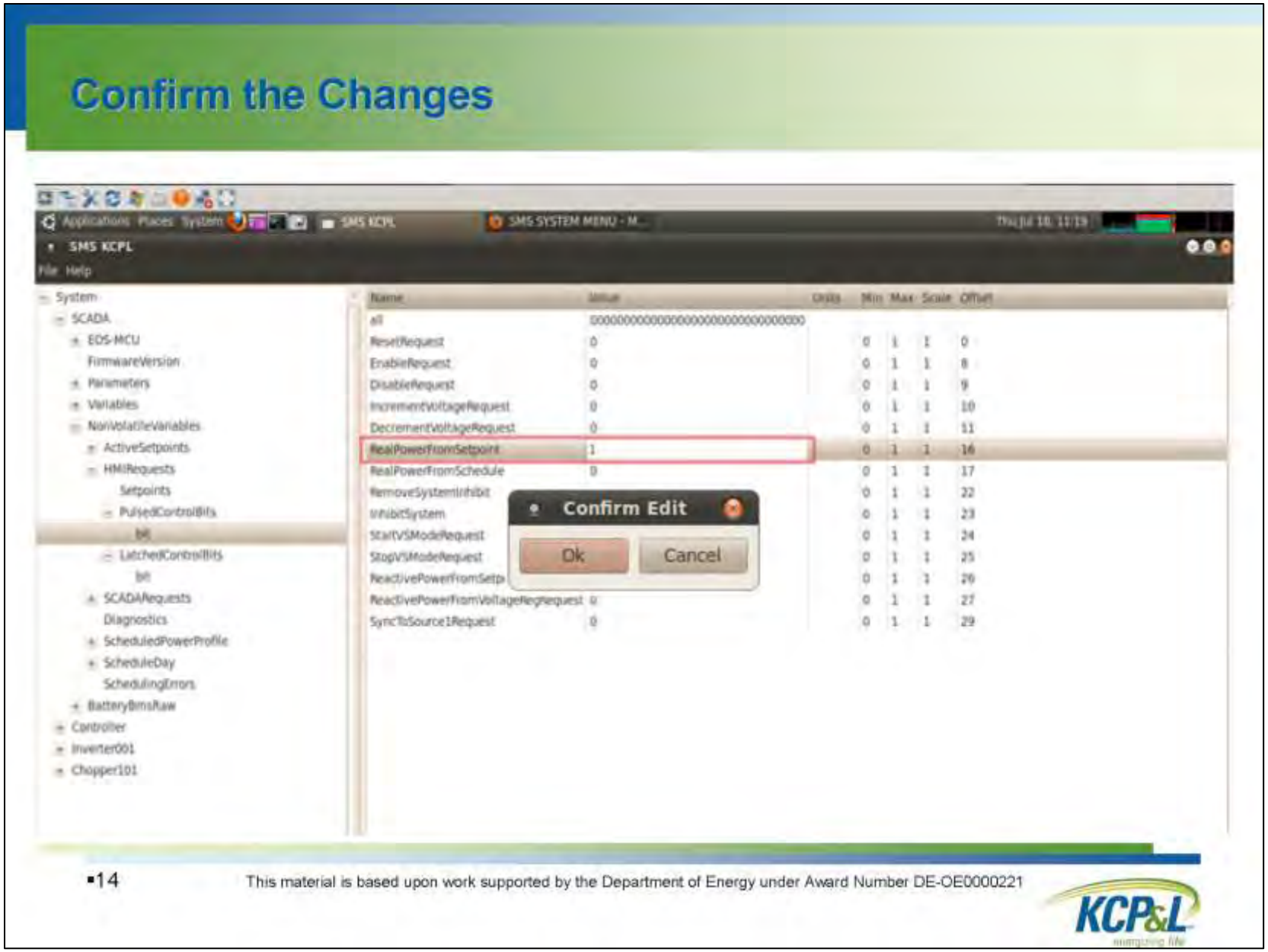

Expand "PulsedControlBits"
SMS KCPL
File Help
System
SCADA
EOS-MCU
FirmwareVersion
Parameters
Variables
NonVolatileVariables
ActiveSetpoints
HMIRequests
Setpoints
PulsedControlBits
bit
LatchedControlBits
SCADARequests
Diagnostics
ScheduledPowerProfile
ScheduleDay
SchedulingErrors
BatteryBmsRaw
Controller
Inverter001
Name Value Units Min Max Scale Offset
11
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

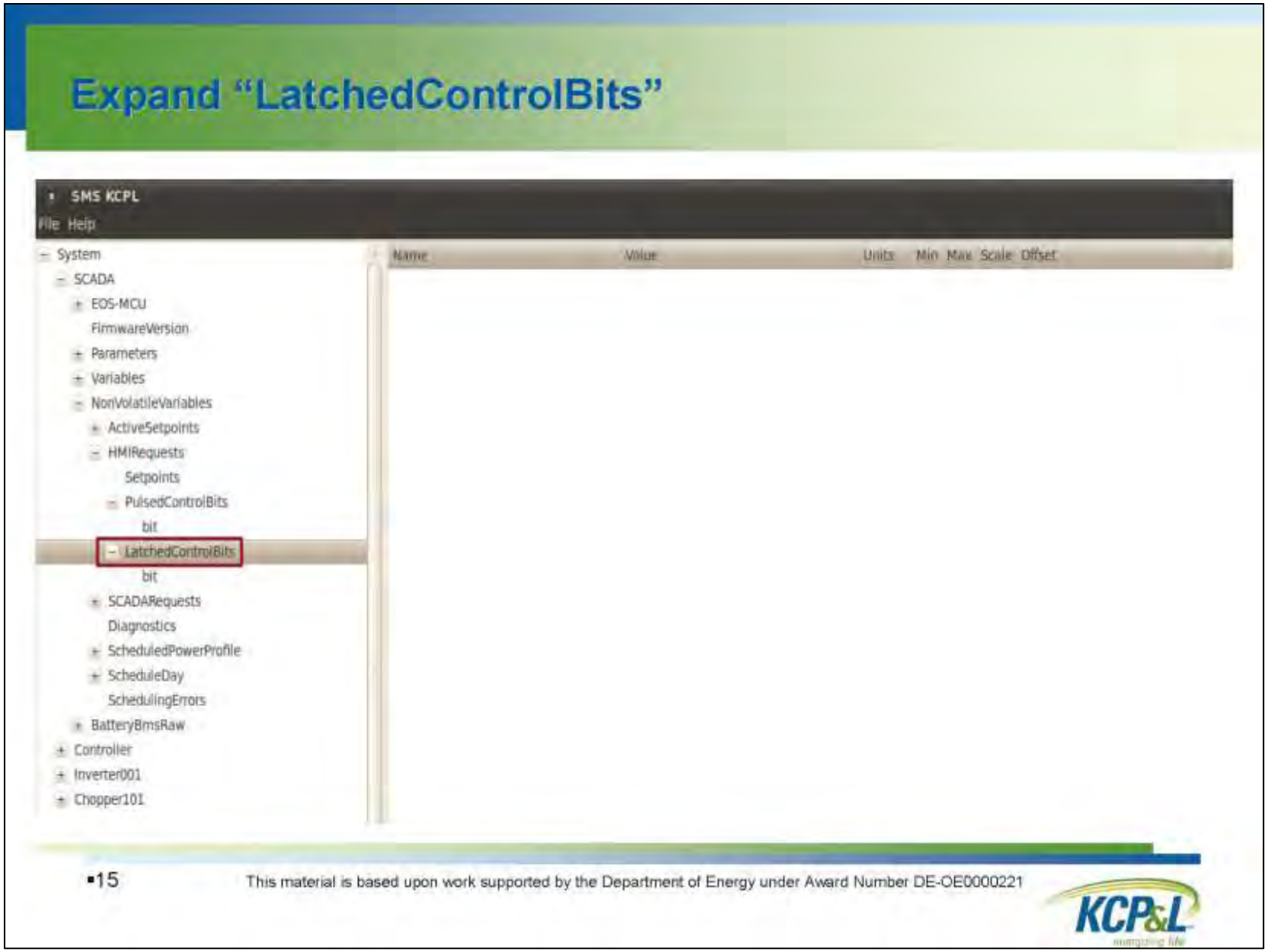

Click on "bit"
SMS KCPL
File Help
System
SCADA
EOS-MCU
FirmwareVersion
Parameters
Variables
NonVolatileVariables
ActiveSetpoints
HMIRequests
Setpoints
PulsedControlBits
bit
LatchedControlBits
SCADARequests
Diagnostics
ScheduledPowerProfile
ScheduleDay
SchedulingErrors
BatteryBmsRaw
Controller
Inverter001
Chopper101
Name Value Units Min Max Scale Offset
all 00000000000000000000000000000000
ResetRequest 0 0 1 1 0
EnableRequest 0 0 1 1 8
DisableRequest 0 0 1 1 9
IncrementVoltageRequest 0 0 1 1 10
DecrementVoltageRequest 0 0 1 1 11
RealPowerFromSetpoint 0 0 1 1 16
RealPowerFromSchedule 0 0 1 1 17
RemoveSystemInhibit 0 0 1 1 22
InhibitSystem 0 0 1 1 23
StartVSModeRequest 0 0 1 1 24
StopVSModeRequest 0 0 1 1 25
ReactivePowerFromSetpointRequest 0 0 1 1 26
ReactivePowerFromVoltageRegRequest 0 0 1 1 27
SyncToSource1Request 0 0 1 1 29
12
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

Set RealPowerFromSetpoint Value to 1

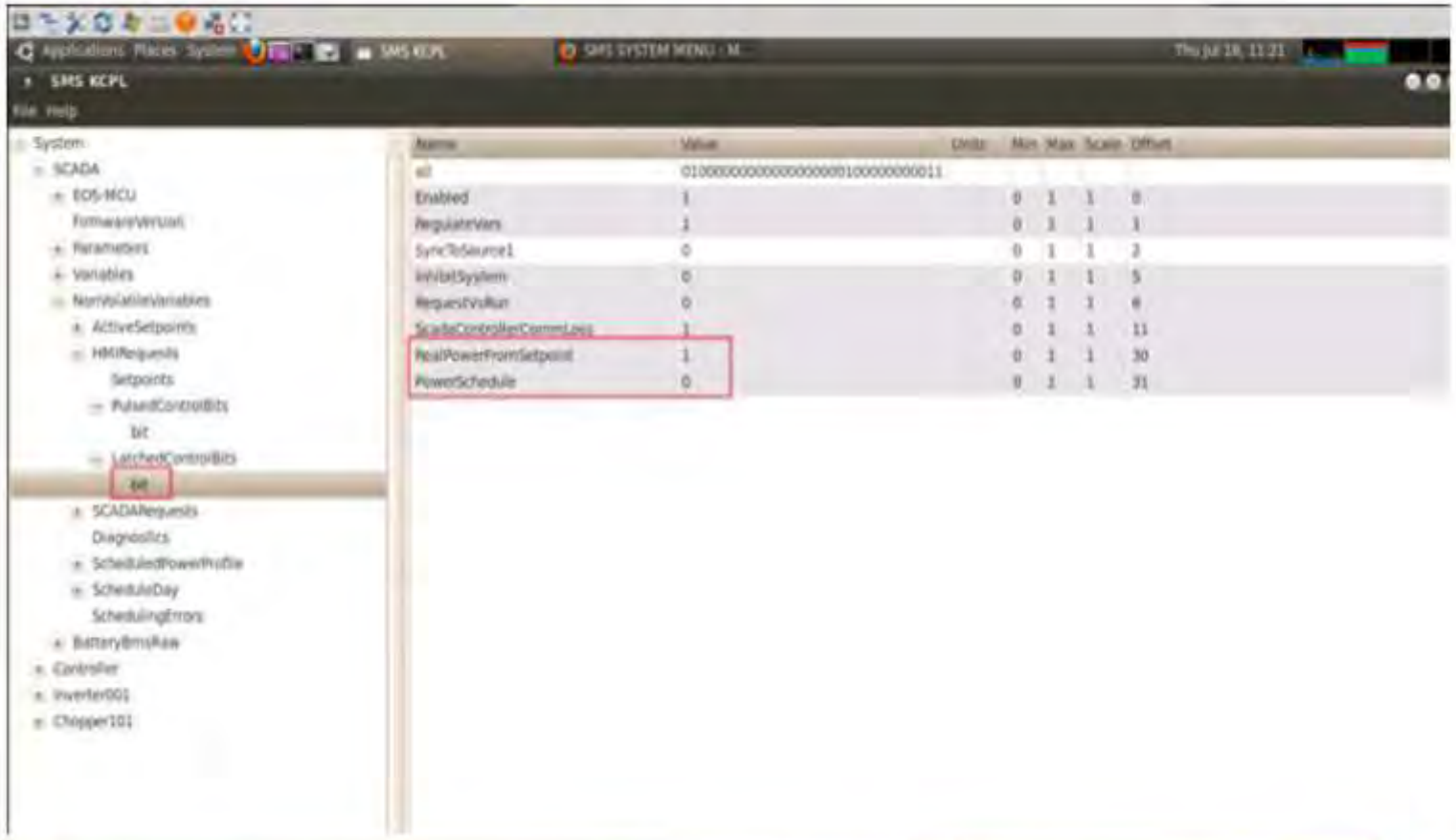


This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

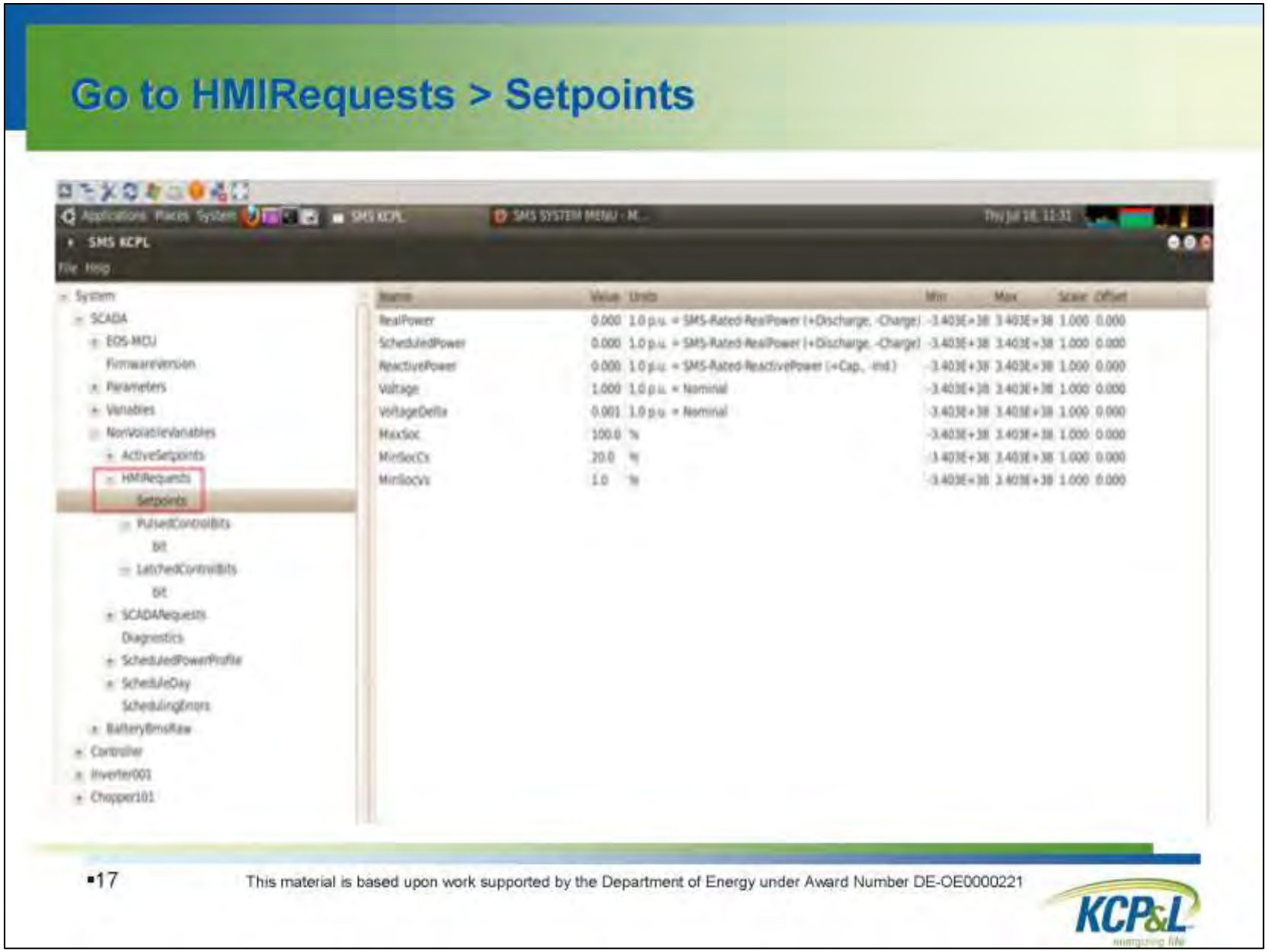

Confirm the Changes
SMS KCPL
File Help
System
SCADA
EDS-MCU
FirmwareVersion
Parameters
Variables
NonVolatileVariables
ActiveSetpoints
HMIRequests
Setpoints
PulsedControlBits
bit
LatchedControlBits
bit
SCADARequests
Diagnostics
ScheduledPowerProfile
ScheduleDay
SchedulingErrors
BatteryBmsRaw
Controller
Inverter001
Chopper101
Name
Value
Units
Min
Max
Scale
Offset
all
ResetRequest
EnableRequest
DisableRequest
IncrementVoltageRequest
DecrementVoltageRequest
RealPowerFromSetpoint
RealPowerFromSchedule
RemoveSystemInhibit
InhibitSystem
StartVSModeRequest
StopVSModeRequest
ReactivePowerFromSetp
ReactivePowerFromVoltageRegRequest
SyncToSource1Request
Confirm Edit
Ok
Cancel
14
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L


Expand "LatchedControlBits"
SMS KCPL
File Help
System
SCADA
EOS-MCU
FirmwareVersion
Parameters
Variables
NonVolatileVariables
ActiveSetpoints
HMIRequests
Setpoints
PulsedControlBits
bit
LatchedControlBits
bit
SCADARequests
Diagnostics
ScheduledPowerProfile
ScheduleDay
SchedulingErrors
BatteryBmsRaw
Controller
Inverter001
Chopper101
Name
Value
Units
Min
Max
Scale
Offset
15
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

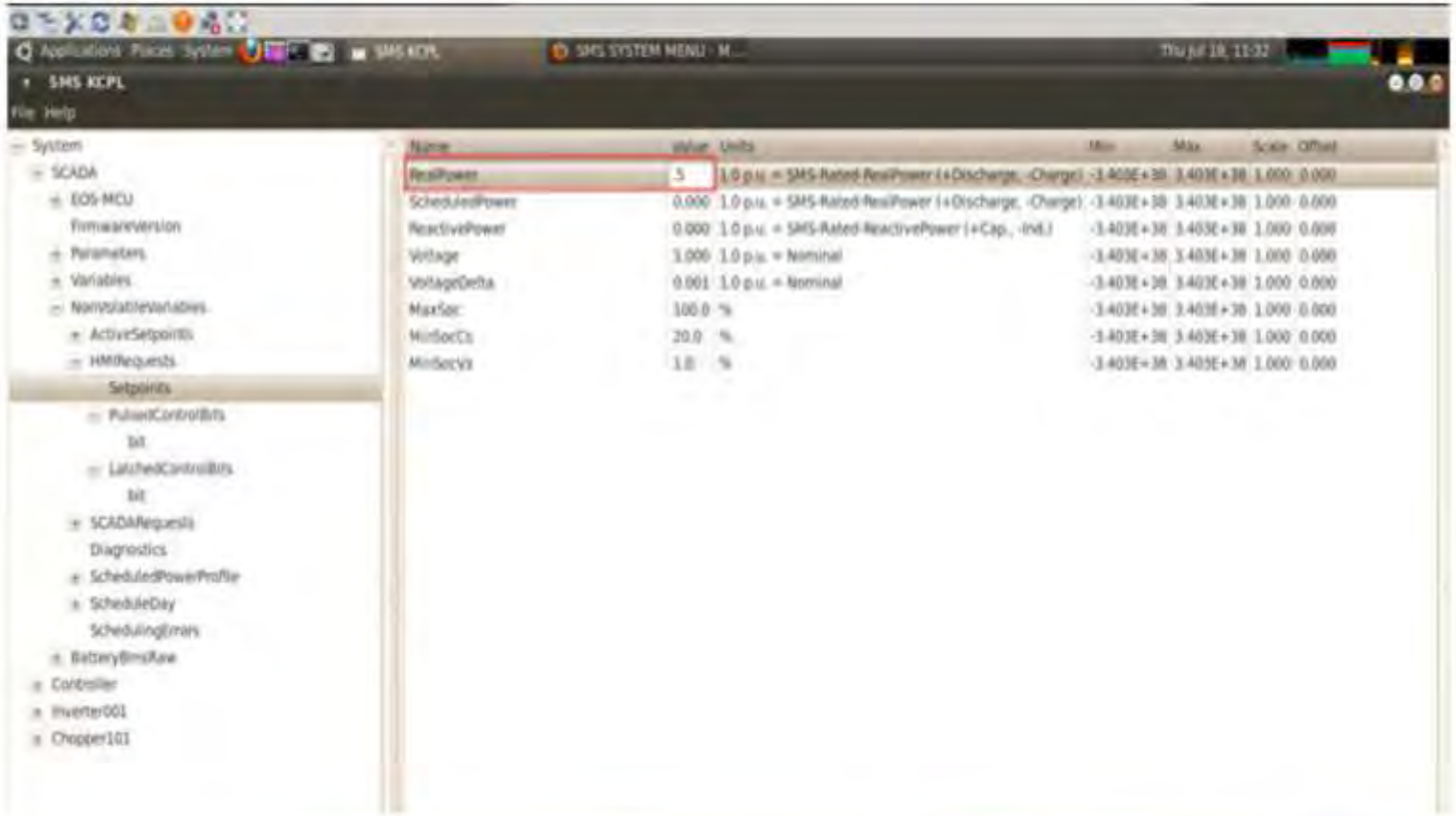
Click on "bit" Verify RealPowerFromSetpoint is 1



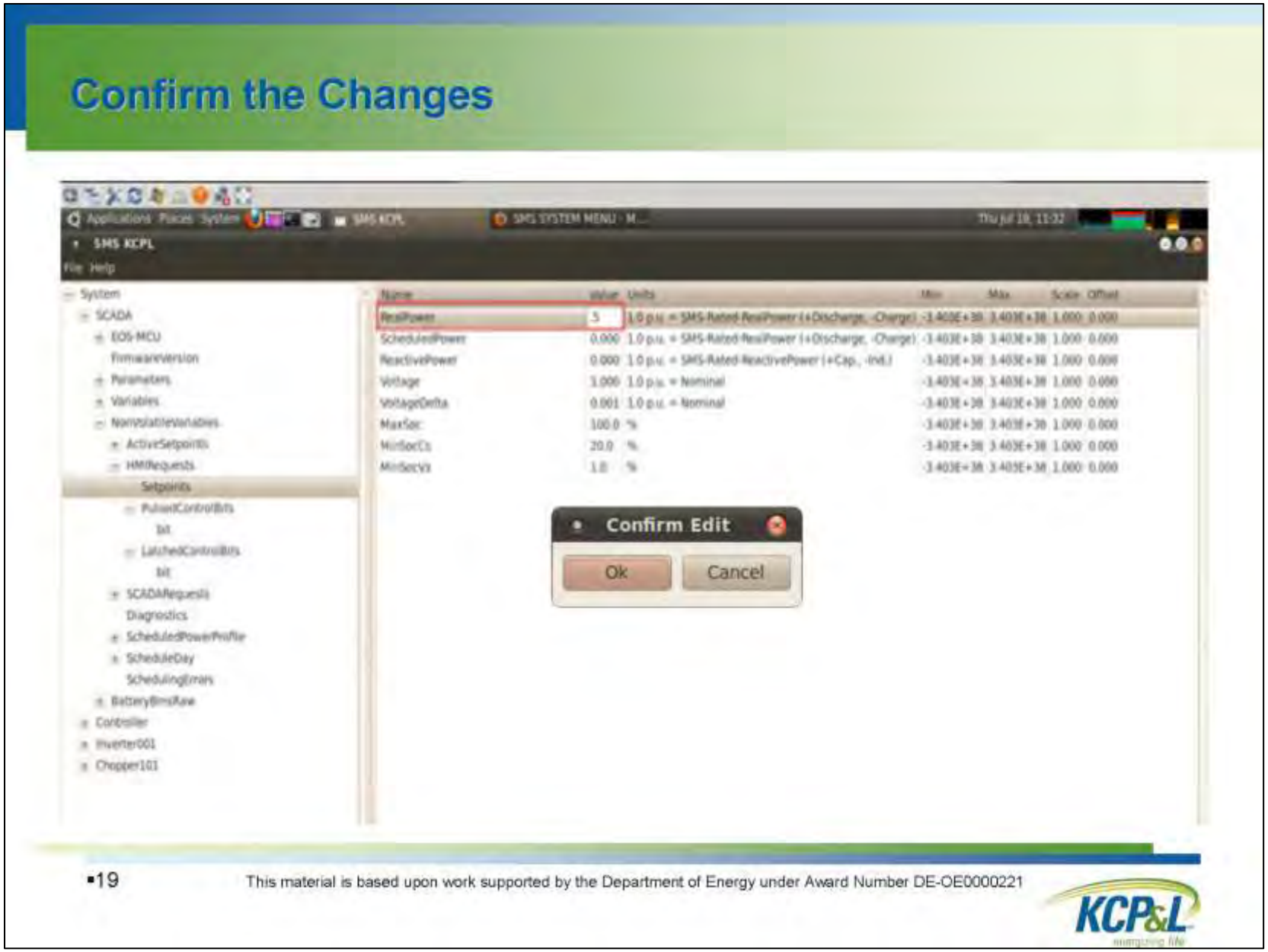
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221


Go to HMIRequests > Setpoints
SMS KCPL
File Help
System
SCADA
EOS-MCU
FirmwareVersion
Parameters
Variables
NonVolatileVariables
ActiveSetpoints
HMIRequests
Setpoints
PulsedControlBits
bit
LatchedControlBits
bit
SCADARequests
Diagnostics
ScheduledPowerProfile
ScheduleDay
SchedulingErrors
BatteryBmsRaw
Controller
Inverter001
Chopper101
Name Value Units Min Max Scale Offset
RealPower 0.000 1.0 p.u. = SMS-Rated-RealPower (+Discharge, -Charge) -3.403E+38 3.403E+38 1.000 0.000
ScheduledPower 0.000 1.0 p.u. = SMS-Rated-RealPower (+Discharge, -Charge) -3.403E+38 3.403E+38 1.000 0.000
ReactivePower 0.000 1.0 p.u. = SMS-Rated-ReactivePower (+Cap., -Ind.) -3.403E+38 3.403E+38 1.000 0.000
Voltage 1.000 1.0 p.u. = Nominal -3.403E+38 3.403E+38 1.000 0.000
VoltageDelta 0.001 1.0 p.u. = Nominal -3.403E+38 3.403E+38 1.000 0.000
MaxSoc 100.0 % -3.403E+38 3.403E+38 1.000 0.000
MinSocCs 20.0 % -3.403E+38 3.403E+38 1.000 0.000
MinSocVs 1.0 % -3.403E+38 3.403E+38 1.000 0.000
17
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

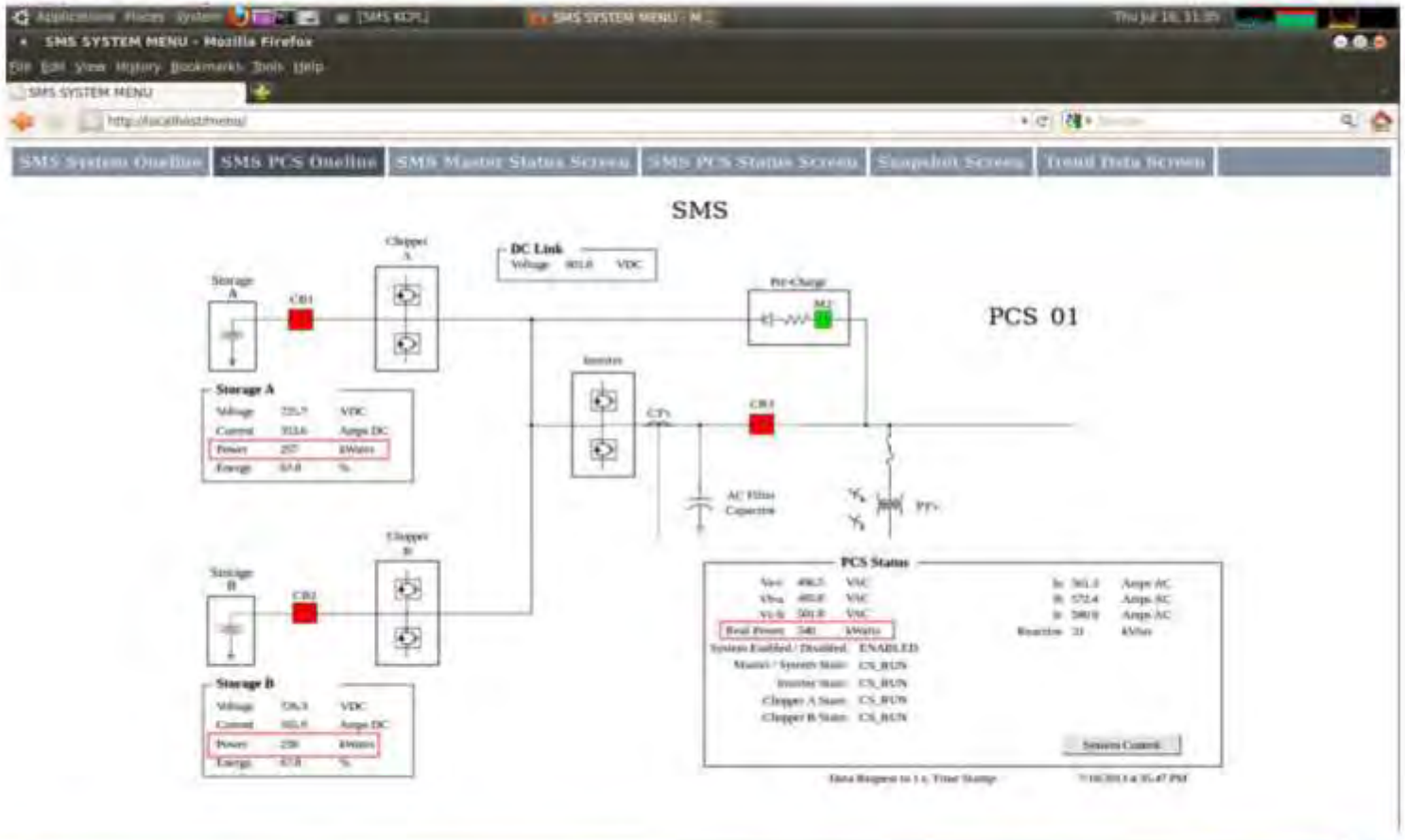
Set the Discharge Value in RealPower Value



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221


Confirm the Changes
SMS KCPL
File Help
System
SCADA
EOS-MCU
FirmwareVersion
Parameters
Variables
NonVolatileVariables
ActiveSetpoints
HMIRequests
Setpoints
Diagnostics
Controller
Inverter001
Chopper101
Name
Value
Units
RealPower
5
ScheduledPower
ReactivePower
Voltage
VoltageDelta
MaxSoc
100.0
MinSocCs
20.0
MinSocV3
Confirm Edit
Ok
Cancel
19
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

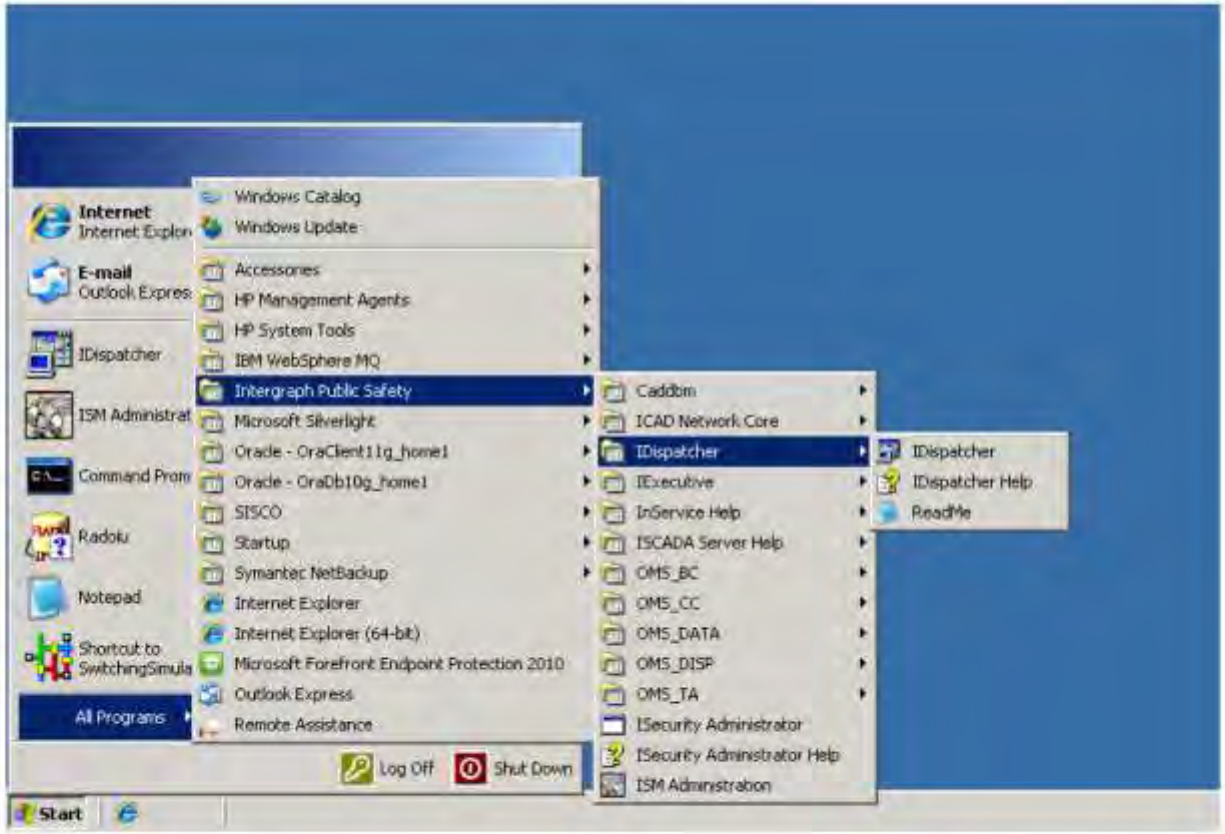
Navigate to SMS PCS Oneline to view Battery Discharging



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221


Battery Operation: Fixed kW Discharge
- KC Green Impact Zone Initiative
- DOE Regional SmartGrid Demonstration Program
- EPRI SmartGrid Demonstration Program
KCP&L
SmartGrid
the future of energy

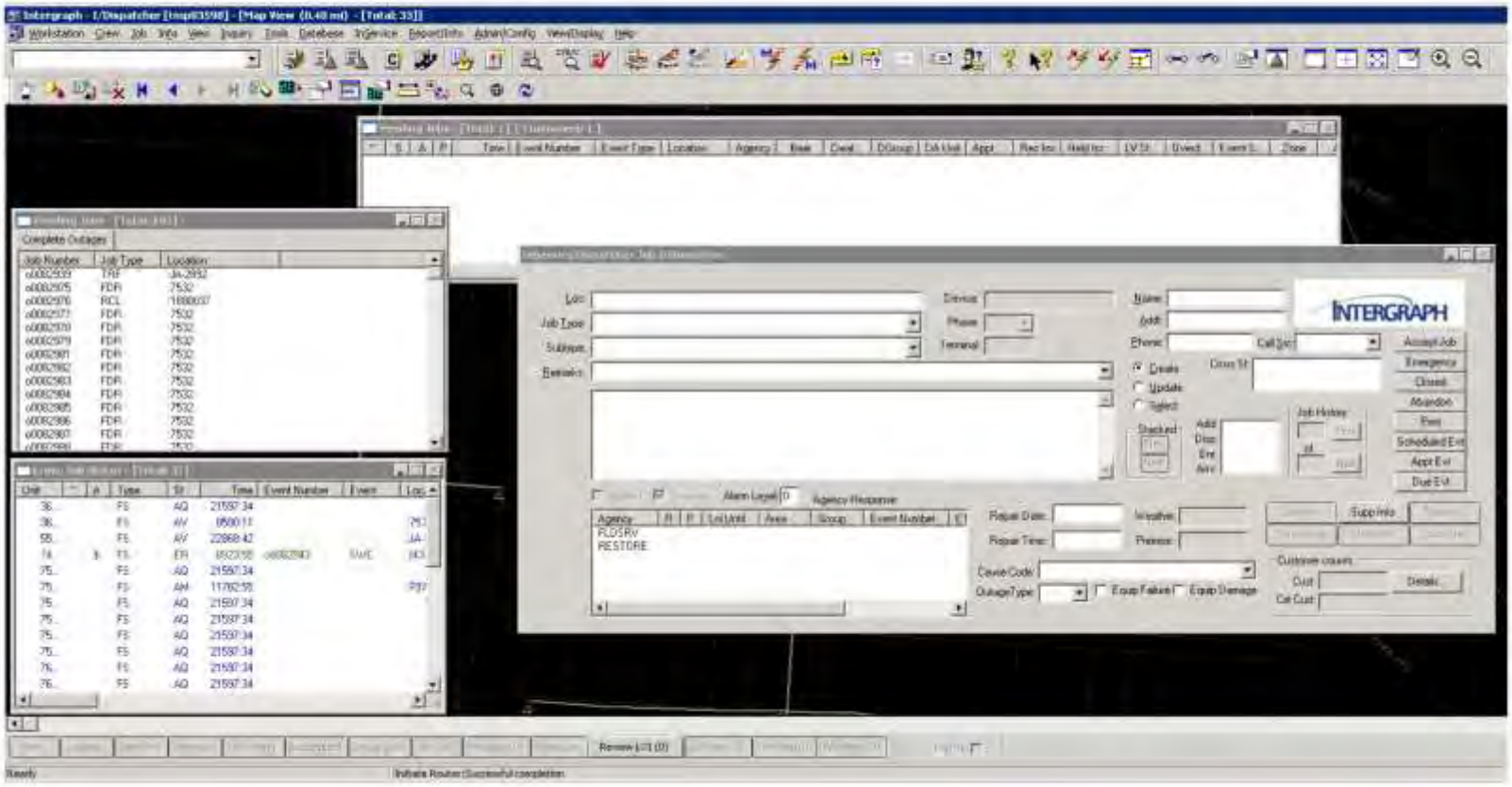
Launch InService I/Dispatcher



▪2

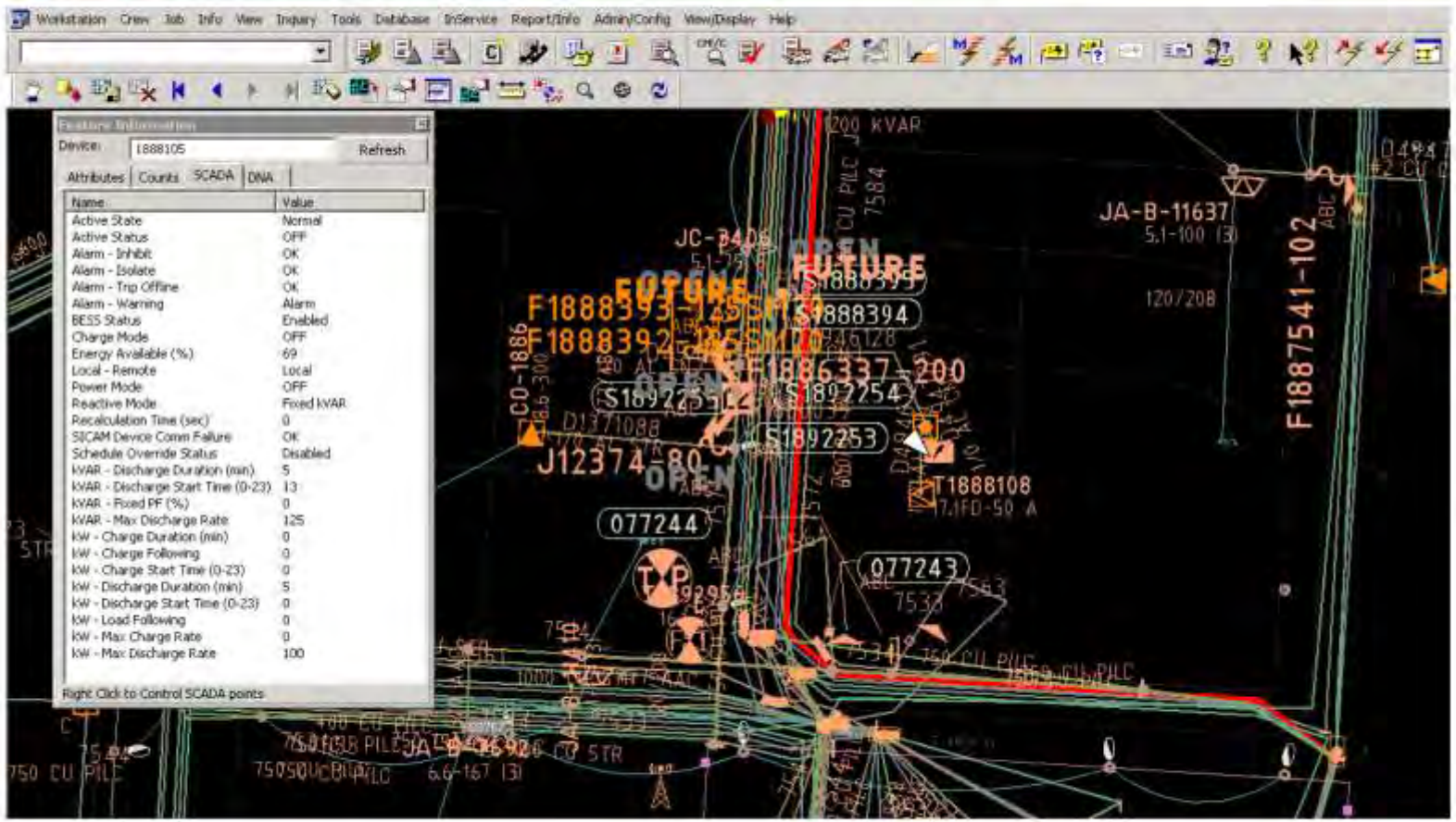
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

InService I/Dispatcher Main Screen



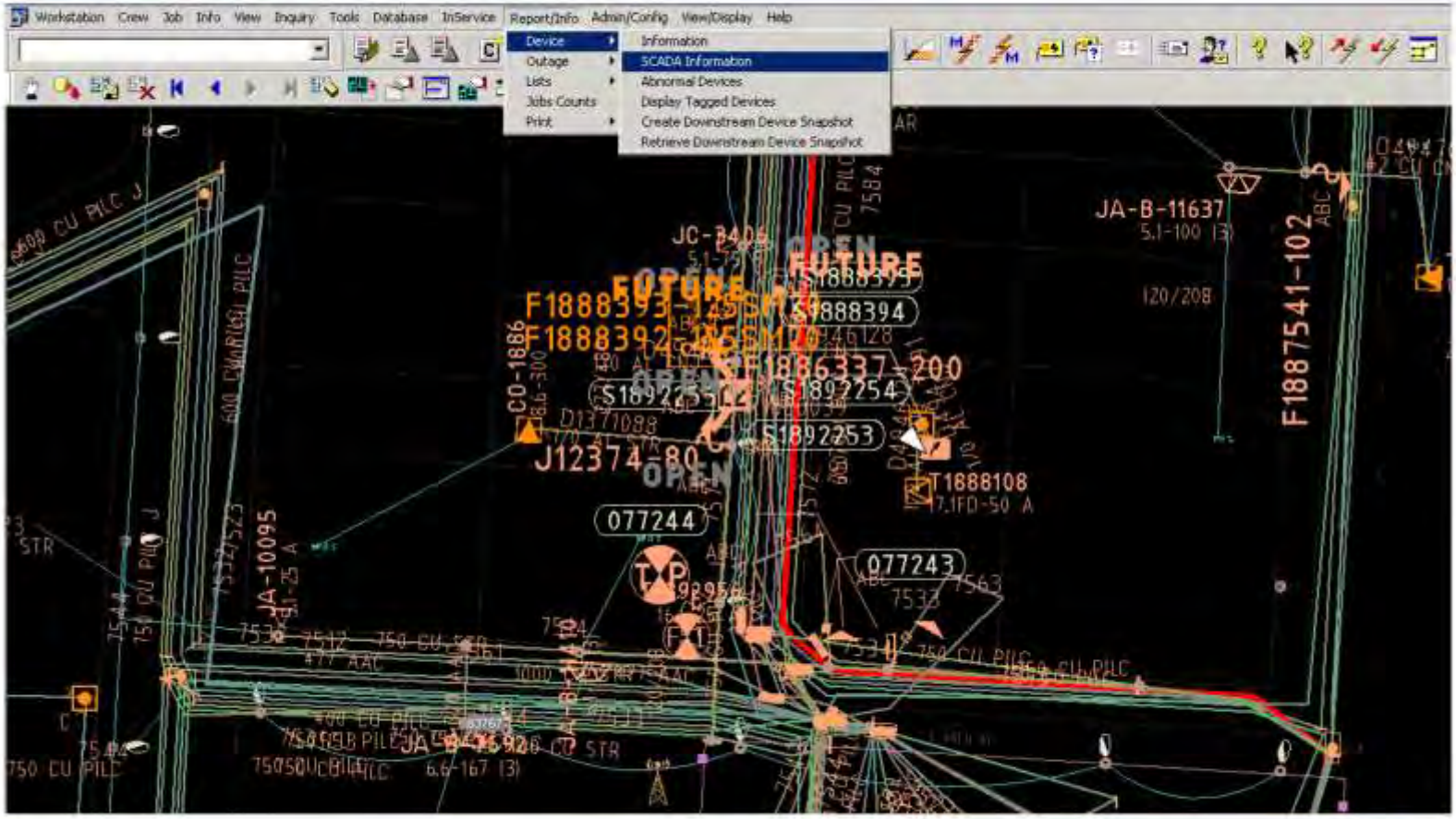
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Feature Information: Battery



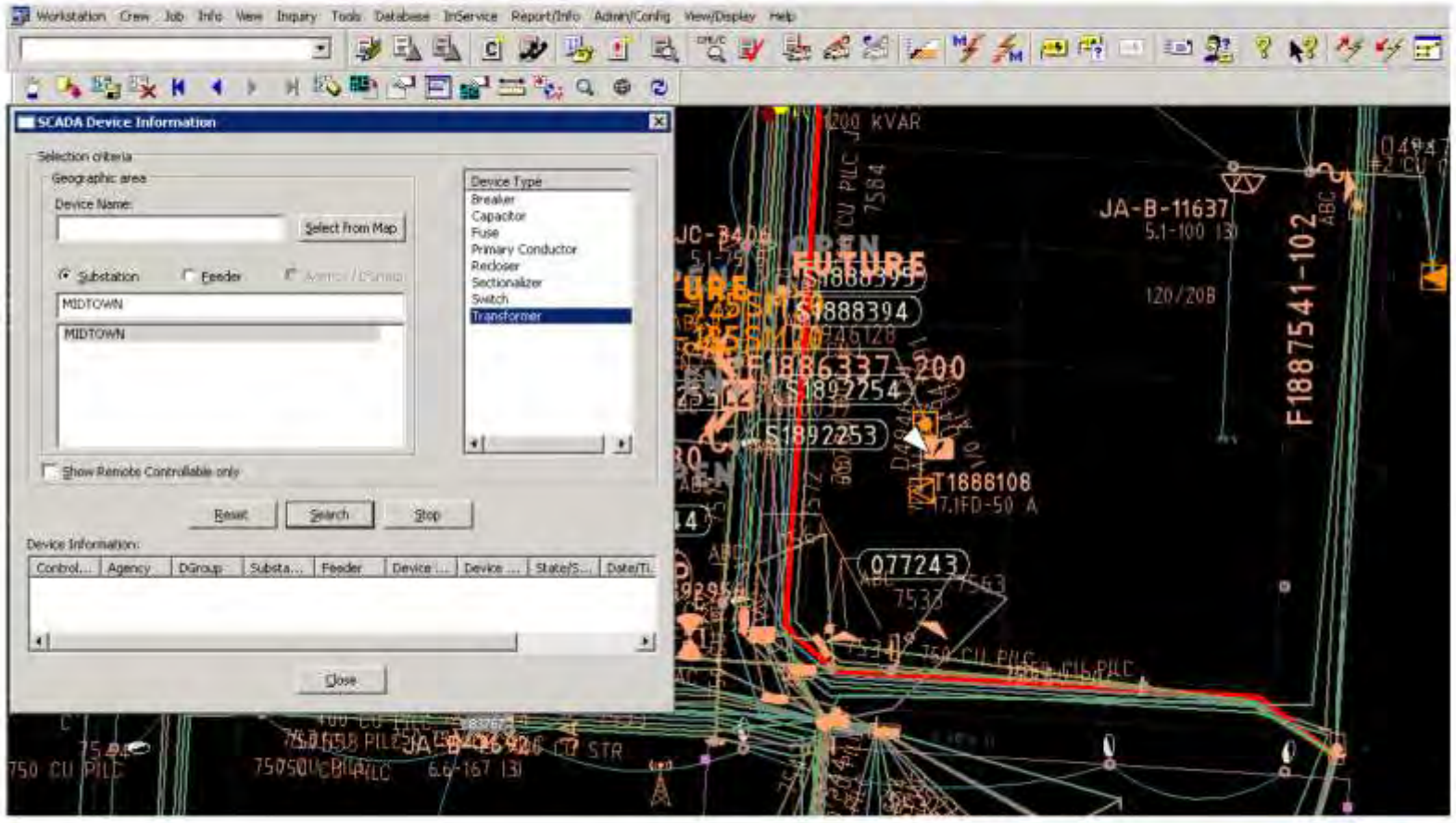
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Launch "SCADA Device Information"

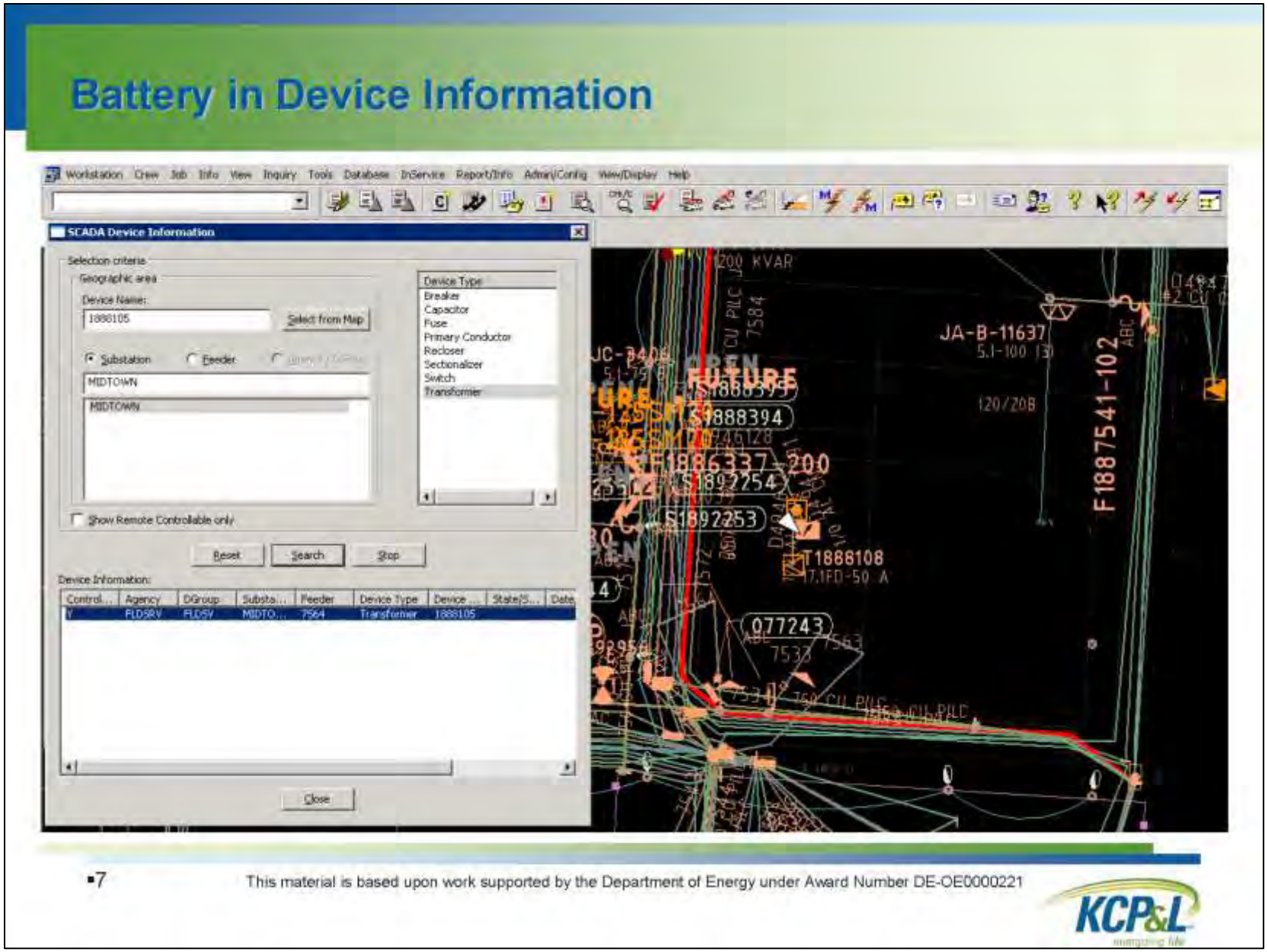


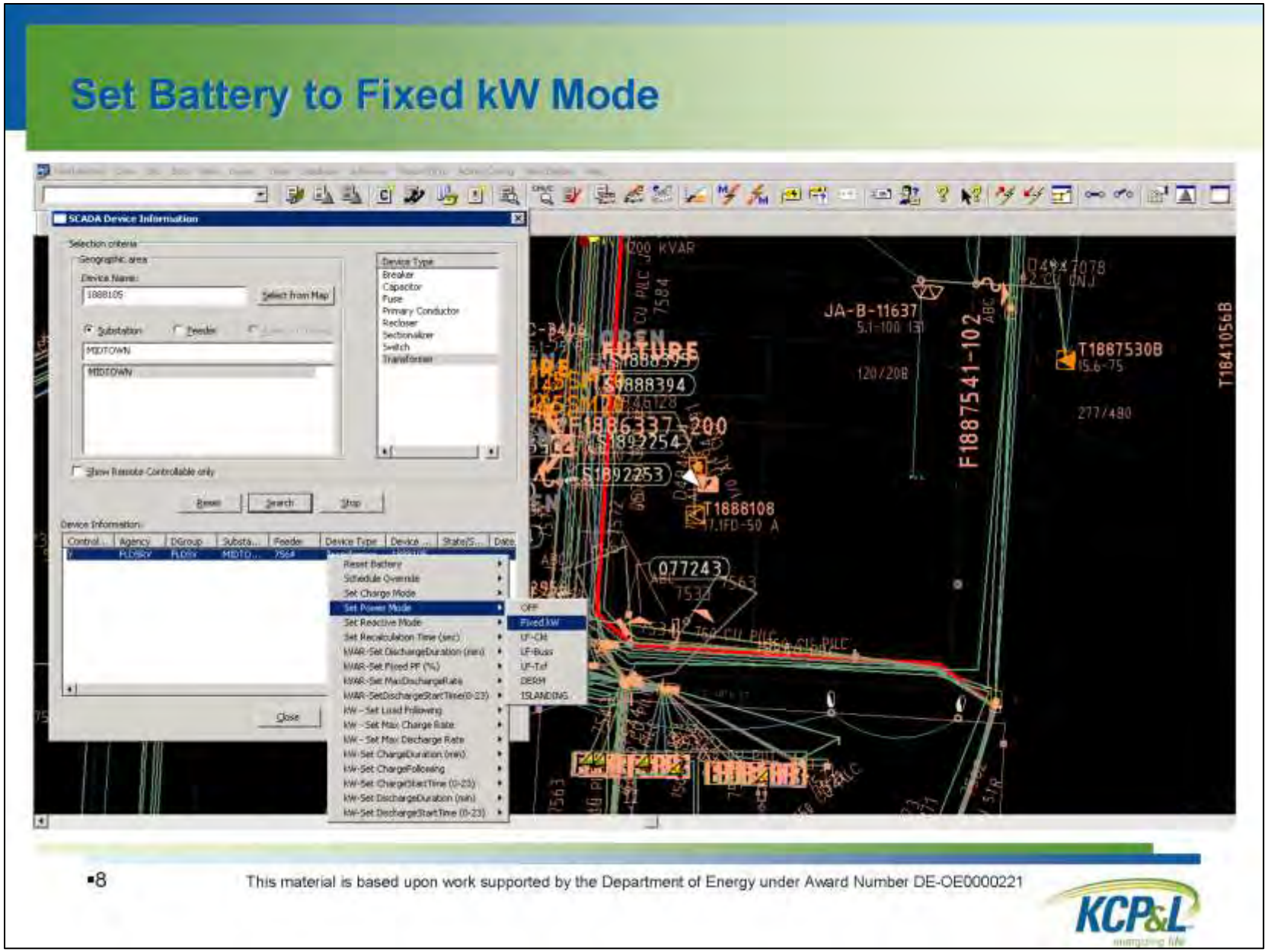
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

SCADA Device Information Window

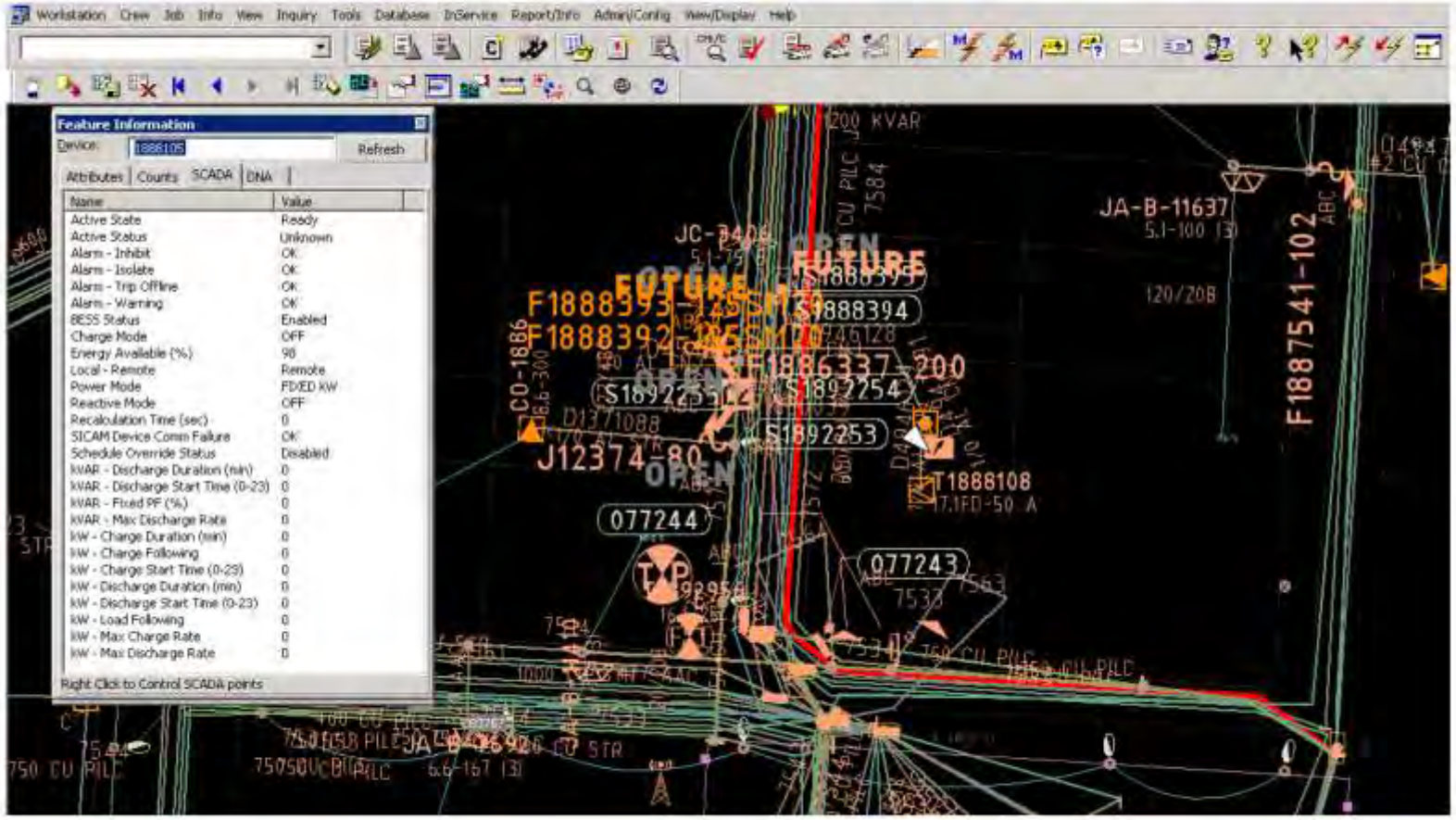


This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

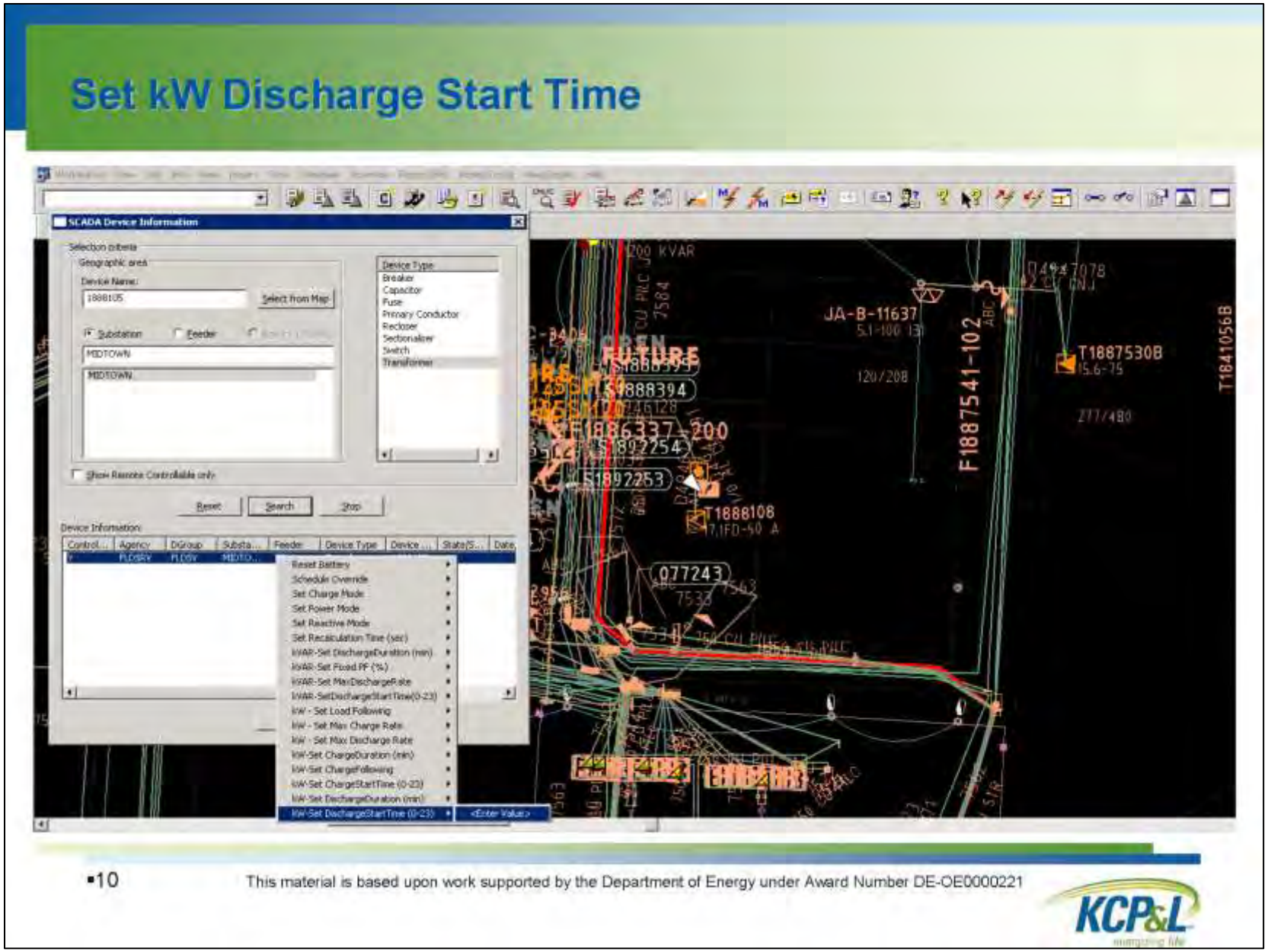

Battery in Device Information
SCADA Device Information
Selection criteria
Geographic area
Device Name:
1888105
Select from Map
Substation
Feeder
MIDTOWN
MIDTOWN
Device Type
Breaker
Capacitor
Fuse
Primary Conductor
Recloser
Sectionalizer
Switch
Transformer
Show Remote Controllable only
Reset
Search
Stop
Device Information:
Control...
Agency
DGroup
Substa...
Feeder
Device Type
Device ...
State/S...
Date
FLDSRV
FLDSV
MIDTO...
7564
Transformer
1888105
Close
JA-B-11637
F1887541-102
FUTURE
T1888108
077243
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

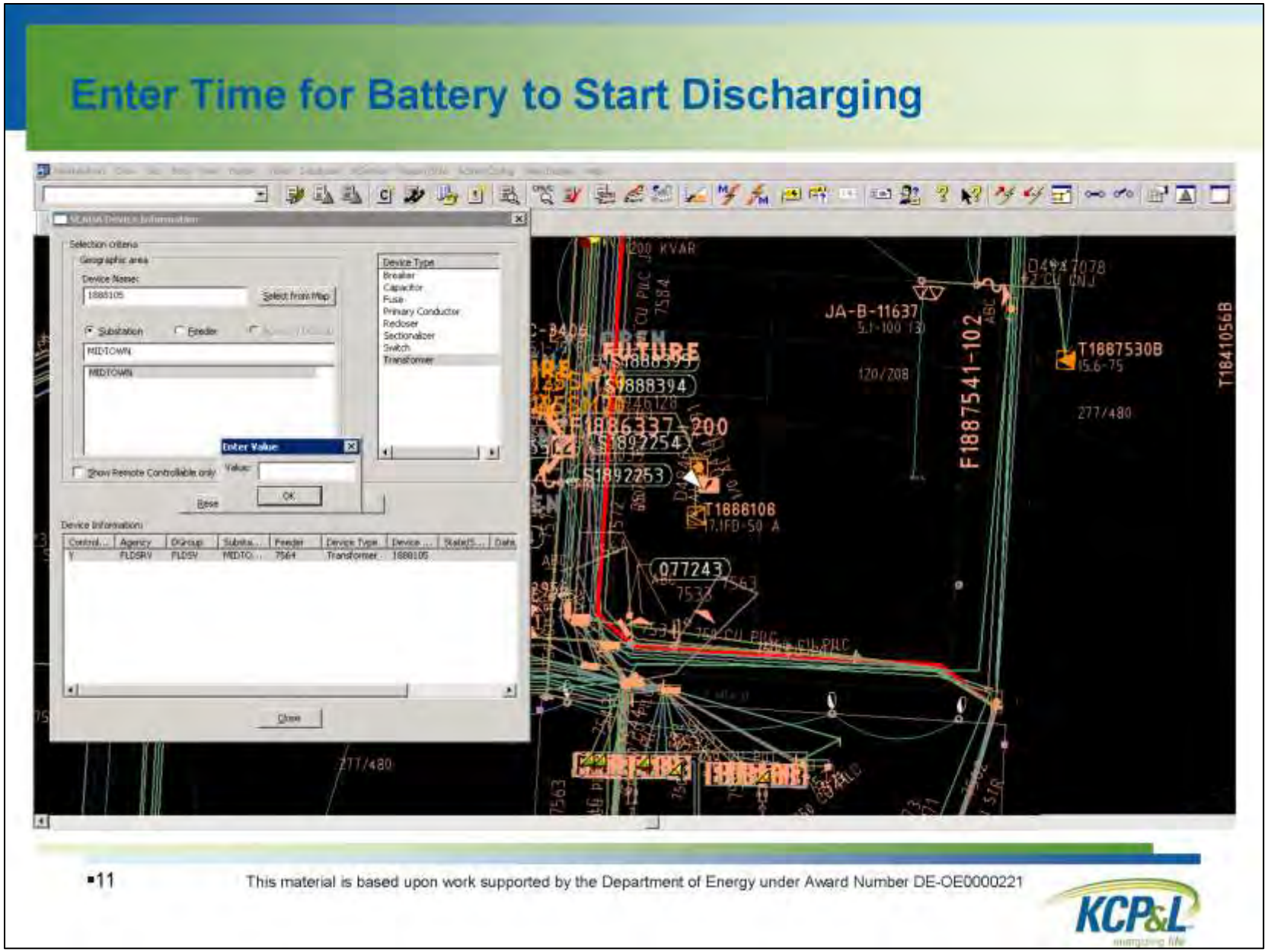

Set Battery to Fixed kW Mode
SCADA Device Information
Selection criteria
Geographic area
Device Name:
Select from Map
Substation
Feeder
Device Type
Breaker
Capacitor
Fuse
Primary Conductor
Recloser
Sectionalizer
Switch
Transformer
Reset
Search
Stop
Device Information:
Close
Reset Battery
Schedule Override
Set Charge Mode
Set Power Mode
Set Reactive Mode
Set Recalculation Time (sec)
kVAR-Set DischargeDuration (min)
kVAR-Set Fixed PF (%)
kVAR-Set MaxDischargeRate
kVAR-SetDischargeStartTime(0-23)
kW - Set Load Following
kW - Set Max Charge Rate
kW - Set Max Discharge Rate
kW-Set ChargeDuration (min)
kW-Set ChargeFollowing
kW-Set ChargeStartTime (0-23)
kW-Set DischargeDuration (min)
kW-Set DischargeStartTime (0-23)
OFF
Fixed kW
LF-CM
LF-Buss
LF-Tot
DERM
ISLANDING
JA-B-11637
T1887530B
F1887541-102
T1888108
T1841056B
277/480
120/208
8
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L
energizing life

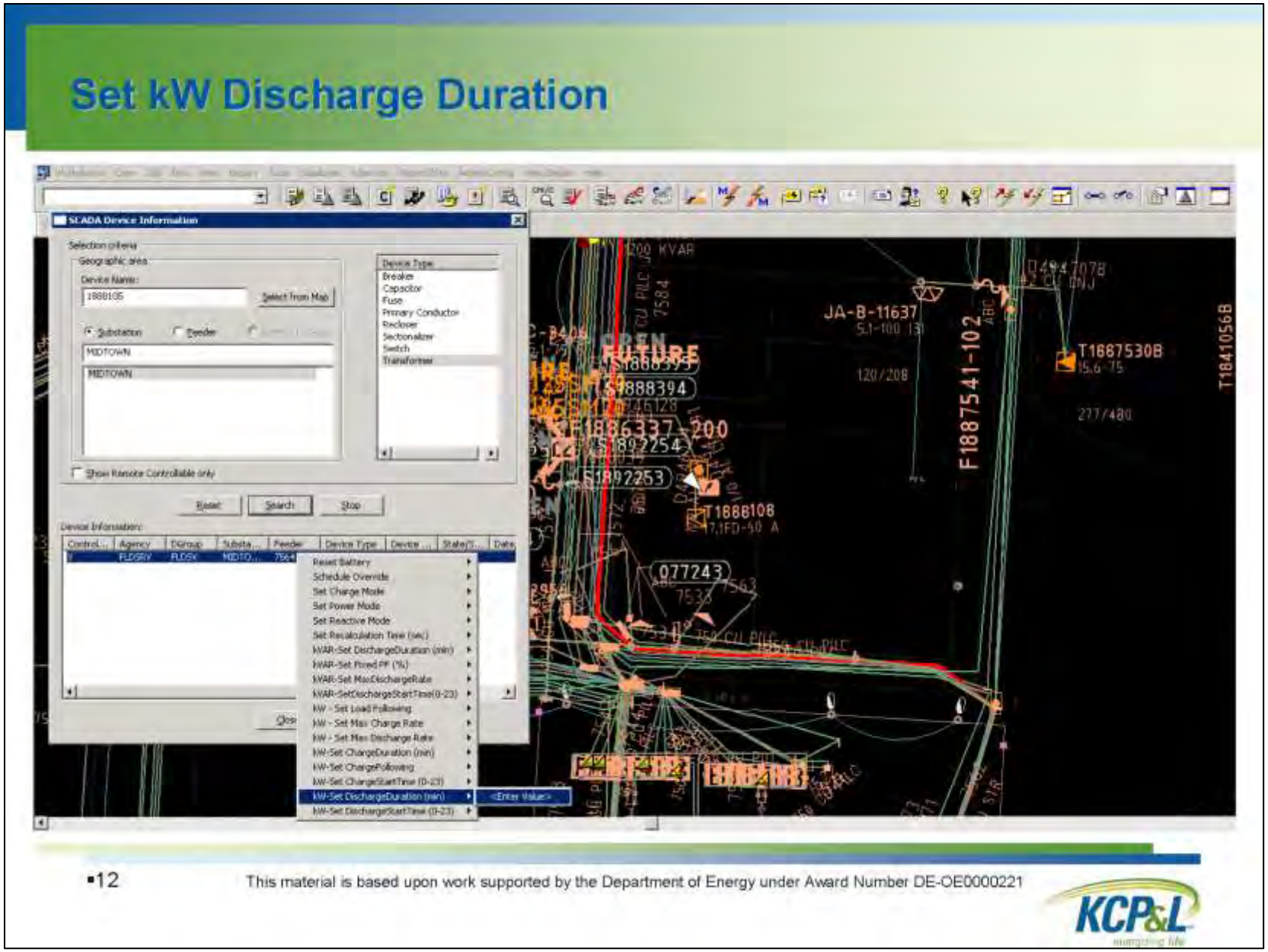
Battery set to Fixed kW Power Mode

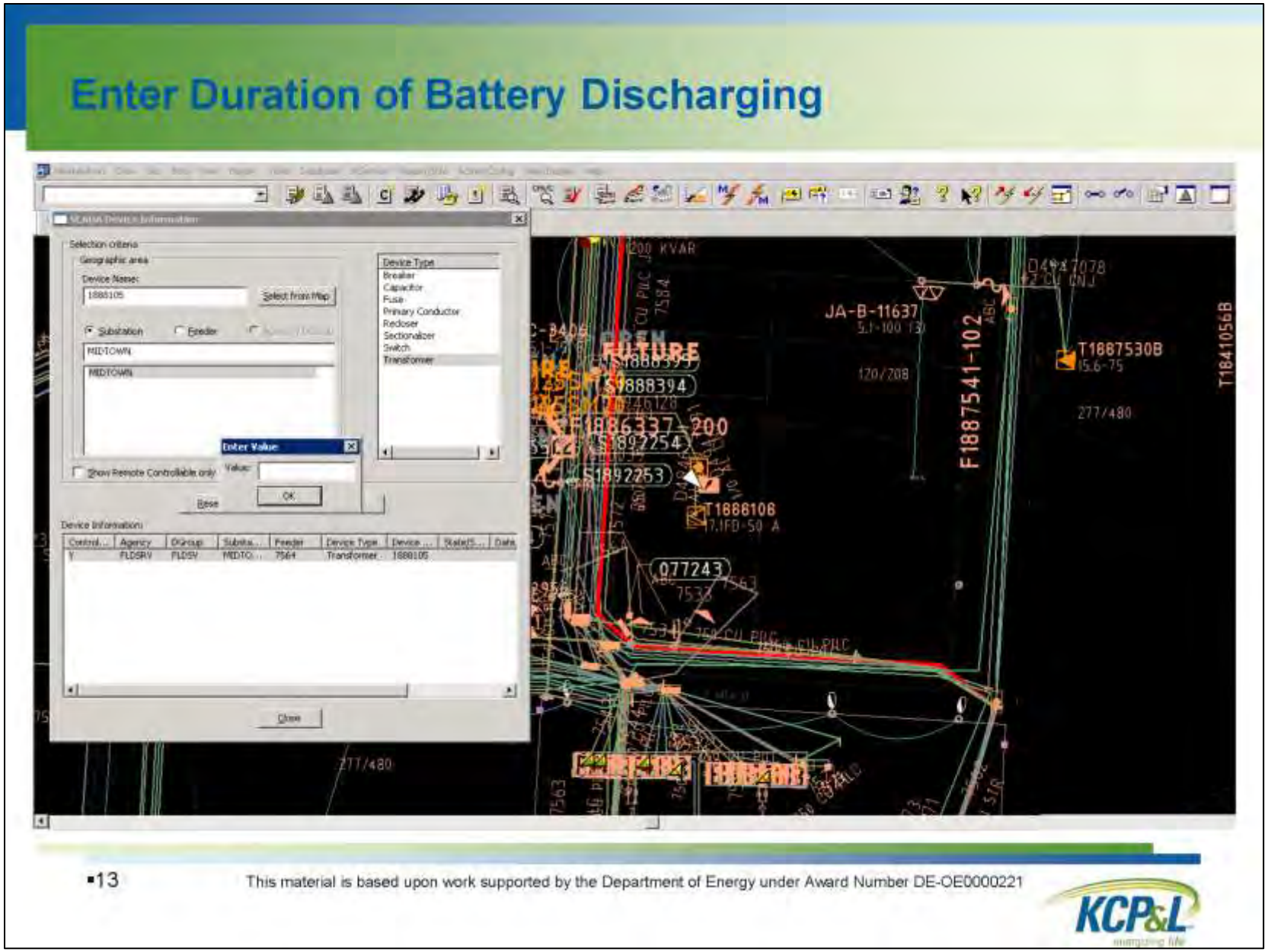


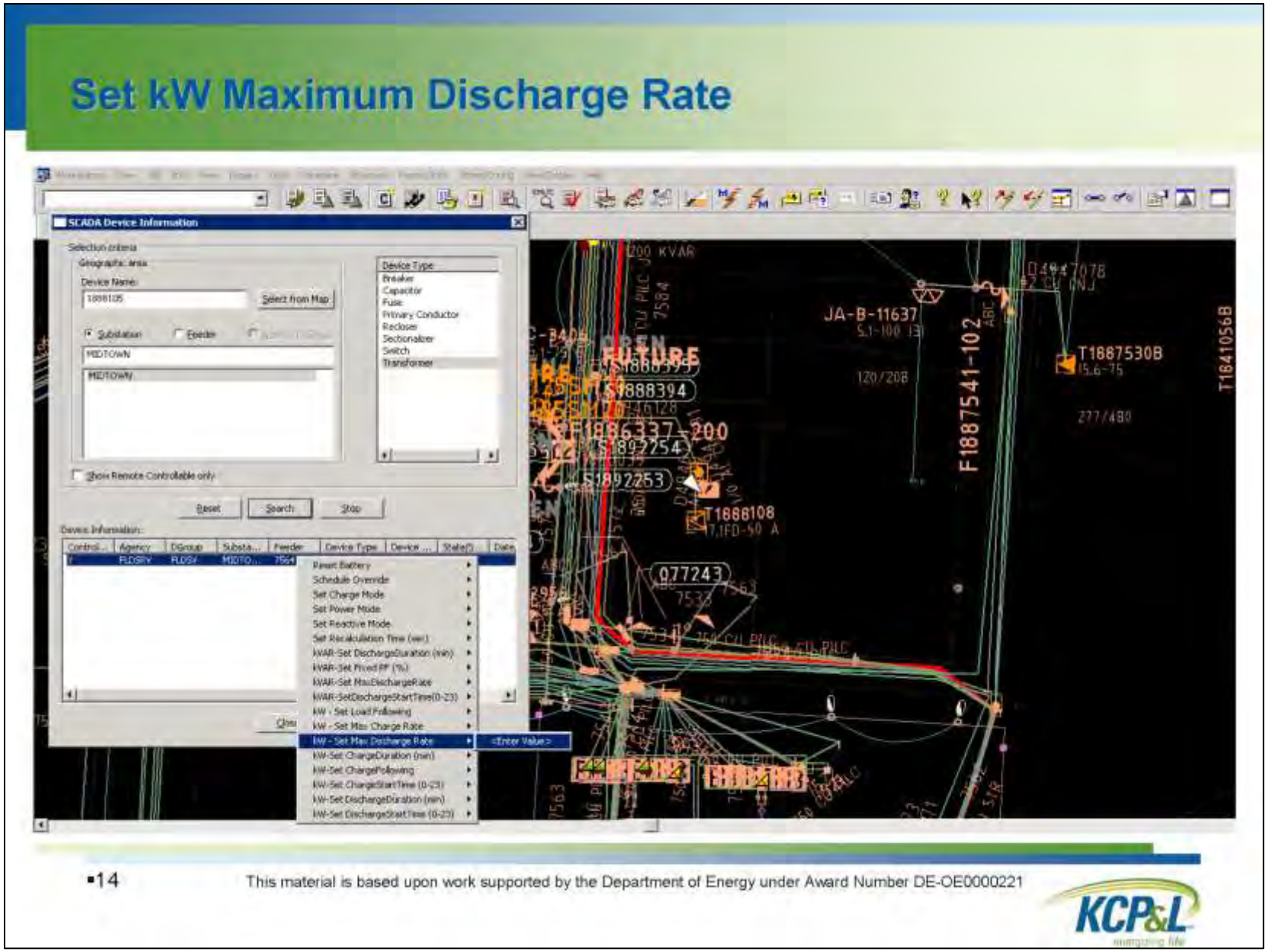
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

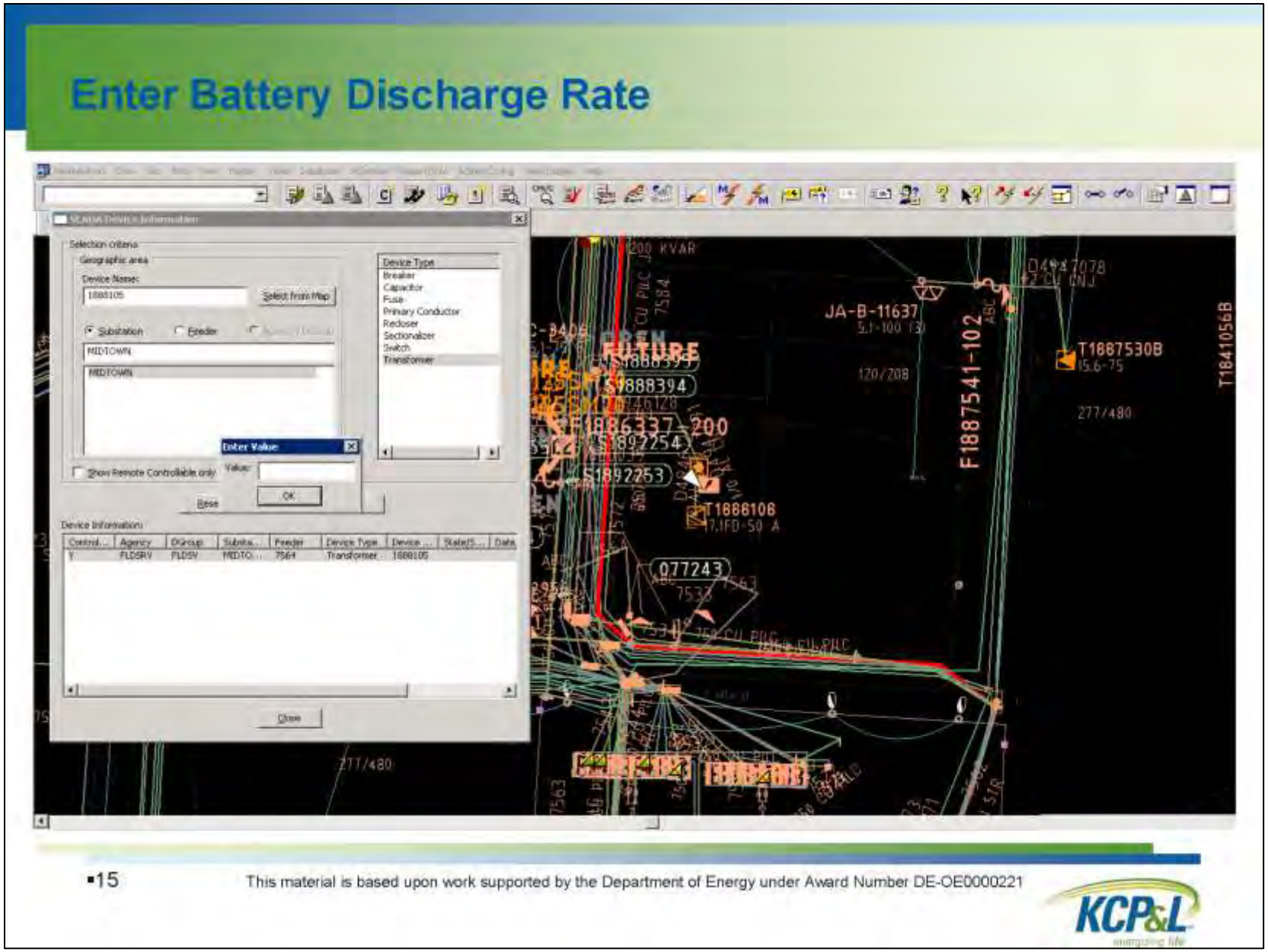

Set kW Discharge Start Time
SCADA Device Information
Selection criteria
Geographic area
Device Name:
1888105
Select from Map
Substation
Feeder
MIDTOWN
Device Type
Breaker
Capacitor
Fuse
Primary Conductor
Recloser
Sectionalizer
Switch
Transformer
Reset
Search
Stop
Device Information:
Control...
Agency
DGroup
Substa...
Feeder
Device Type
Device ...
State/S...
Date
Reset Battery
Schedule Override
Set Charge Mode
Set Power Mode
Set Reactive Mode
Set Recalculation Time (sec)
kVAR-Set DischargeDuration (min)
kVAR-Set Fixed PF (%)
kVAR-Set MaxDischargeRate
kVAR-SetDischargeStartTime(0-23)
kW - Set Load Following
kW - Set Max Charge Rate
kW - Set Max Discharge Rate
kW-Set ChargeDuration (min)
kW-Set ChargeFollowing
kW-Set ChargeStartTime (0-23)
kW-Set DischargeDuration (min)
kW-Set DischargeStartTime (0-23)
<Enter Value>
JA-B-11637
T18887308
T1888108
F1887541-102
T1841056B
077243
51888394
51892253
120/208
277/480
10
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

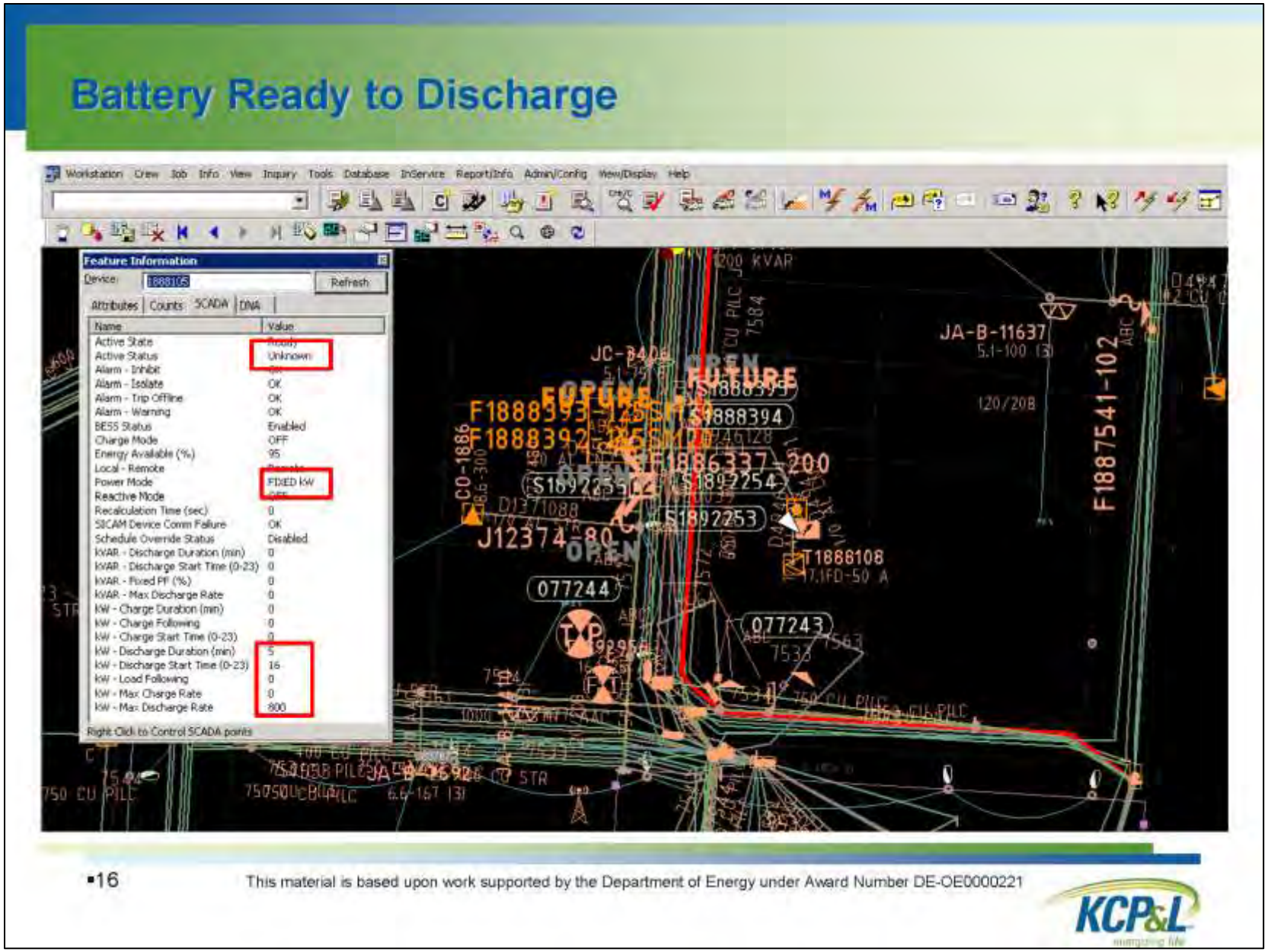

Enter Time for Battery to Start Discharging
Selection criteria
Geographic area
Device Name:
1888105
Select from Map
Substation
Feeder
MIDTOWN
MIDTOWN
Device Type
Breaker
Capacitor
Fuse
Primary Conductor
Recloser
Sectionalizer
Switch
Transformer
Enter Value
Value:
OK
Base
Show Remote Controllable only
Device Information
Close
JA-B-11637
T1887530B
T1888108
T1841056B
F1887541-102
277/480
120/208
FUTURE
077243
11
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L
energizing life


Set kW Discharge Duration
SCADA Device Information
Selection criteria
Geographic area
Device Name:
Select from Map
Substation
Feeder
MIDTOWN
Device Type
Breaker
Capacitor
Fuse
Primary Conductor
Recloser
Sectionalizer
Switch
Transformer
Show Remote Controllable only
Reset
Search
Stop
Device Information:
Reset Battery
Schedule Override
Set Charge Mode
Set Power Mode
Set Reactive Mode
Set Recalculation Time (sec)
kVAR-Set DischargeDuration (min)
kVAR-Set Fixed PF (%)
kVAR-Set MaxDischargeRate
kVAR-SetDischargeStartTime(0-23)
kW - Set Load Following
kW - Set Max Charge Rate
kW - Set Max Discharge Rate
kW-Set ChargeDuration (min)
kW-Set ChargeFollowing
kW-Set ChargeStartTime (0-23)
kW-Set DischargeDuration (min)
kW-Set DischargeStartTime (0-23)
<Enter Value>
JA-B-11637
T1887530B
T1888108
F1887541-102
T1841056B
120/208
277/480
FUTURE
12
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L
energizing life

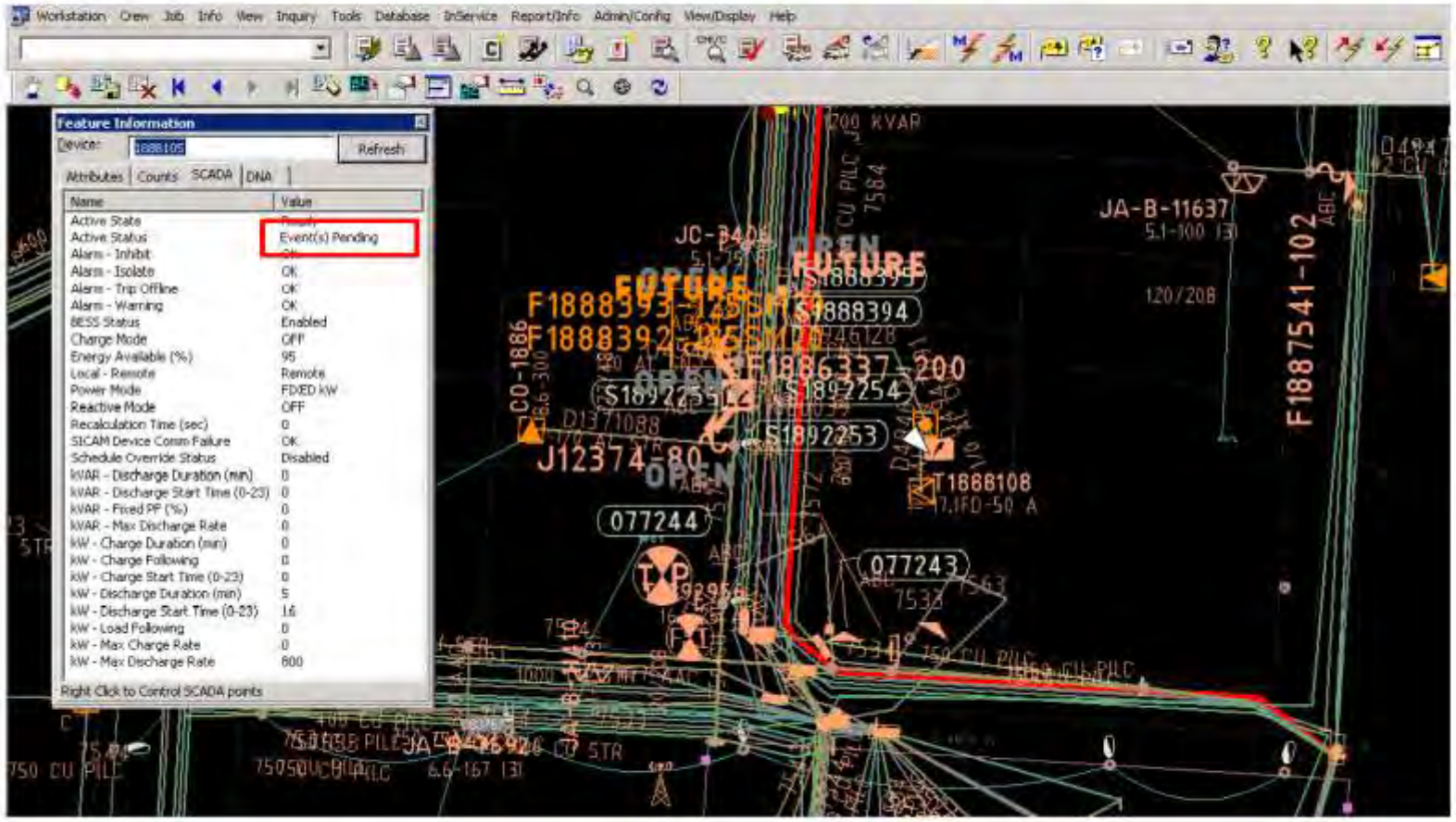

Enter Duration of Battery Discharging
Selection criteria
Geographic area
Device Name:
1888105
Select from Map
Substation
Feeder
MIDTOWN
MIDTOWN
Device Type
Breaker
Capacitor
Fuse
Primary Conductor
Recloser
Sectionalizer
Switch
Transformer
Enter Value
Value:
OK
Base
Show Remote Controllable only
Device Information
Close
JA-B-11637
T1887530B
T1888108
F1887541-102
277/480
120/208
13
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221


Set kW Maximum Discharge Rate
SCADA Device Information
Selection criteria
Geographic area
Device Name:
1888105
Select from Map
Substation
Feeder
MIDTOWN
MIDTOWN
Device Type
Breaker
Capacitor
Fuse
Primary Conductor
Recloser
Sectionalizer
Switch
Transformer
Show Remote Controllable only
Reset
Search
Stop
Device Information:
Control...
Agency
DGroup
Substa...
Feeder
Device Type
Device ...
State(I)
Date
FLDSRV
FLDSV
MIDTO...
7564
Reset Battery
Schedule Override
Set Charge Mode
Set Power Mode
Set Reactive Mode
Set Recalculation Time (sec)
kVAR-Set DischargeDuration (min)
kVAR-Set Fixed PF (%)
kVAR-Set MaxDischargeRate
kVAR-SetDischargeStartTime(0-23)
kW - Set Load Following
kW - Set Max Charge Rate
kW - Set Max Discharge Rate
<Enter Value>
kW-Set ChargeDuration (min)
kW-Set ChargeFollowing
kW-Set ChargeStartTime (0-23)
kW-Set DischargeDuration (min)
kW-Set DischargeStartTime (0-23)
200 KVAR
JA-B-11637
T1887530B
F1887541-102
T1841056B
120/208
277/480
S1888394
S1892754
S1892253
T1888108
077243
OPEN
FUTURE
14
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L
energizing life


Enter Battery Discharge Rate
Selection criteria
Geographic area
Device Name:
1888105
Select from Map
Substation
Feeder
MIDTOWN
MIDTOWN
Device Type
Breaker
Capacitor
Fuse
Primary Conductor
Recloser
Sectionalizer
Switch
Transformer
Enter Value
Value:
OK
Base
Show Remote Controllable only
Device Information
Control...
Agency
DiGroup
Substa...
Feeder
Device Type
Device ...
State(S...
Data
Y
FLDSRV
FLDSV
MIDTO...
7564
Transformer
1888105
Close
JA-B-11637
T1887530B
T1888108
077243
F1887541-102
277/480
120/208
FUTURE
▪15
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L
energizing life


Battery Ready to Discharge
Workstation Crew Job Info View Inquiry Tools Database InService Report/Info Admin/Config View/Display Help
Feature Information
Device: 1888105
Refresh
Attributes Counts SCADA DNA
Name Value
Active State Ready
Active Status Unknown
Alarm - Inhibit OK
Alarm - Isolate OK
Alarm - Trip Offline OK
Alarm - Warning OK
BESS Status Enabled
Charge Mode OFF
Energy Available (%) 95
Local - Remote Remote
Power Mode FIXED kW
Reactive Mode OFF
Recalculation Time (sec) 0
SICAM Device Comm Failure OK
Schedule Override Status Disabled
kVAR - Discharge Duration (min) 0
kVAR - Discharge Start Time (0-23) 0
kVAR - Fixed PF (%) 0
kVAR - Max Discharge Rate 0
kW - Charge Duration (min) 0
kW - Charge Following 0
kW - Charge Start Time (0-23) 0
kW - Discharge Duration (min) 5
kW - Discharge Start Time (0-23) 16
kW - Load Following 0
kW - Max Charge Rate 0
kW - Max Discharge Rate 800
Right Click to Control SCADA points
JA-B-11637
F1887541-102
F1888394
F1886337-200
S1892254
S1892253
T1888108
077244
077243
J12374
CO-1886
120/208
750 CU PILC
16
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

Battery Started to Discharge

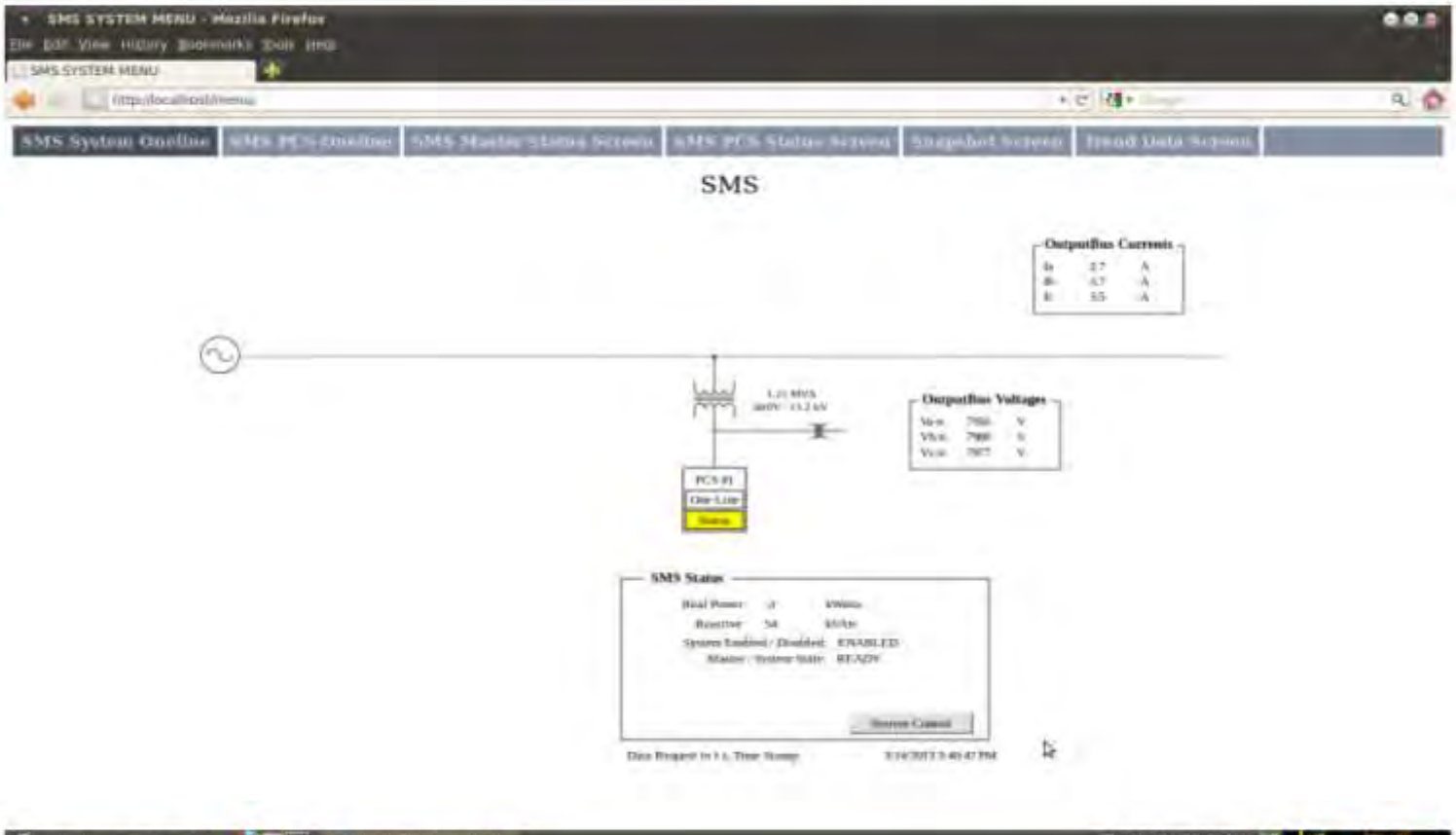


This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Launch Browser Based HMI

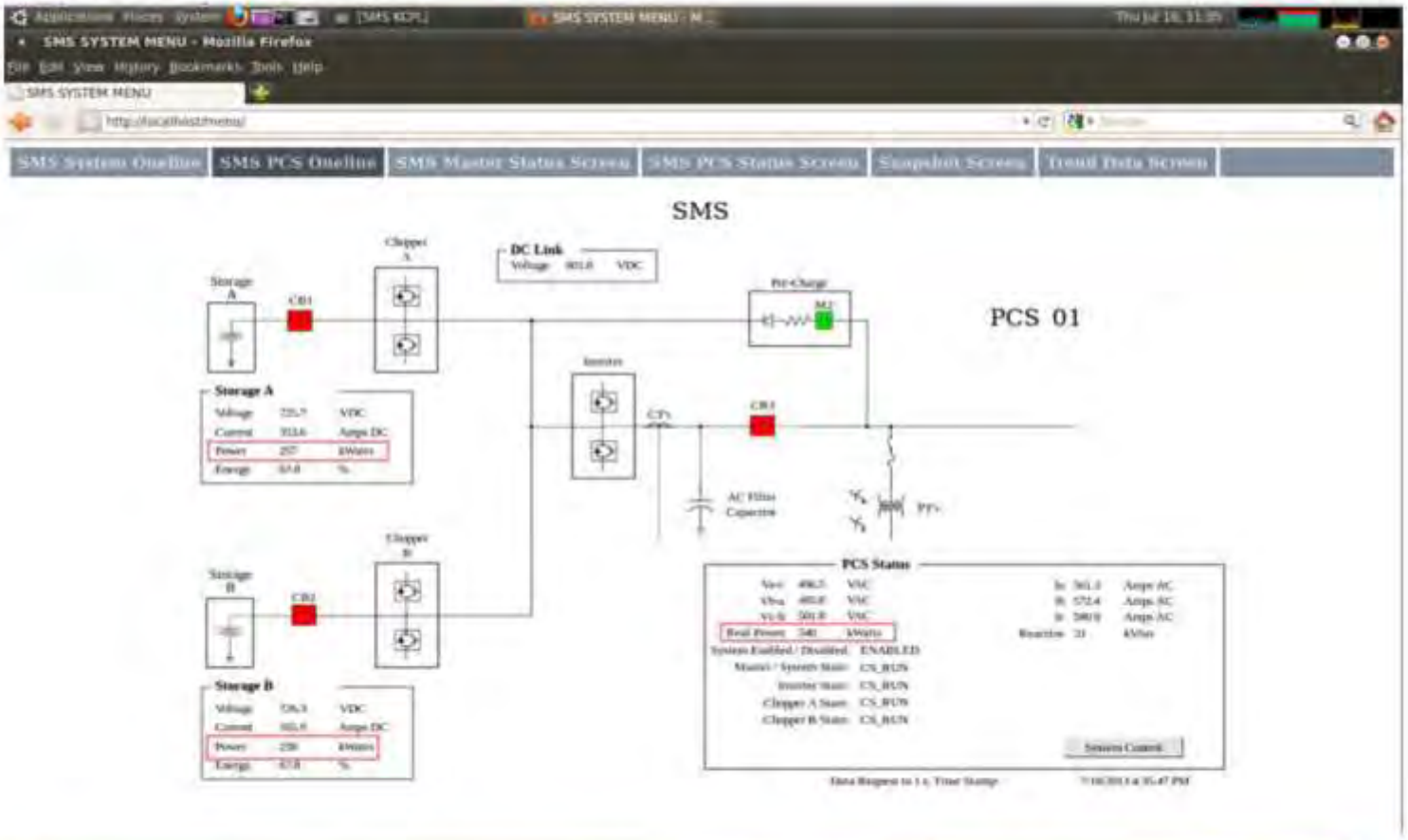
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

SMS System Menu Main Screen



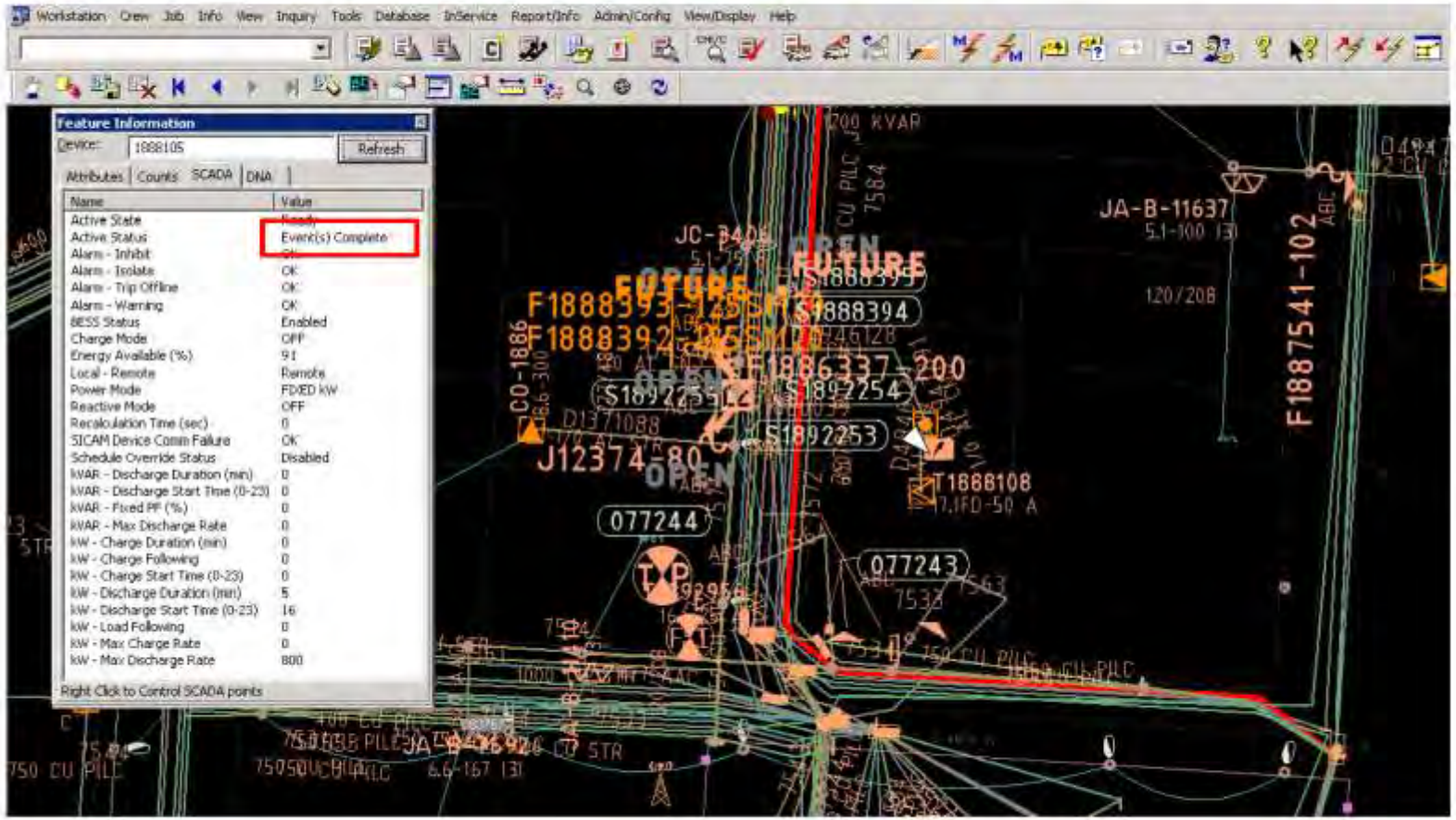
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

SMS PCS Oneline: Battery is Discharging



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

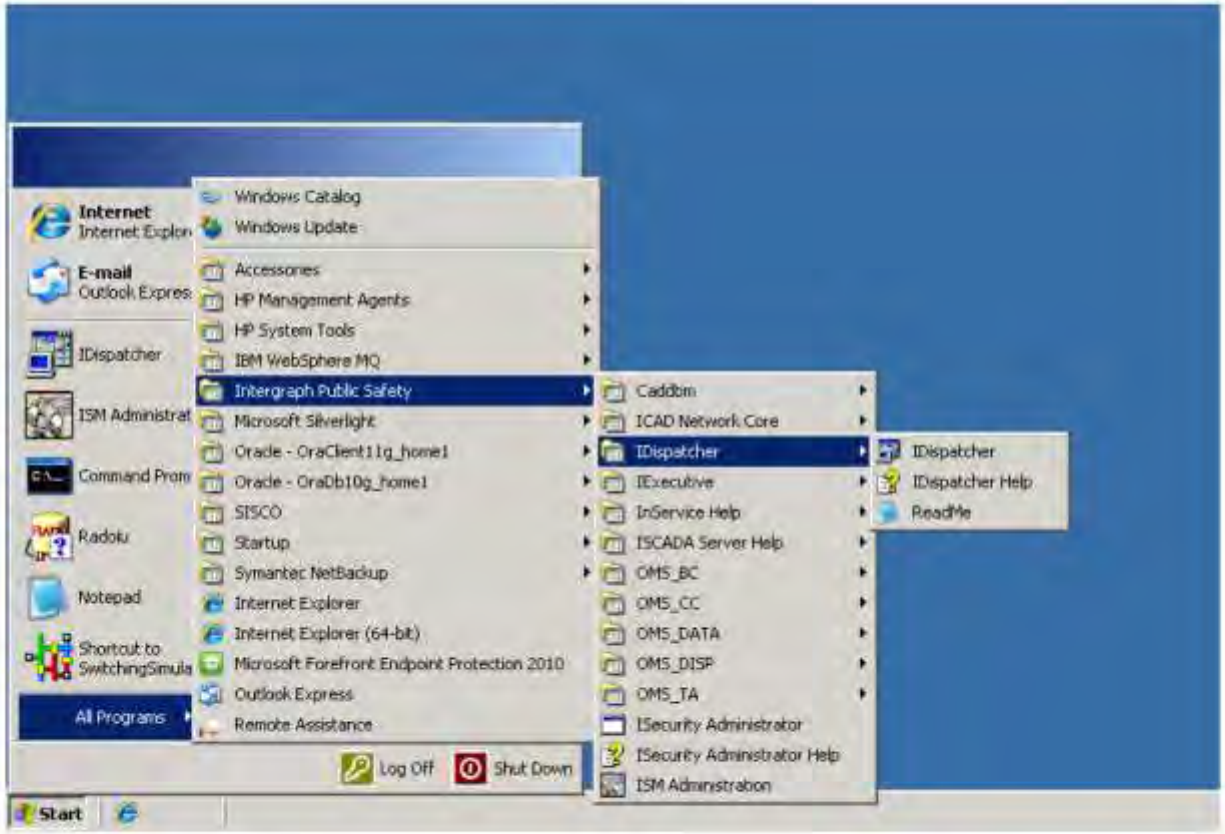
Battery Finished Discharging



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221


Battery Operation: Load Following Discharge
- KC Green Impact Zone Initiative
- DOE Regional SmartGrid Demonstration Program
- EPRI SmartGrid Demonstration Program
KCP&L
SmartGrid
the future of energy

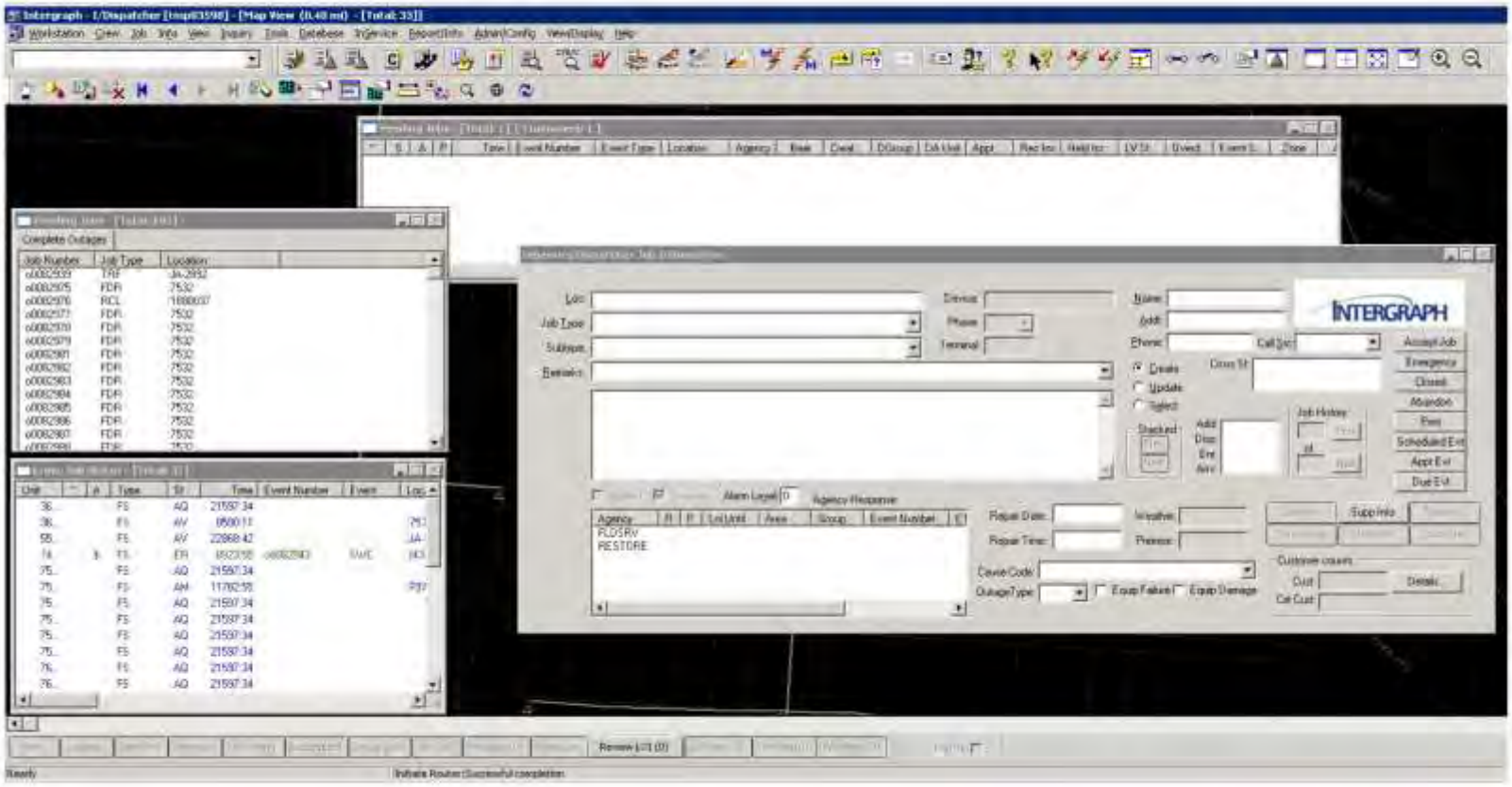
Launch InService I/Dispatcher



▪2

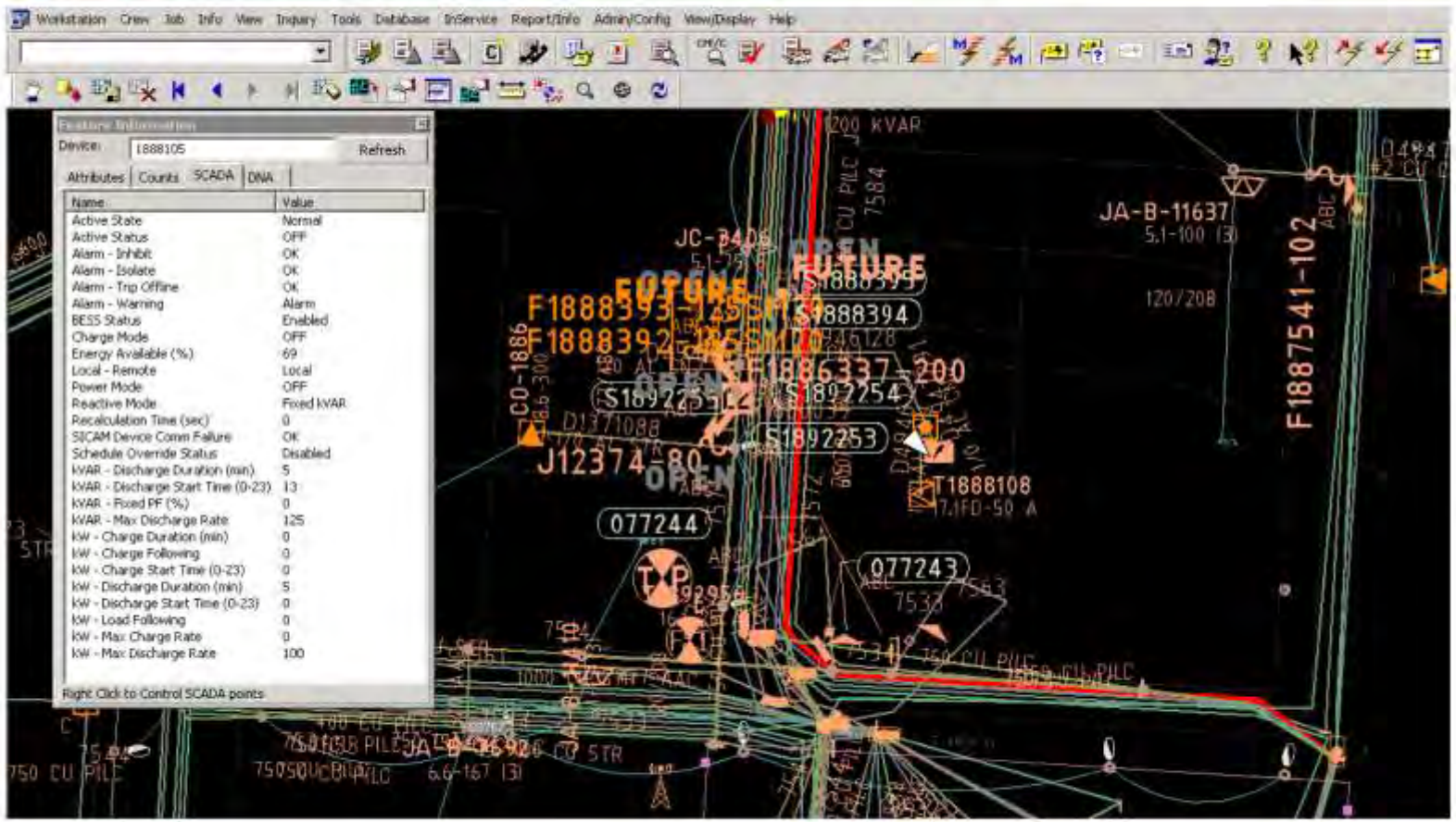
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

InService I/Dispatcher Main Screen

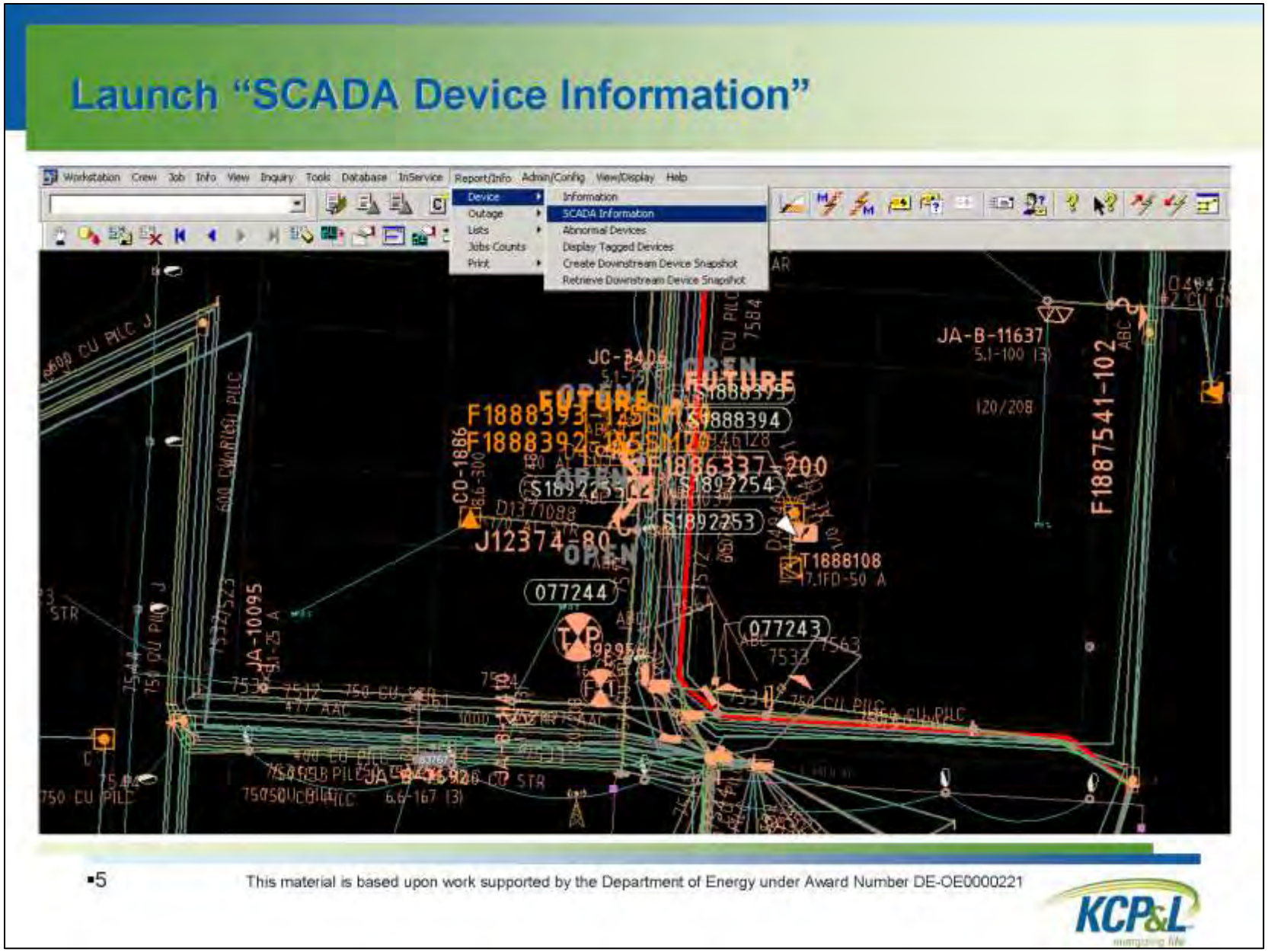


This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

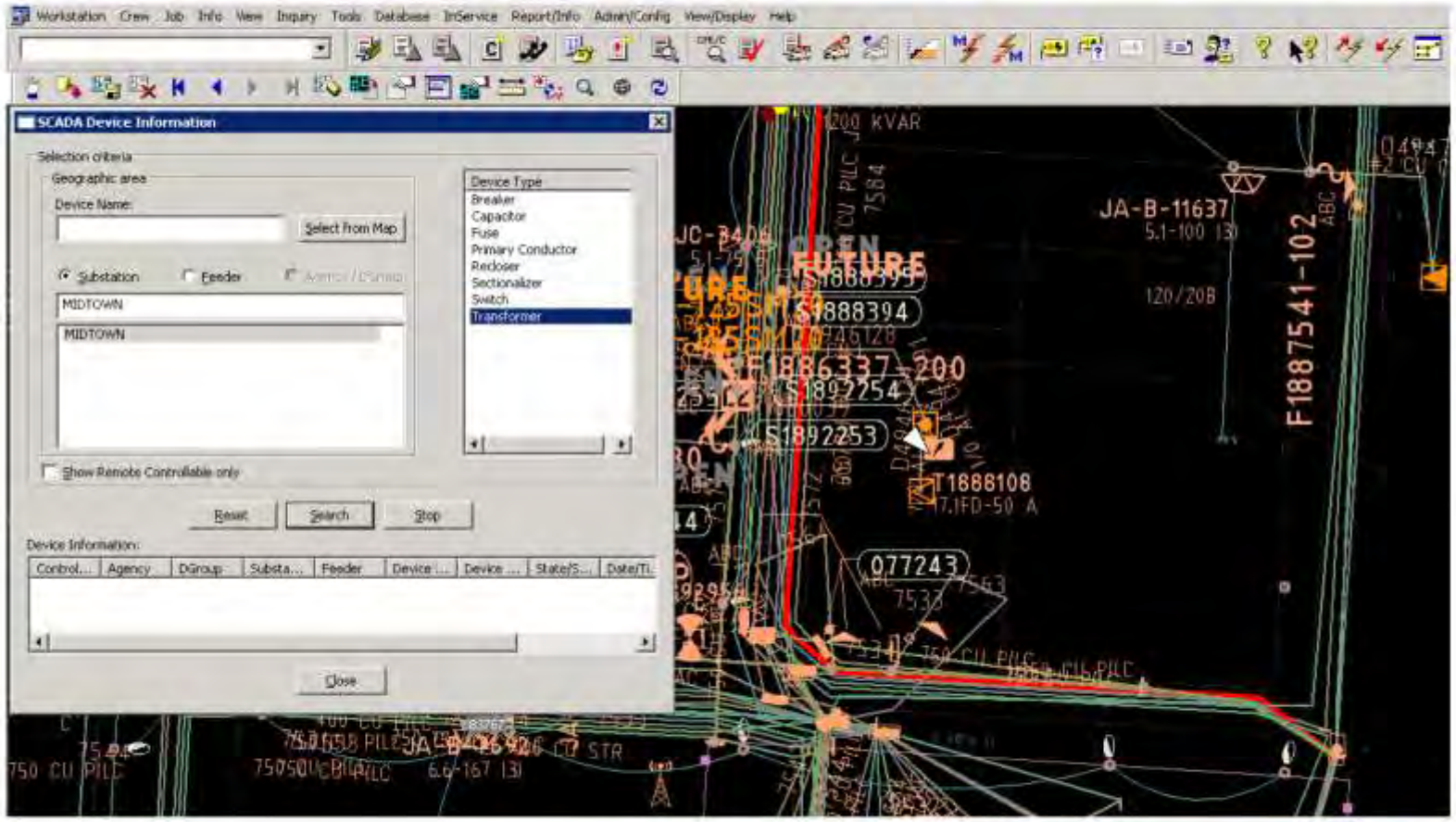
Feature Information: Battery



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

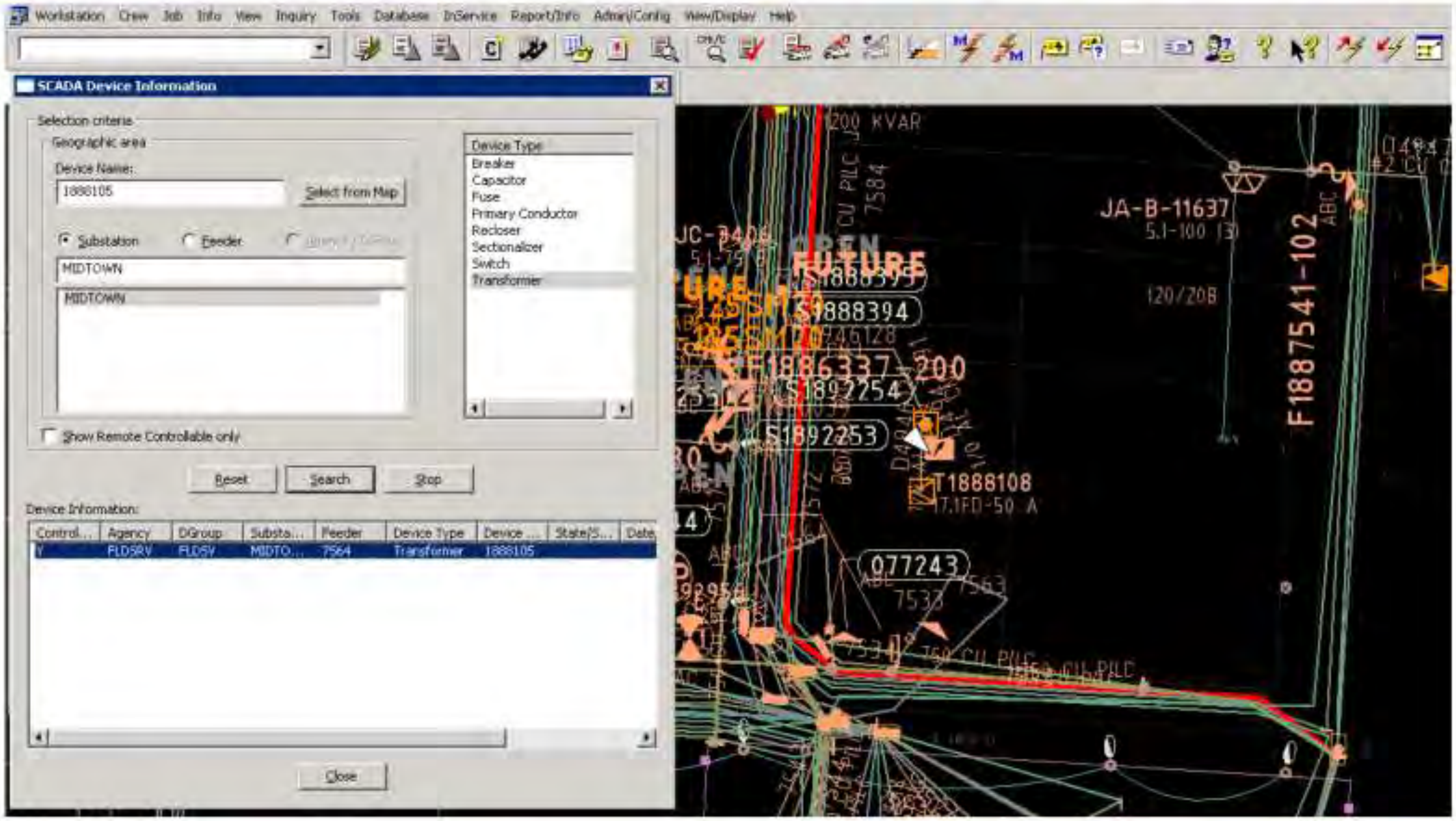

Launch "SCADA Device Information"
Workstation Crew Job Info View Inquiry Tools Database InService Report/Info Admin/Config View/Display Help
Device
Outage
Lists
Jobs Counts
Print
Information
SCADA Information
Abnormal Devices
Display Tagged Devices
Create Downstream Device Snapshot
Retrieve Downstream Device Snapshot
JA-B-11637
F1887541-102
FUTURE
OPEN
J12374-80
T1888108
077244
077243
JA-10095
▪5
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

SCADA Device Information Window



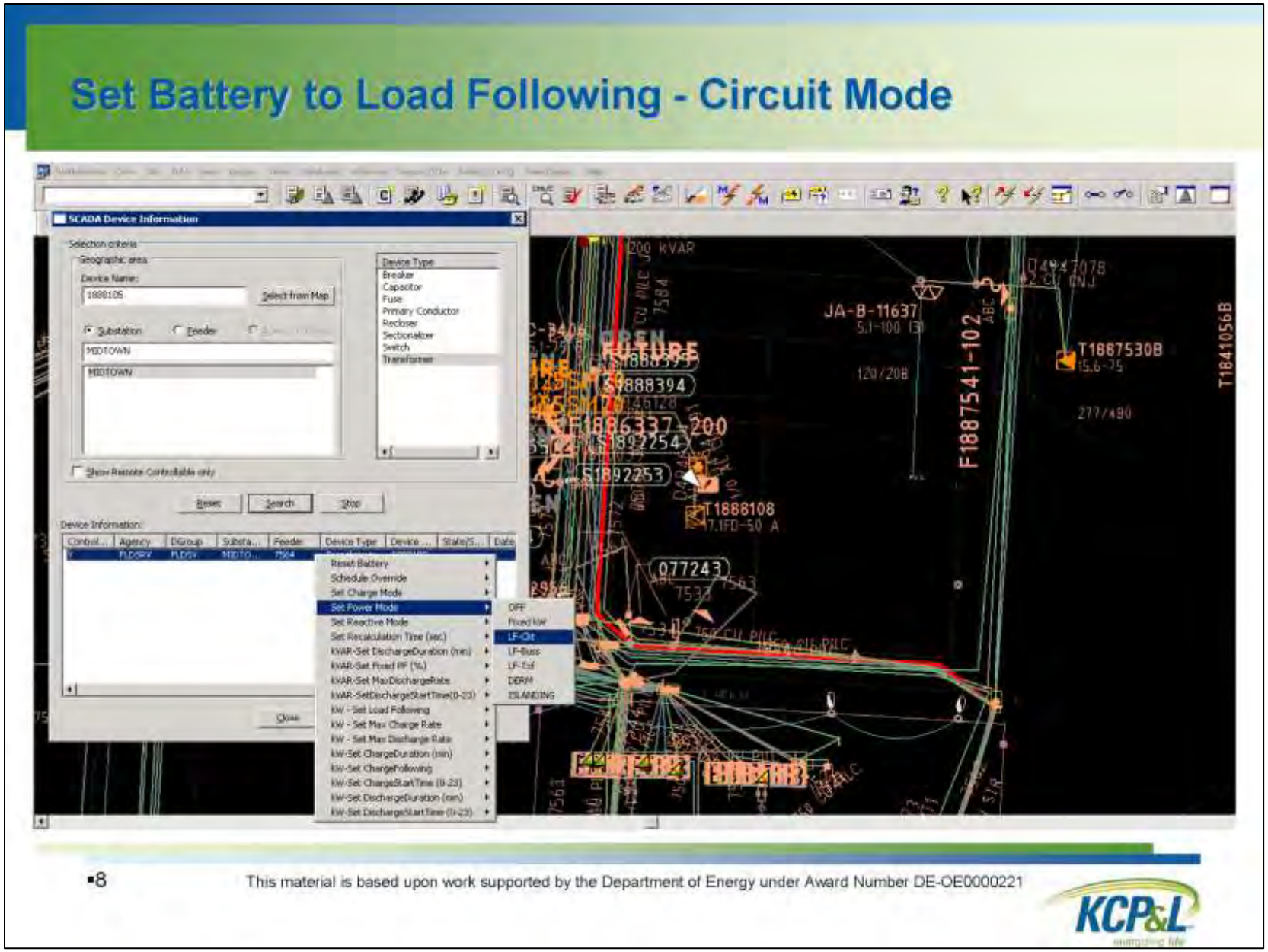
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Battery in Device Information

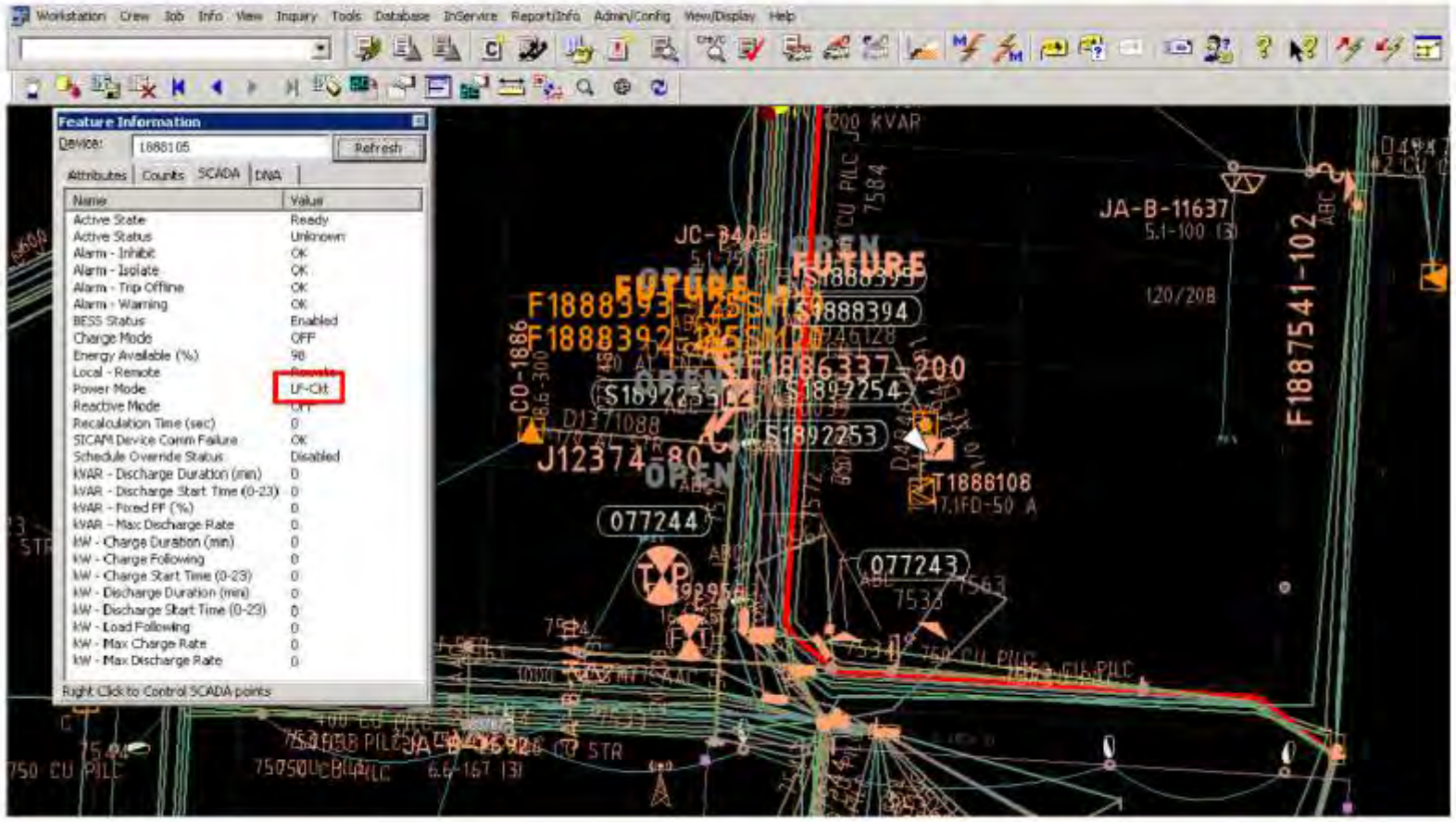


▪7

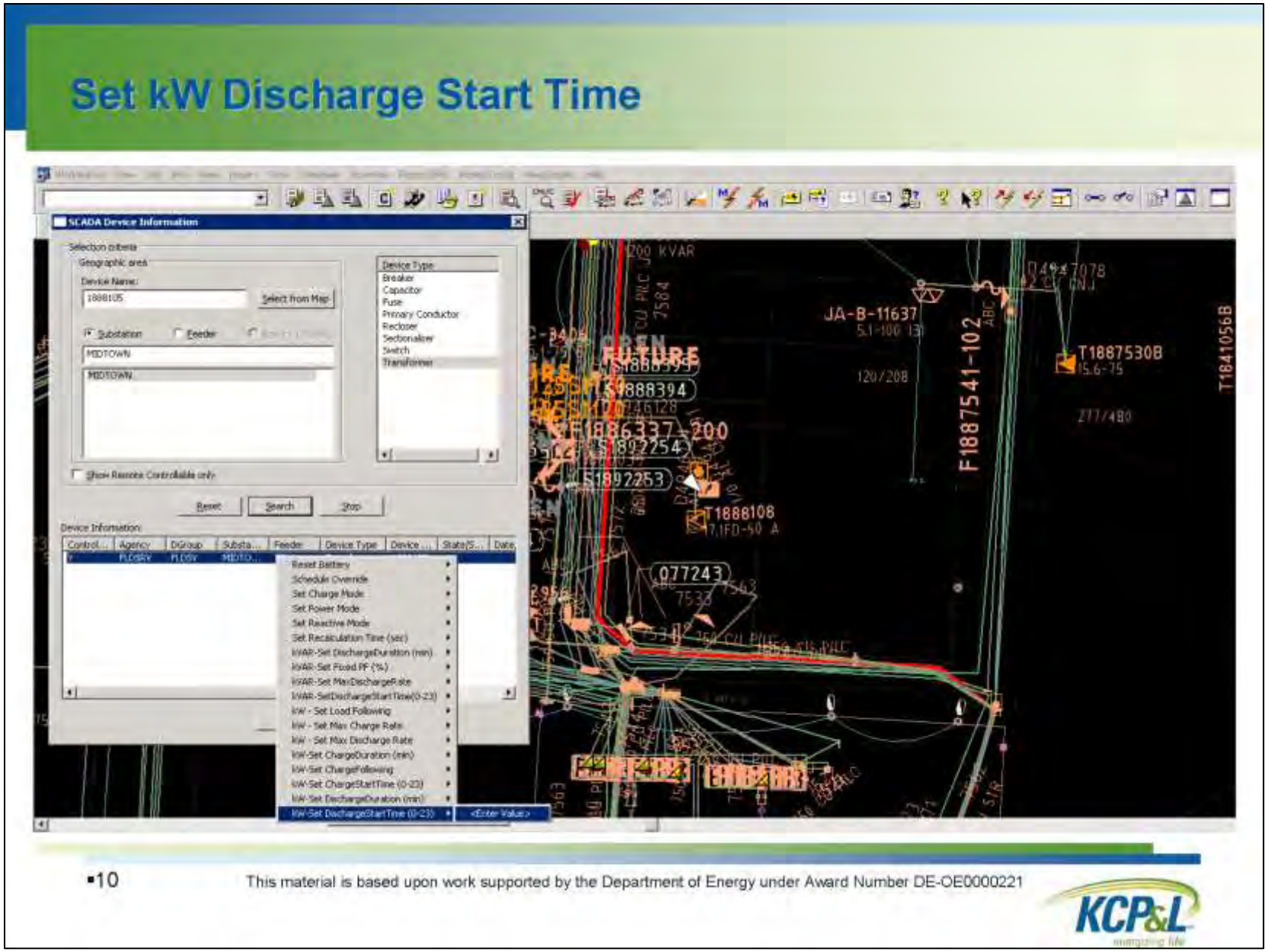
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

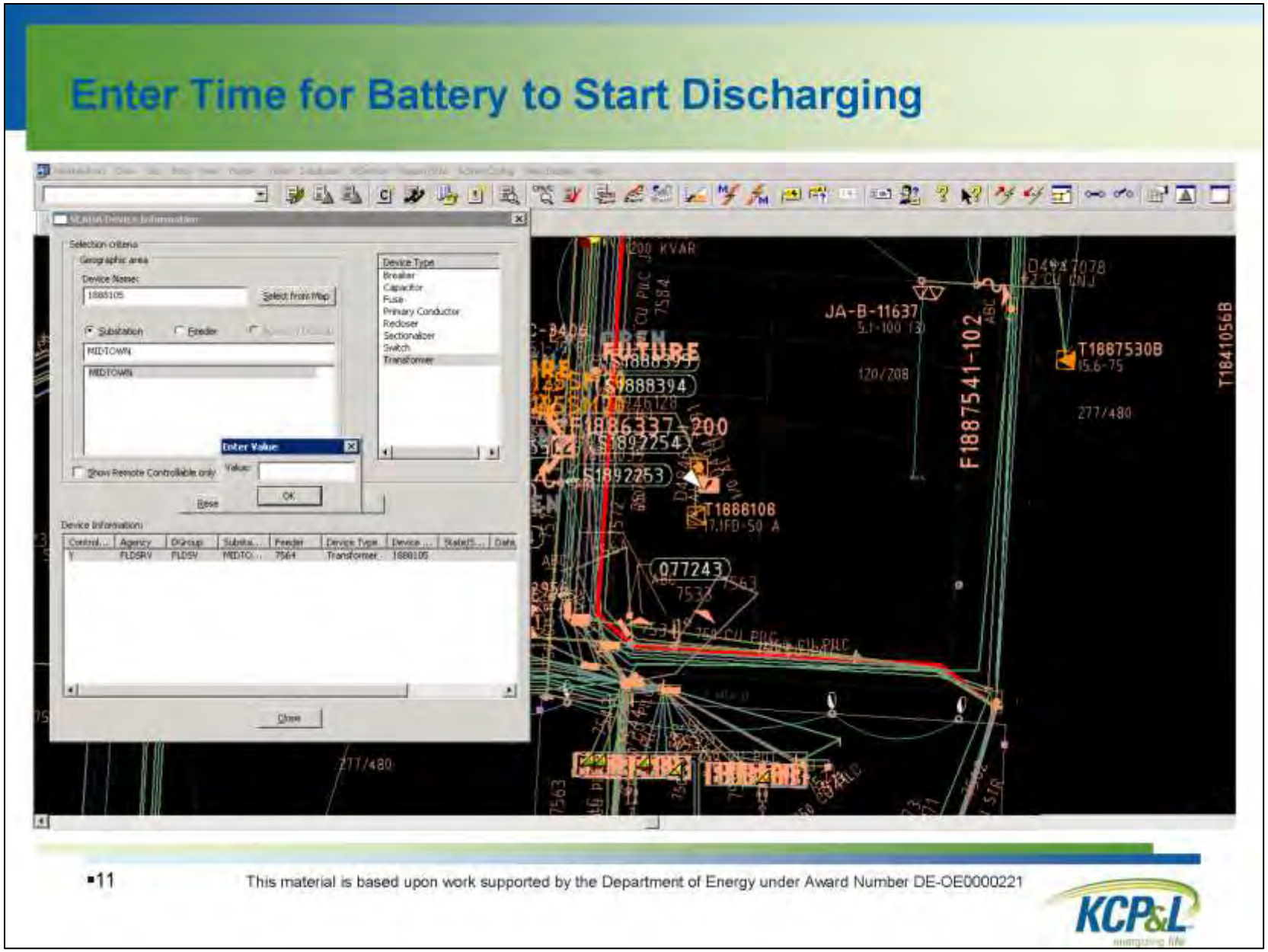

Set Battery to Load Following - Circuit Mode
SCADA Device Information
Selection criteria
Geographic area
Device Name:
Select from Map
Substation
Feeder
MIDTOWN
Device Type
Breaker
Capacitor
Fuse
Primary Conductor
Recloser
Sectionalizer
Switch
Transformer
Reset
Search
Stop
Device Information:
Close
Reset Battery
Schedule Override
Set Charge Mode
Set Power Mode
Set Reactive Mode
Set Recalculation Time (sec)
kVAR-Set DischargeDuration (min)
kVAR-Set Fixed PF (%)
kVAR-Set MaxDischargeRate
kVAR-SetDischargeStartTime(0-23)
kW - Set Load Following
kW - Set Max Charge Rate
kW - Set Max Discharge Rate
kW-Set ChargeDuration (min)
kW-Set ChargeFollowing
kW-Set ChargeStartTime (0-23)
kW-Set DischargeDuration (min)
kW-Set DischargeStartTime (0-23)
OFF
Fixed kW
LF-Ckt
LF-Buss
LF-Sol
DERM
ISLANDING
JA-B-11637
T1887530B
T1886108
F1887541-102
T1841056B
S1888394
S1892254
S1892253
077243
120/208
277/480
200 KVAR
FUTURE
8
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L
energizing life

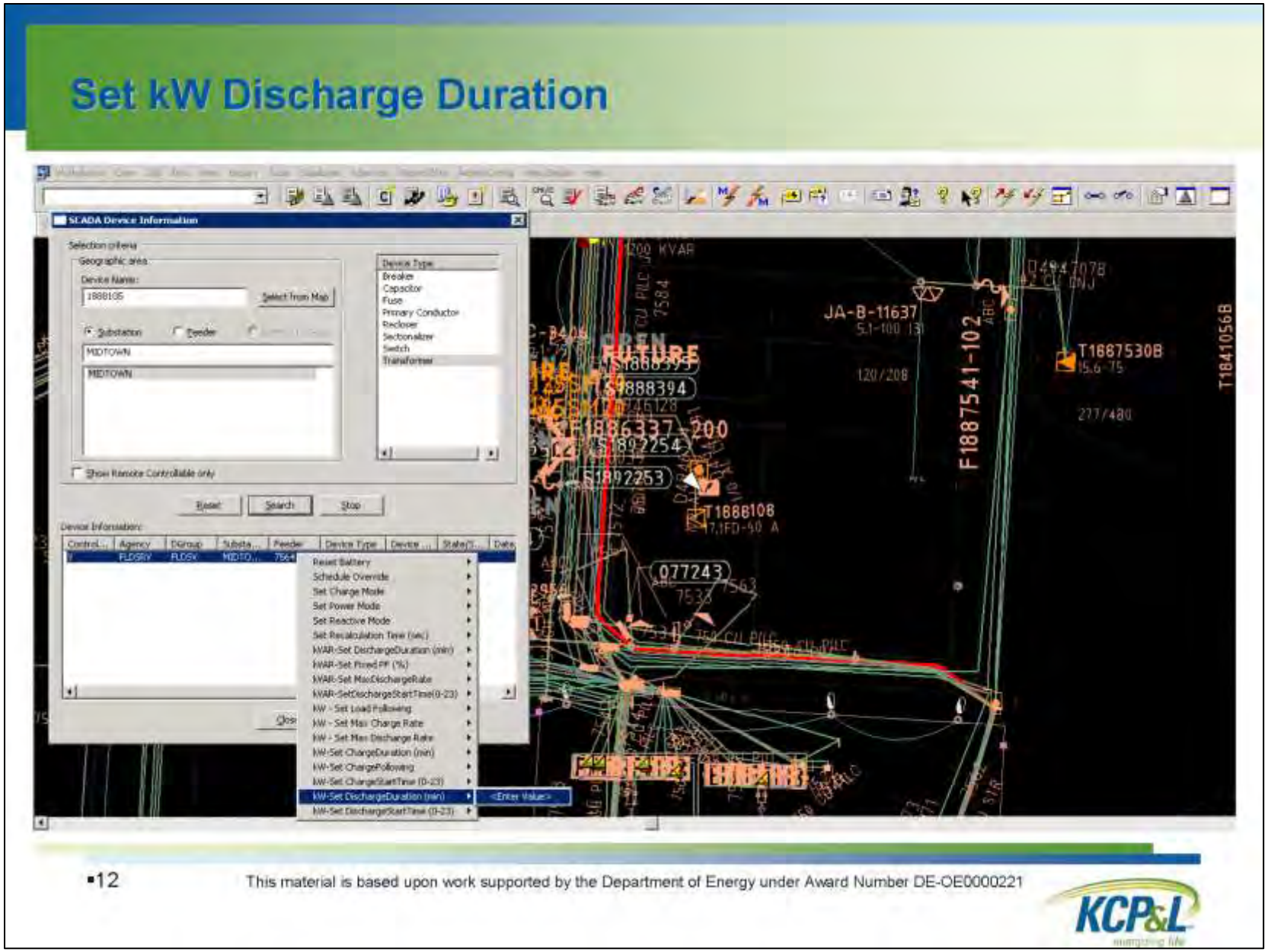
Battery set to LF-Ckt Power Mode

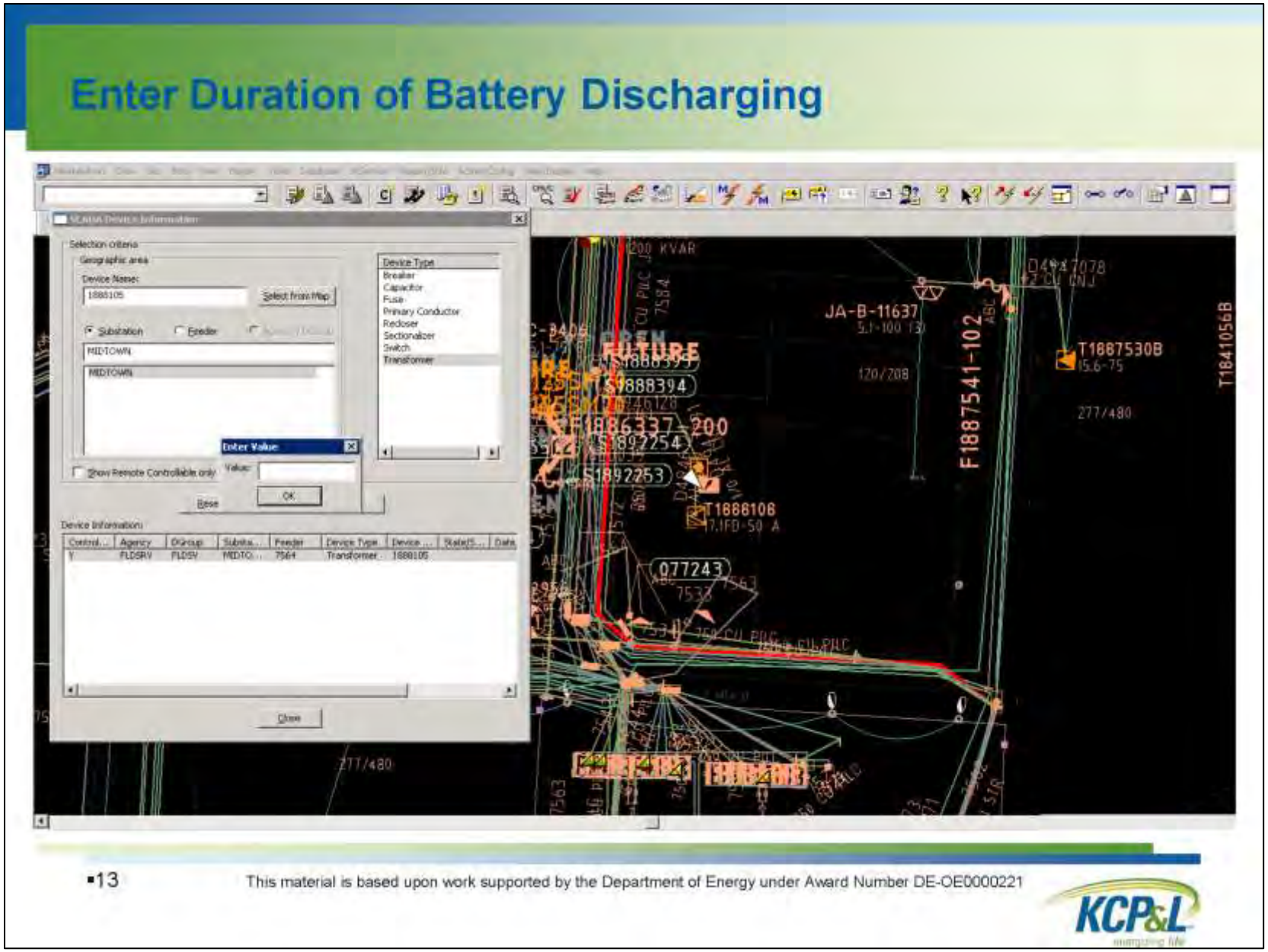


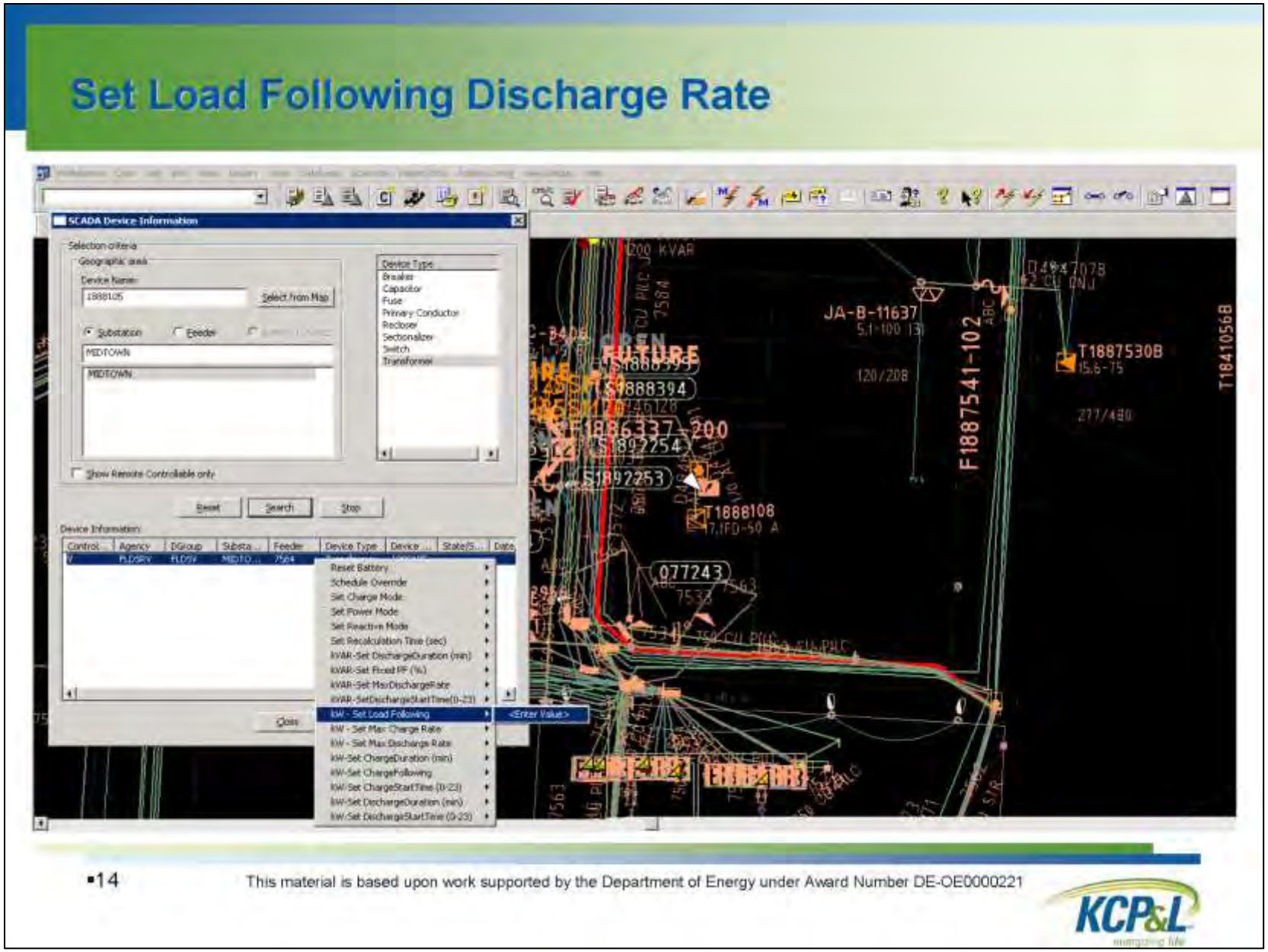
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

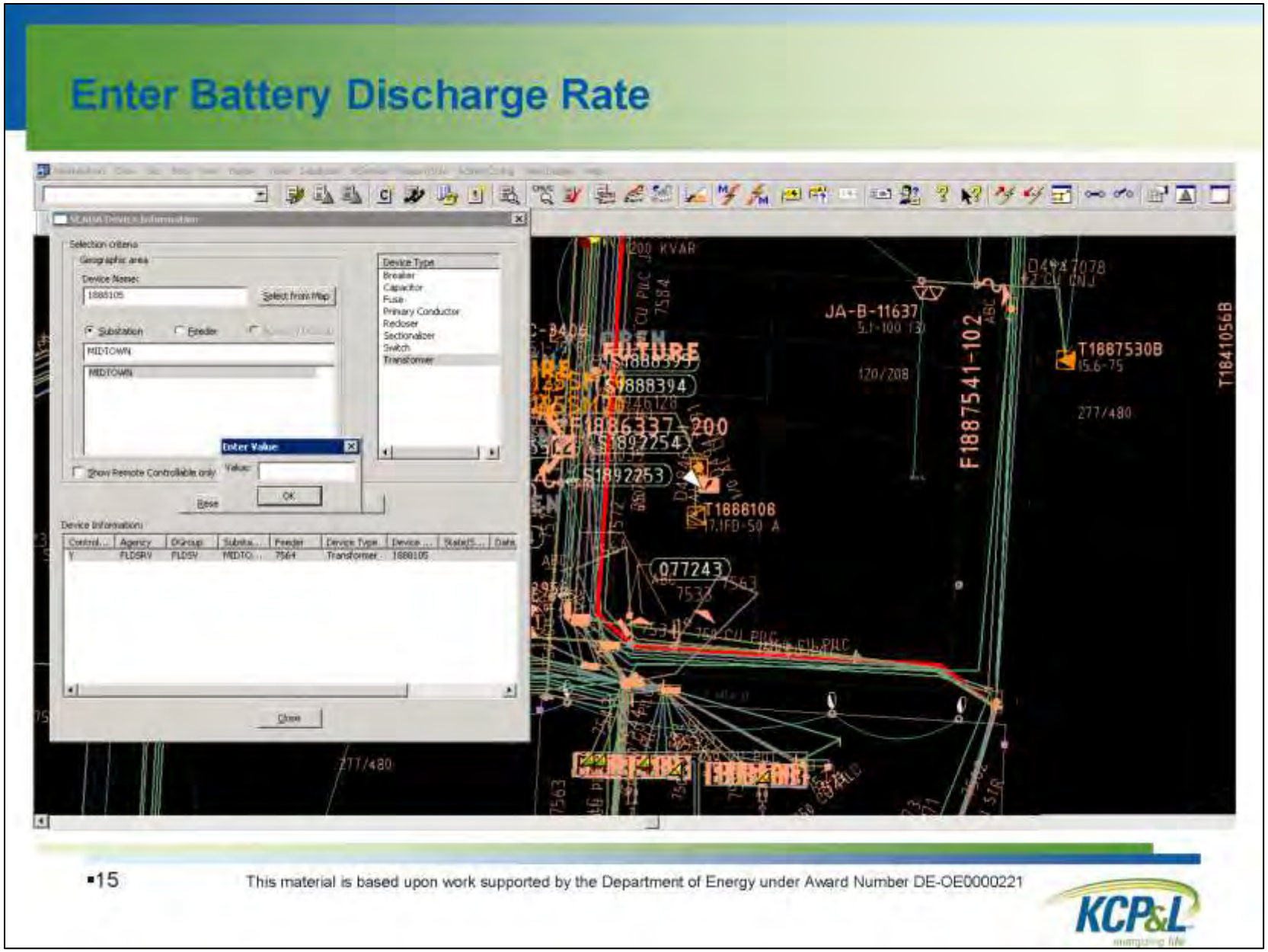

Set kW Discharge Start Time
SCADA Device Information
Selection criteria
Geographic area
Device Name:
1888105
Select from Map
Substation
Feeder
MIDTOWN
Device Type
Breaker
Capacitor
Fuse
Primary Conductor
Recloser
Sectionalizer
Switch
Transformer
Reset
Search
Stop
Device Information:
Control...
Agency
DGroup
Substa...
Feeder
Device Type
Device ...
State/S...
Date
Reset Battery
Schedule Override
Set Charge Mode
Set Power Mode
Set Reactive Mode
Set Recalculation Time (sec)
kVAR-Set DischargeDuration (min)
kVAR-Set Fixed PF (%)
kVAR-Set MaxDischargeRate
kVAR-SetDischargeStartTime(0-23)
kW - Set Load Following
kW - Set Max Charge Rate
kW - Set Max Discharge Rate
kW-Set ChargeDuration (min)
kW-Set ChargeFollowing
kW-Set ChargeStartTime (0-23)
kW-Set DischargeDuration (min)
kW-Set DischargeStartTime (0-23)
<Enter Value>
JA-B-11637
T18887308
T1888108
F1887541-102
T1841056B
077243
120/208
277/480
FUTURE
10
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L


Enter Time for Battery to Start Discharging
Selection criteria
Geographic area
Device Name:
1888105
Select from Map
Substation
Feeder
MIDTOWN
MIDTOWN
Device Type
Breaker
Capacitor
Fuse
Primary Conductor
Recloser
Sectionalizer
Switch
Transformer
Enter Value
Value:
OK
Base
Show Remote Controllable only
Device Information
Close
JA-B-11637
T1887530B
T1888108
T1841056B
F1887541-102
277/480
120/208
FUTURE
077243
11
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L
energizing life

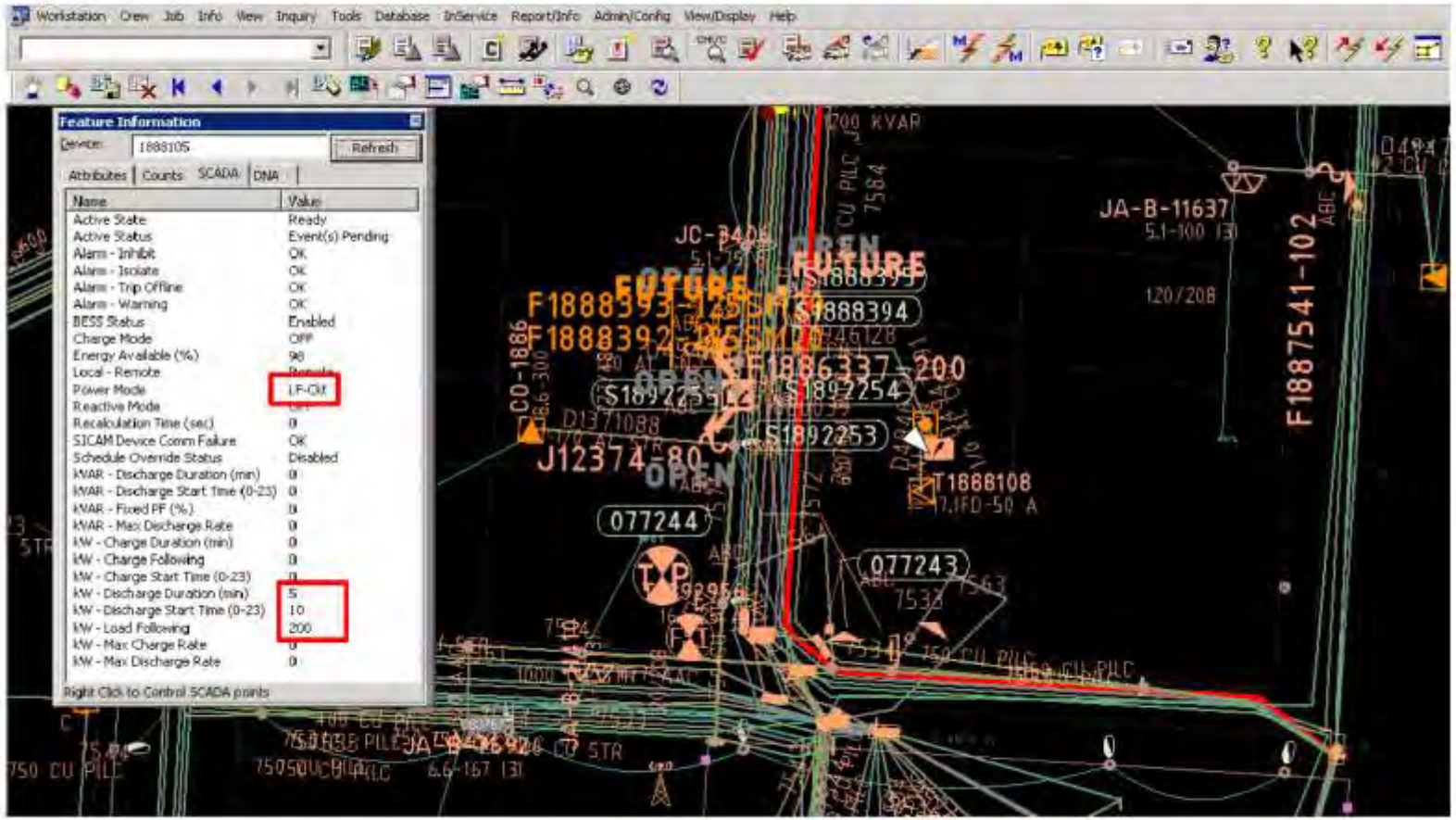

Set kW Discharge Duration
SCADA Device Information
Selection criteria
Geographic area
Device Name:
1888105
Select from Map
Substation
Feeder
MIDTOWN
MIDTOWN
Device Type
Breaker
Capacitor
Fuse
Primary Conductor
Recloser
Sectionalizer
Switch
Transformer
Show Remote Controllable only
Reset
Search
Stop
Device Information:
Control...
Agency
DGroup
Substa...
Feeder
Device Type
Device ...
State/T...
Date
Reset Battery
Schedule Override
Set Charge Mode
Set Power Mode
Set Reactive Mode
Set Recalculation Time (sec)
kVAR-Set DischargeDuration (min)
kVAR-Set Fixed PF (%)
kVAR-Set MaxDischargeRate
kVAR-SetDischargeStartTime(0-23)
kW - Set Load Following
kW - Set Max Charge Rate
kW - Set Max Discharge Rate
kW-Set ChargeDuration (min)
kW-Set ChargeFollowing
kW-Set ChargeStartTime (0-23)
kW-Set DischargeDuration (min)
kW-Set DischargeStartTime (0-23)
<Enter Value>
JA-B-11637
F1887541-102
T16875308
T1888108
T18410568
120/208
277/480
FUTURE
12
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L


Enter Duration of Battery Discharging
Selection criteria
Geographic area
Device Name:
1888105
Select from Map
Substation
Feeder
MIDTOWN
MIDTOWN
Device Type
Breaker
Capacitor
Fuse
Primary Conductor
Recloser
Sectionalizer
Switch
Transformer
Enter Value
Value:
OK
Base
Show Remote Controllable only
Device Information
Control...
Agency
DiGroup
Substa...
Feeder
Device Type
Device ...
State(S...
Data
Y
FLDSRV
FLDSV
MIDTO...
7564
Transformer
1888105
Close
JA-B-11637
T1887530B
T1888108
F1887541-102
T1841056B
277/480
120/208
FUTURE
077243
•13
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

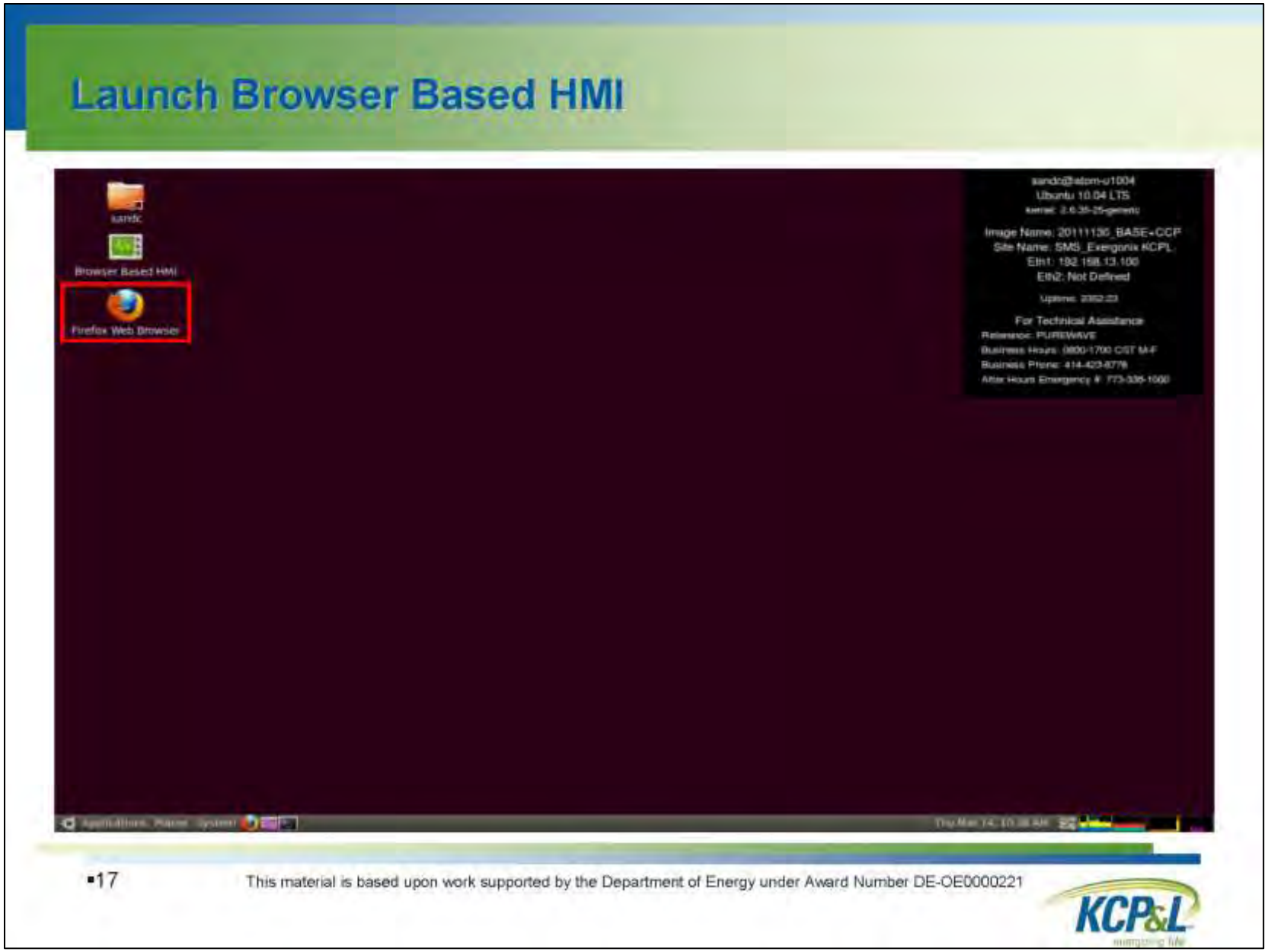

Set Load Following Discharge Rate
SCADA Device Information
Selection criteria
Geographic area
Device Name:
Select from Map
Substation
Feeder
MIDTOWN
Device Type
Breaker
Capacitor
Fuse
Primary Conductor
Recloser
Sectionalizer
Switch
Transformer
Show Remote Controllable only
Reset
Search
Stop
Device Information
Control...
Agency
DGroup
Substa...
Feeder
Device Type
Device ...
State/S...
Date
Reset Battery
Schedule Override
Set Charge Mode
Set Power Mode
Set Reactive Mode
Set Recalculation Time (sec)
kVAR-Set DischargeDuration (min)
kVAR-Set FixedPF (%)
kVAR-Set MaxDischargeRate
kVAR-SetDischargeStartTime(0-23)
kW - Set Load Following
<Enter Value>
kW - Set Max Charge Rate
kW - Set Max Discharge Rate
kW-Set ChargeDuration (min)
kW-Set ChargeFollowing
kW-Set ChargeStartTime (0-23)
kW-Set DischargeDuration (min)
kW-Set DischargeStartTime (0-23)
Close
JA-B-11637
T1887530B
F1887541-102
T1888108
FUTURE
S1888394
S1892254
S1892253
077243
T18410568
14
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L


Enter Battery Discharge Rate
Selection criteria
Geographic area
Device Name:
1888105
Select from Map
Substation
Feeder
MIDTOWN
MIDTOWN
Device Type
Breaker
Capacitor
Fuse
Primary Conductor
Recloser
Sectionalizer
Switch
Transformer
Enter Value
Value:
OK
Base
Show Remote Controllable only
Device Information
Close
JA-B-11637
T1887530B
T1888108
F1887541-102
T1841056B
277/480
120/208
15
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

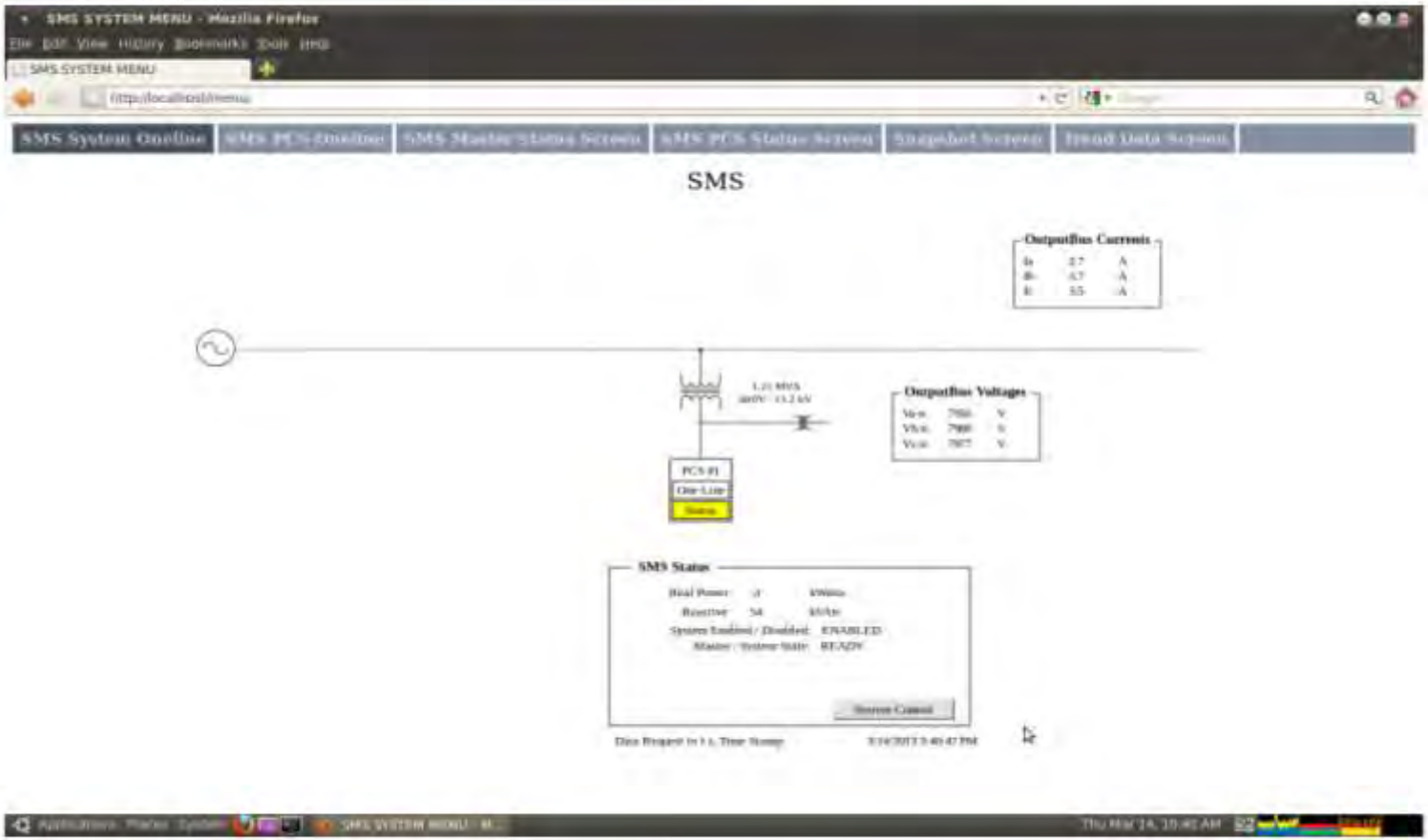
Battery Started to Discharge



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

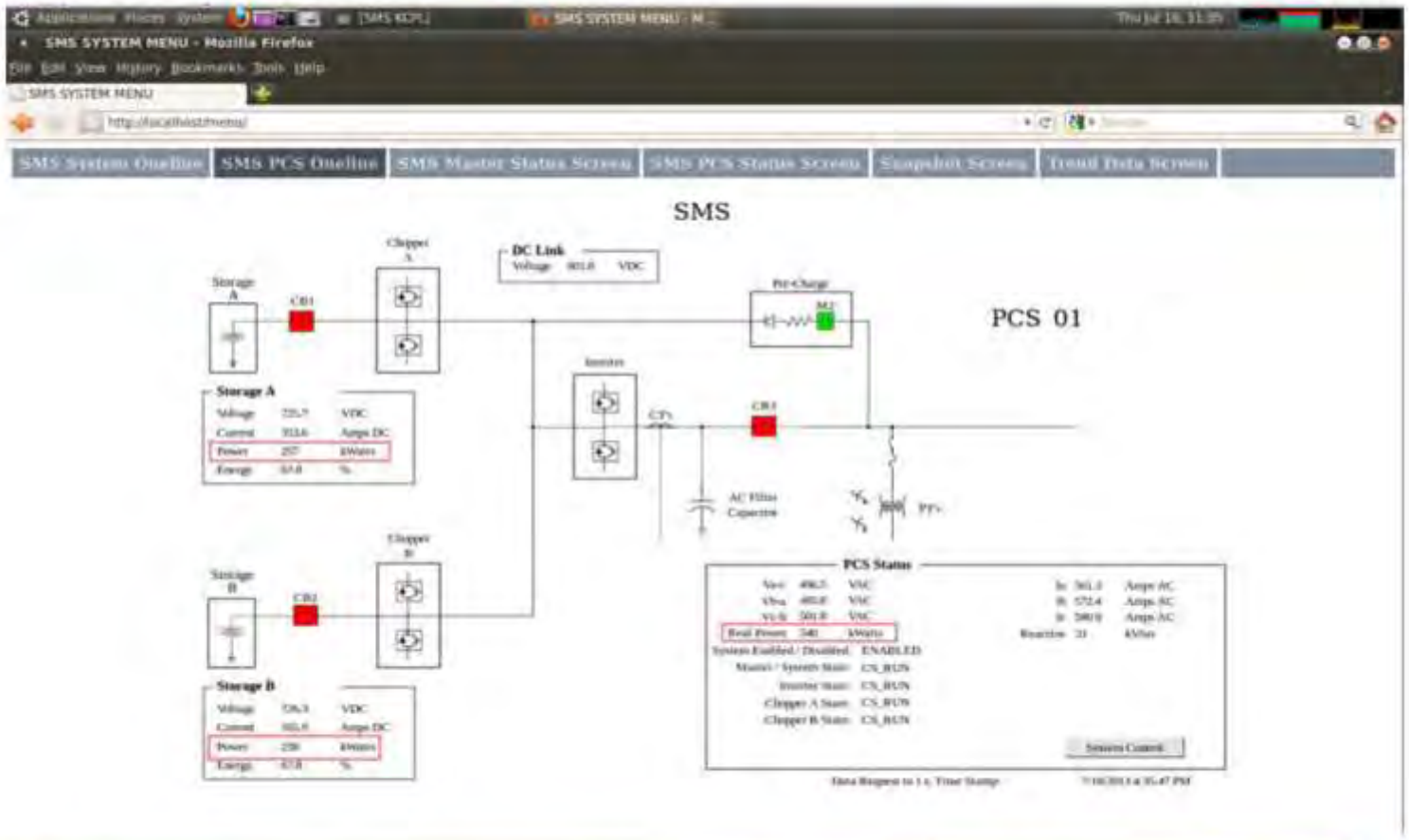

Launch Browser Based HMI
sandc
Browser Based HMI
Firefox Web Browser
Ubuntu 10.04 LTS
For Technical Assistance
17
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221
KCP&L

SMS System Menu Main Screen



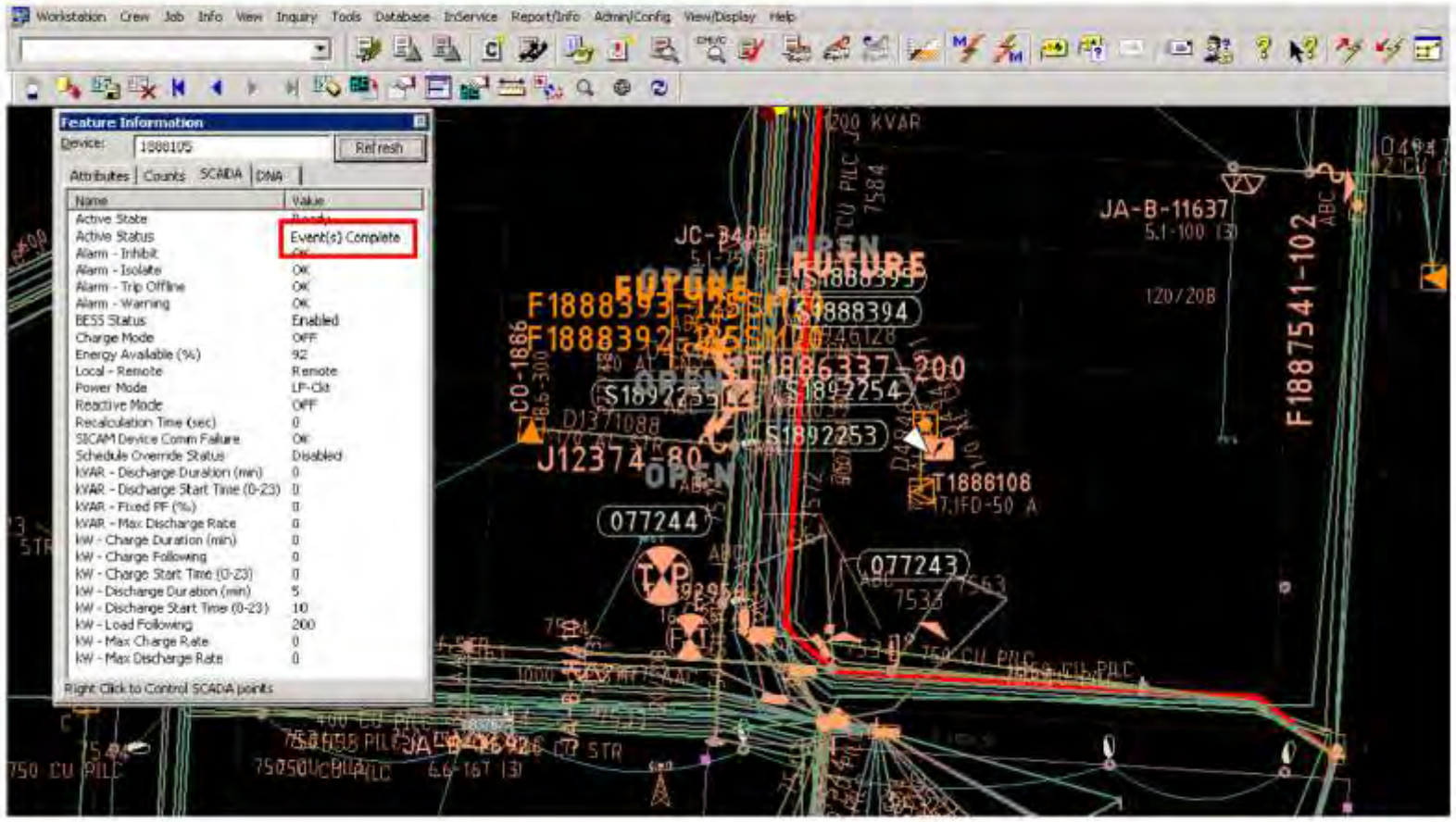
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

SMS PCS Oneline: Battery is Discharging



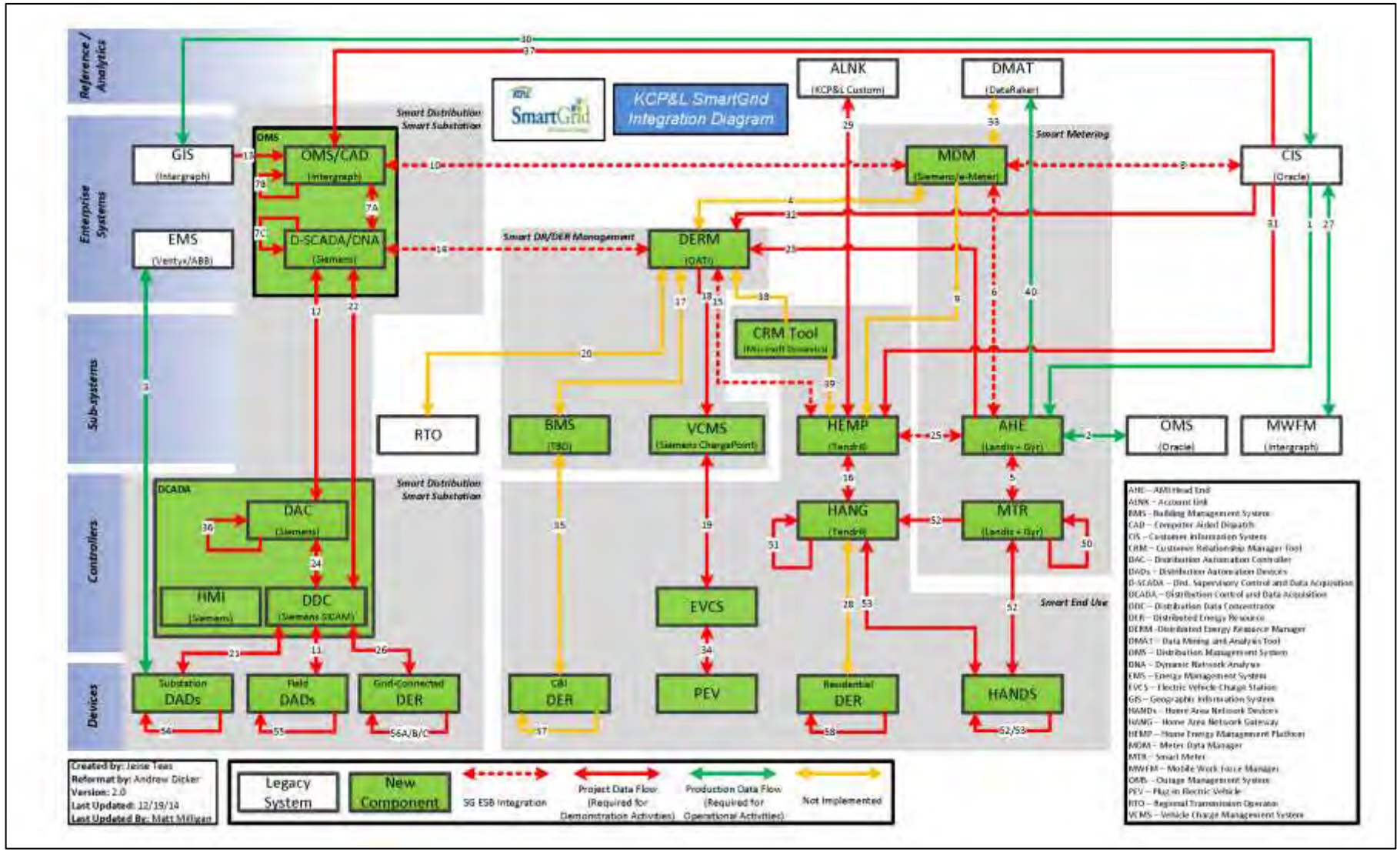
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Battery Finished Discharging



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Appendix L SmartGrid Interoperability Implemented



Msg ID	Producer (Actor 1)	Receiver (Actor 2)	Name of Process/Transaction	Description of Process/Transaction	Information Object Name	Information Object Description	Transport Method	Network Protocols	Interface Standard	Standard Msg Name
1.a.1	CIS	AHE	Daily Bill TrueUp Msg Transfer	CIS sends Daily Bill TrueUp Msg to AHE via Legacy MQ.	Daily Bill TrueUp Msg	Tunnel Text Msg from CIS to AHE that contains Daily Bill TrueUp data.	Legacy MQ	TCP/IP	N/A	N/A
2.a.1	AHE	OMS	Outage Event Msg Transfer	AHE sends Outage Event Msg to OMS via Legacy MQ.	Outage Event Msg	Msg generated by a MTR and sent from the MFR to the AHE when the MFR detects a sustained voltage loss lasting at least 30 seconds.	Legacy MQ	TCP/IP	MultiSpeak	ODEventNotification
2.b.1	OMS	AHE	On-Demand Meter Status Request Transfer	OMS issues On-Demand Meter Status Request to AHE via Legacy MQ. This process is also considered the Restoration Verification Application flow (RVA) internally.	On-Demand Meter Status Request	Request from OMS to AHE for current meter status, which is accomplished through a meter reading.	Legacy MQ	TCP/IP	MultiSpeak	GetOutagedODDevices
5.a.1	AHE	MFR	On-Demand Meter Read Request Transfer	AHE sends On-Demand Meter Read Request to MFR via FAN	On-Demand Meter Read Request	Request from AHE to MMB's internal reading table for current meter usage data.	FAN	L+G Proprietary	L+G Proprietary	Command(OnDemandRead)
5.a.2	AHE	MFR	On-Demand Meter Status Request Transfer	DMS issues On-Demand Meter Status Request to MDM via ESB	On-Demand Meter Status Request	Request from AHE to MMB's internal reading table for current meter reading data. This data is used to determine meter status.	FAN	L+G Proprietary	L+G Proprietary	Command(OnDemandRead)
5.a.3	AHE	MFR	Remote Service Order Request Transfer	AHE sends Remote Service Order Request to MFR	Remote Service Order Request	Remote request entered into AHE by AMIOP or external system.	FAN	L+G Proprietary	IEC 61968-9	CREATE(EndDeviceControls) CREATE(MeterReadings)
5.a.4	AHE	MFR	Commission HAN Command Transfer	AHE sends Commission HAN Command to MFR via FAN	Commission HAN Command	Command from the AHE to the MTR to turn on the ESI and enable the UHAN.	FAN	L+G Proprietary	L+G Proprietary	Command(CommissionHAN)
5.a.5	AHE	MFR	Provision HAND Command Transfer	AHE sends Provision HAND Command to MFR via FAN	Provision HAND Command	Request from AHE to MTR for HAND provisioning. Contains Meter ID, HAND MAC Address and HAND Install Code, and Allow Joining duration.	FAN	L+G Proprietary	L+G - Aligns with SEP 1.0	Command(ProvisionHANDevice)
5.a.6	AHE	MFR	Text Msg Transfer	AHE sends Text Msg to MFR via FAN	Text Msg	Request from AHE to ESI to send a text Msg to HAND. Contains text Msg, start time, duration and confirmation flag.	FAN	L+G Proprietary	L+G - Aligns with SEP 1.0	Command(HANMsg)
5.a.8	AHE	MFR	Pricing Signals Transfer	AHE sends Pricing Signals to MFR via FAN	Pricing Signals	Pricing information sent from AHE to ESI. Contains flat, time-of-use, or critical peak pricing.	FAN	L+G Proprietary	L+G - Aligns with SEP 1.0	Command(HANPricing)
5.a.9	AHE	MFR	HAND Pairing Info Request Transfer	AHE sends HAND Pairing Info Request to MFR via FAN	HAND Pairing Info Request	Request from AHE to ESI for HAND pairing information.	FAN	L+G Proprietary	L+G - Aligns with SEP 1.0	Command(GetPairingDetails)
5.a.10	AHE	MFR	HAND De-Provision Request Transfer	AHE sends HAND De-Provision Request to MFR via FAN	HAND De-Provision Request	Request sent from AHE to ESI for the de-provisioning of a HAND.	FAN	L+G Proprietary	L+G - Aligns with SEP 1.0	Command(DeprovisionHANDevice)
5.a.11	AHE	MFR	UHAN De-Commission Request Transfer	AHE sends UHAN De-Commission Request to MFR via FAN	UHAN De-Commission Request	Request from AHE to ESI for de-commissioning of the UHAN.	FAN	L+G Proprietary	L+G Proprietary	Command(DecommissionHAN)
5.a.12	AHE	MFR	DR Event Msg Transfer	AHE sends DR Event Msg to MFR via FAN	DR Event Msg	Msg from AHE to ESI, through MFR, that contains the load curtailment details for a specific MTR. Details are based upon the type of DR event and user defined preferences in the HEMP.	FAN	L+G Proprietary	L+G - Aligns with SEP 1.0	Command(LoadControl)
5.a.13	AHE	MFR	Gap-Filling Meter Read Request Transfer	AHE sends Gap-Filling Meter Read Request to MFR via FAN	Gap-Filling Meter Read Request	Request from AHE to MMB for a specific set of interval and/or register MTR data.	FAN	L+G Proprietary	L+G Proprietary	GET(MeterReadings)
5.a.15	AHE	MFR	MTR Configuration Update Transfer	AHE sends MTR Configuration Update to MFR of target MTR via FAN	MTR Configuration Update	Msg from AHE to MMB that contains a modification to the MTR Configuration.	FAN	L+G Proprietary	L+G Proprietary	N/A
5.a.16	AHE	MFR	MFR Firmware Update Transfer	AHE sends MFR Firmware Update to MFR of target MTR via FAN	MFR Firmware Update	Msg from AHE to MFR that contains a new version of firmware.	FAN	L+G Proprietary	L+G Proprietary	N/A
5.a.17	AHE	MFR	MMB Firmware Update Transfer	AHE sends MMB Firmware Update to MFR of target MTR via FAN	MMB Firmware Update	Msg from AHE to MMB that contains a new version of firmware.	FAN	L+G Proprietary	L+G Proprietary	N/A
5.a.18	AHE	MFR	ESI Firmware Update Transfer	AHE sends ESI Firmware Update to MFR of target MTR via FAN	ESI Firmware Update	Msg from AHE to ESI that contains a new version of firmware.	FAN	L+G Proprietary	L+G Proprietary	N/A
5.a.19	AHE	MFR	Daily Bill TrueUp Msg Transfer	AHE sends Daily Bill TrueUp Msg to MFR via FAN	Daily Bill TrueUp Msg	Tunnel Text Msg from AHE to ESI that contains Daily Bill TrueUp data.	FAN	L+G Proprietary	L+G - Aligns with SEP 1.0	Command(HANMsg)
5.b.1	MFR	AHE	On-Demand Meter Read Data Transfer	MFR sends On-Demand Meter Read Data to AHE via FAN	On-Demand Meter Read Data	Current meter usage data retrieved from MMB's internal reading table and sent to AHE.	FAN	L+G Proprietary	L+G Proprietary	Response(Readings)
5.b.2	MFR	AHE	On-Demand Meter Status Response Transfer	MFR sends On-Demand Meter Status Response to AHE via FAN	On-Demand Meter Status Response	Current meter reading data retrieved from MMB's internal reading table and sent to AHE. This data is used to determine meter status.	FAN	L+G Proprietary	L+G Proprietary	Response(Readings)
5.b.3	MFR	AHE	Aggregated Meter Read Data Transfer	MFR pulls Interval and Register Meter Read Data stored since its last data push and sends it to the AHE via FAN	Aggregated Meter Read Data	Aggregated data (could include Interval Meter Read Data and Register Meter Read Data) from a single MTR compiled at the MFR and sent to the AHE.	FAN	L+G Proprietary	L+G Proprietary	N/A
5.b.4	MFR	AHE	Outage Event Msg Transfer	MFR sends Outage Event Msg to AHE via FAN	Outage Event Msg	Msg generated by a MTR and sent from the MFR to the AHE when the MFR detects a sustained voltage loss lasting at least 30 seconds.	FAN	L+G Proprietary	L+G Proprietary	Event (Endpoint Power Outage)
5.b.5	MFR	AHE	Restoration Event Msg Transfer	MFR sends Restoration Event Msg to AHE via FAN	Restoration Event Msg	Msg generated by a MTR and sent from the MFR to the AHE when the MFR detects a voltage following an outage.	FAN	L+G Proprietary	L+G Proprietary	Event (Endpoint Power Restore)
5.b.6	MFR	AHE	Advisory Event Msg Transfer	MFR sends Advisory Event Msg to AHE via FAN	Advisory Event Msg	Msg generated in MTR and sent from the MFR to the AHE. Contains any MTR events defined as "advisory" that were created since the last data push.	FAN	L+G Proprietary	L+G Proprietary	Various. See AMI-06 for details.
5.b.7	MFR	AHE	Alarm Event Msg Transfer	MFR sends Alarm Event Msg to AHE via FAN	Alarm Event Msg	Msg generated in MTR and sent from the MFR to the AHE. Contains any MTR events defined as "alarm".	FAN	L+G Proprietary	L+G Proprietary	Various. See AMI-05 for details.
5.b.8	MFR	AHE	Remote Service Order Completion Msg Transfer	MFR issues Remote Service Order Completion Msg to the AHE via FAN	Remote Service Order Completion Msg	Response from MFR indicating that the Remote Service Order Request was received and implemented.	FAN	L+G Proprietary	IEC 61968-9	CREATED(EndDeviceControls) CREATED(MeterReading)

Msg ID	Producer (Actor 1)	Receiver (Actor 2)	Name of Process/Transaction	Description of Process/Transaction	Information Object Name	Information Object Description	Transport Method	Network Protocols	Interface Standard	Standard Msg Name
5.b.9	MFR	AHE	HAN Commissioned Response Transfer	MFR sends HAN Commissioned Response to AHE via FAN	HAN Commissioned Response Transfer	Response from the ESI to the AHE indicating that the ESI has been enabled and the UHAN has been established. Contains Meter ID and HAN Network ID.	FAN	L+G Proprietary	L+G Proprietary	Response(HANCommissioned)
5.b.10	MFR	AHE	Ready-to-Pair Response Transfer	MFR sends Ready-to-Pair Response to AHE via FAN	Ready-to-Pair Response	Response from MTR to AHE indicating UHAN is commissioned and ESI is ready to begin the pairing process.	FAN	L+G Proprietary	L+G - Aligns with SEP 1.0	Response(Ready-to-Pair)
5.b.11	MFR	AHE	Provision Complete Response Transfer	MFR sends Provision Complete Response to AHE via FAN	Provision Complete Response	Response from MTR to AHE indicating that HAND has been provisioned to ESI.	FAN	L+G Proprietary	L+G - Aligns with SEP 1.0	Response(PairingComplete)
5.b.12	MFR	AHE	Text Msg Response Transfer	MFR sends Text Msg Response to AHE via FAN	Text Msg Response	Confirmation from ESI to AHE that CUST acknowledged receipt of text Msg. Requirement for this Msg is controlled by the Text Msg.	FAN	L+G Proprietary	L+G - Aligns with SEP 1.0	Response(TextMsgCreated)
5.b.14	MFR	AHE	Pricing Signals Acknowledgement Transfer	MFR sends Pricing Signals Acknowledgement to AHE via FAN	Pricing Signals Acknowledgement	Acknowledgement from ESI to AHE that Pricing Signals were received. Requirement for this Msg is controlled by the Pricing Signals.	FAN	L+G Proprietary	L+G - Aligns with SEP 1.0	Response(HANPricing)
5.b.15	MFR	AHE	HAND Pairing Info Response Transfer	MFR sends HAND Pairing Info Response to AHE via FAN	HAND Pairing Info Response	Response from ESI to AHE containing HAND pairing information. Response includes MAC Address, Device Type and Pair ID.	FAN	L+G Proprietary	L+G - Aligns with SEP 1.0	Response(PairingDetails)
5.b.16	MFR	AHE	HAND De-Provision Confirmation Transfer	MFR sends HAND De-Provision Confirmation to AHE via FAN	HAND De-Provision Confirmation	Confirmation from ESI to AHE that the HAND has been de-provisioned.	FAN	L+G Proprietary	L+G - Aligns with SEP 1.0	Response(HANDeviceDeprovisioned)
5.b.17	MFR	AHE	UHAN De-Commission Confirmation Transfer	MFR sends UHAN De-Commission Confirmation to AHE via FAN	UHAN De-Commission Confirmation	Response from ESI to AHE confirming that the UHAN has been de-commissioned.	FAN	L+G Proprietary	L+G Proprietary	Response(HANDecommissioned)
5.b.18	MFR	AHE	DR Event Received Acknowledgement Transfer	MFR sends DR Event Received Acknowledgement to AHE via FAN	DR Event Received Acknowledgement	Response Msg from ESI to AHE, through MFR, indicating that the demand response event has been scheduled at the PCT.	FAN	L+G Proprietary	L+G - Aligns with SEP 1.0	Response(LoadControl)
5.b.19	MFR	AHE	Gap-Filling Meter Read Data Transfer	MFR sends Gap-Filling Meter Read Data to AHE via FAN	Gap-Filling Meter Read Data	Interval and/or register MTR data for a specific period of time that is retrieved from MMB and sent to AHE.	FAN	L+G Proprietary	L+G Proprietary	REPLY(MeterReadings)
5.b.21	MFR	AHE	MTR Configuration Update Confirmation Transfer	MFR sends MTR Configuration Update Confirmation to AHE via FAN	MTR Configuration Update Confirmation	Response Msg from MFR to AHE to confirm that MTR Configuration Update was made successfully.	FAN	L+G Proprietary	L+G Proprietary	N/A
5.b.22	MFR	AHE	MFR Firmware Update Confirmation Transfer	MFR sends MFR Firmware Update Confirmation to AHE via FAN	MFR Firmware Update Confirmation	Response Msg from MFR to AHE to confirm that firmware update was installed successfully.	FAN	L+G Proprietary	L+G Proprietary	N/A
5.b.23	MFR	AHE	MMB Firmware Update Confirmation Transfer	MFR sends MMB Firmware Update Confirmation to AHE via FAN	MMB Firmware Update Confirmation	Response Msg from MMB to AHE to confirm that firmware update was installed successfully.	FAN	L+G Proprietary	L+G Proprietary	N/A
5.b.24	MFR	AHE	ESI Firmware Update Confirmation Transfer	MFR sends ESI Firmware Update Confirmation to AHE via FAN	ESI Firmware Update Confirmation	Response Msg from ESI to AHE to confirm that firmware update was installed successfully.	FAN	L+G Proprietary	L+G Proprietary	N/A
5.b.26	MFR	AHE	DR Event Started Msg Transfer	MFR sends DR Event Started Msg to AHE via FAN	DR Event Started Msg	Msg from ESI to AHE, through MFR, indicating that the demand response event has started.	FAN	L+G Proprietary	L+G - Aligns with SEP 1.0	Response(LoadControl)
5.b.27	MFR	AHE	DR Event Completed Msg Transfer	MFR sends DR Event Completed Msg to AHE via FAN	DR Event Completed Msg	Msg from ESI to AHE, through MFR, indicating that the demand response event has ended.	FAN	L+G Proprietary	L+G - Aligns with SEP 1.0	Response(LoadControl)
6.a.1	MDM	AHE	On-Demand Meter Read Request Transfer	MDM sends On-Demand Meter Read Request to appropriate AHE via ESB	On-Demand Meter Read Request	Request from MDM to AHE for current meter usage data.	ESB	HTTP(S)	IEC 61968-9	REPLY(MeterReading)
6.a.2	MDM	AHE	On-Demand Meter Status Request Transfer	MDM sends On-Demand Meter Status Request to appropriate AHE via ESB	On-Demand Meter Status Request	Request from DMS (or other system) to AHE for current meter status, which is accomplished through a meter reading.	ESB	HTTP(S)	IEC 61968-9	GET(MeterReading)
6.a.3	MDM	AHE	Remote Service Order Completion Msg Transfer	MDM sends Remote Service Order Request to AHE via ESB.	Remote Service Order Request	Remote request forwarded by MDM. Original request entered into CIS by a CSR in the call center.	ESB	HTTP(S)	IEC 61968-9	CREATE(EndDeviceControls) CREATE(MeterReadings)
6.b.1	AHE	MDM	On-Demand Meter Read DataTransfer	AHE sends On-Demand Meter Read Data to MDM via ESB	On-Demand Meter Read Data	Current meter usage data retrieved from MMB's internal reading table and sent from AHE to CIS (or other system).	ESB	HTTP(S)	IEC 61968-9	REPLY(MeterReading)
6.b.2	AHE	MDM	On-Demand Meter Status Response Transfer	AHE sends On-Demand Meter Status Response to MDM via ESB	On-Demand Meter Status Response	Current meter reading data retrieved from MMB's internal reading table and sent from AHE to DMS (or other system). This data is used to determine meter status.	ESB	HTTP(S)	IEC 61968-9	REPLY(MeterReading)
6.b.3	AHE	MDM	Aggregated Multi-Meter Data Transfer	AHE pulls Aggregated Meter Read Data from multiple MTRs stored since its last data push and sends it to the MDM via ESB	Aggregated Multi-Meter Data	Aggregated data from multiple MTRs compiled at the AHE and sent as a batch file to the MDM.	ESB	HTTP(S)	IEC 61968-9	REPLY(MeterReadings)
6.b.4	AHE	MDM	Outage Event Msg Transfer	AHE sends Outage Event Msg to MDM via ESB	Outage Event Msg	Msg generated by a MTR and sent from the AHE to the MDM when the MFR detects a sustained voltage loss lasting at least 30 seconds.	ESB	HTTP(S)	IEC 61968-9	CREATED(EndDeviceEvents)
6.b.5	AHE	MDM	Restoration Event Msg Transfer	AHE sends Restoration Event Msg to MDM via ESB	Restoration Event Msg	Msg generated by a MTR and sent from the AHE to the MDM when the MFR detects a voltage following an outage.	ESB	HTTP(S)	IEC 61968-9	CREATED(EndDeviceEvents)
6.b.6	AHE	MDM	Advisory Alert Msg Transfer	AHE sends Advisory Event Msg to MDM via ESB	Advisory Event Msg	Msg sent from the AHE to the MDM. Contains any MTR events defined as "advisory" that were created since the last data push.	ESB	HTTP(S)	IEC 61968-9	CREATED(EndDeviceEvents) Various. See AMI-06 for details.
6.b.7	AHE	MDM	Alarm Event Msg Transfer	AHE sends Alarm Event Msg to MDM via ESB	Alarm Event Msg	Msg sent from the AHE to the MDM. Contains any MTR events defined as "alarm".	ESB	HTTP(S)	IEC 61968-9	CREATED(EndDeviceEvents) Various. See AMI-05 for details.
6.b.8	AHE	MDM	Remote Service Order Completion Msg Transfer	AHE forwards Remote Service Order Completion Msg to MDM via ESB.	Remote Service Order Completion Msg	Response from MFR indicating that the Remote Service Order Request was received and implemented.	ESB	HTTP(S)	IEC 61968-9	CREATED(EndDeviceControls)

Msg ID	Producer (Actor 1)	Receiver (Actor 2)	Name of Process/Transaction	Description of Process/Transaction	Information Object Name	Information Object Description	Transport Method	Network Protocols	Interface Standard	Standard Msg Name
7A.a.1	D-SCADA	OMS (DMS)	DAD Status Update Transfer	D-SCADA sends DAD Status Update to OMS (DMS sub-system) via the Back Office Network to be displayed to distribution system operators.	DAD Status Update	The message will contain the current value for either a digital or analog status point that is associated with a specific Substation or Field DAD. The message is triggered anytime D-SCADA receives a DAD Status Update from the downstream system (DDC).	Back Office Network	ICCP	IEC 60870-6	Various
7A.a.2	D-SCADA	OMS (DMS)	Model Updates Request Transfer	D-SCADA sends Model Updates Request to OMS (DMS sub-system) via the Back Office Network.	Model Updates Request	The message will contain a request for any available Tags, Manual Updates, and JCGs (Jumper Cuts and Grounds). The message is triggered when D-SCADA services are starting up.	Back Office Network	MQ	N/A	N/A
7A.a.3	D-SCADA	OMS (DMS)	DNA Notification Transfer	D-SCADA sends DNA Notification to OMS (DMS sub-system) via the Back Office Network to be displayed to distribution system operators.	DNA Notification	The message will contain the results of a DNA application that was run. The message is triggered anytime a distribution systems operator requests that a DNA application is run for a certain portion of the electrical model via the OMS GUI (the message is sent after the DNA application has finished running).	Back Office Network	MQ	N/A	N/A
7A.b.1	OMS (DMS)	D-SCADA	DAD Control Signal Transfer	OMS (DMS sub-system) sends DAD Control Signal to D-SCADA via the Back Office Network.	DAD Control Signal	The message will contain the desired value for either a digital or analog control point that is associated with a specific Substation or Field DAD. The message is triggered anytime a distribution systems operator enters a control via the OMS GUI.	Back Office Network	ICCP	IEC 60870-6	Various
7A.b.2	OMS (DMS)	D-SCADA	Model Updates Transfer	OMS (DMS sub-system) sends Model Updates to D-SCADA via the Back Office Network.	Model Updates	The message will contain any new Tags or Manual Updates. The message is triggered anytime D-SCADA sends a request and after a new Tag or Manual Update is applied to the model via the OMS GUI otherwise.	Back Office Network	MQ	N/A	N/A
7A.c.2	OMS (DMS)	DNA	Model Updates Transfer	OMS (DMS sub-system) sends Model Updates to DNA via the Back Office Network.	Model Updates	The message will contain any new JCGs (Jumper Cuts and Grounds). The message is triggered anytime D-SCADA sends a request and after a new JCG is applied to the model via the OMS GUI otherwise.	Back Office Network	MQ	N/A	N/A
7B.a.1	OMS (DMS)	CAD	Internal Process Communication	These messages are used for internal processes.	Internal Process Data	This data is used for internal control processes.	DMS Internal	Intergraph Proprietary	N/A	N/A
7B.b.1	CAD	OMS (DMS)	Internal Process Communication	These messages are used for internal processes.	Internal Process Data	This data is used for internal control processes.	DMS Internal	Intergraph Proprietary	N/A	N/A
7C.a.1	D-SCADA	DNA	DAD Status Update Transfer	D-SCADA sends DAD Status Update to DNA to perform advanced analysis.	DAD Status Update	The message will contain the current value for either a digital or analog status point that is associated with a specific Substation or Field DAD. The message is triggered anytime a distribution systems operator requests that a DNA application is run for a certain portion of the electrical model via the OMS GUI.	DMS Internal	Siemens Proprietary	N/A	N/A
7C.b.1	DNA	D-SCADA	DAD Control Signal Transfer	After performing advanced analysis, DNA sends DAD Control Signal to D-SCADA.	DAD Control Signal	The message will contain the desired value for either a digital or analog control point that is associated with a specific Substation or Field DAD. The value is based upon the results of the analysis performed by a DNA application.	DMS Internal	Siemens Proprietary	N/A	N/A
8.a.1	CIS	MDM	On-Demand Meter Read Request	CIS issues On-Demand Meter Read Request to MDM via ESB.	On-Demand Meter Read Request	Request from CIS (or other system) to MDM for current meter usage data.	ESB	TCP/IP	IEC 61968-9	GET(MeterReading)
8.a.2	CIS	MDM	Remote Service Order Request Transfer	CIS issues Remote Service Order Request to MDM via ESB.	Remote Service Order Request	Remote request entered into CIS by a CSR in the call center.	ESB	TCP/IP	IEC 61968-9	CREATE(MeterServiceRequest)
8.b.1	MDM	CIS	On-Demand Meter Read Data Transfer	MDM sends On-Demand meter Read Data to CIS via the ESB.	On-Demand Meter Read Data	Current meter usage data retrieved from MMB's internal reading table and sent from AHE to CIS (or other system).	ESB	TCP/IP	IEC 61968-9	REPLY(MeterReading)
8.b.2	MDM	CIS	Remote Service Order Completion Msg Transfer	MDM forwards Remote Service Order Completion Msg to CIS via ESB.	Remote Service Order Completion Msg	Response from MFR indicating that the Remote Service Order Request was received and implemented.	ESB	TCP/IP	IEC 61968-9	UPDATED(MeterServiceRequest)
10.a.1	OMS (DMS)	MDM	On-Demand Meter Status Request	OMS (DMS sub-system) issues On-Demand Meter Status Request to MDM via ESB	On-Demand Meter Status Request	Request from OMS (DMS sub-system) to AHE for current meter status, which is accomplished through a meter reading.	ESB	TCP/IP	IEC 61968-9	GET(MeterReading)
10.b.1	MDM	OMS (DMS)	On-Demand Meter Status Response Transfer	MDM sends On-Demand Meter Status Response to OMS (DMS sub-system) via ESB	On-Demand Meter Status Response	Current meter reading data retrieved from MMB's internal reading table and sent from AHE to OMS (DMS sub-system). This data is used to determine meter status.	ESB	TCP/IP	IEC 61968-9	REPLY(MeterReading)
10.b.2	MDM	OMS (DMS)	Outage Event Msg Transfer	MDM sends Outage Event Msg to OMS (DMS sub-system) via ESB, if necessary	Outage Event Msg	Msg generated by a MTR and sent from the MDM to the OMS (DMS sub-system) when the MFR detects a sustained voltage loss lasting at least 30 seconds.	ESB	TCP/IP	IEC 61968-9	CREATED(EndDeviceEvents)
10.b.3	MDM	OMS (DMS)	Restoration Event Msg Transfer	MDM sends Restoration Event Msg to OMS (DMS sub-system) via ESB	Restoration Event Msg	Msg generated by a MTR and sent from the MDM to the OMS (DMS sub-system) when the MFR detects a voltage following an outage.	ESB	TCP/IP	IEC 61968-9	CREATED(EndDeviceEvents)
11.a.1	DDC	Field DAD	DAD Status Request Transfer	DDC sends DAD Status Request to a Field DAD via DAN	DAD Status Request	A Msg sent from DAC to DDC and a Field DAD containing a request for the configuration settings of the Field DAD.	DAN	DNP3	IEEE 1815	Various
11.a.2	DDC	Field DAD	Circuit Reconfiguration Transfer	DDC sends Circuit Reconfiguration to a Field DAD via DAN	Circuit Reconfiguration	A command sent from DAC to a Field DAD containing the configuration settings of the Field DAD.	DAN	DNP3	IEEE 1815	Various
11.a.3	DDC	Field DAD	DAD Status Request Transfer	DDC sends DAD Status Request to all Field DADs within the area of control via the DAN	DAD Status Request	Monitor request sent by DCADA to one or more Field DADs to determine optimal system parameters.	DAN	DNP3	IEEE 1815	Various

Msg ID	Producer (Actor 1)	Receiver (Actor 2)	Name of Process/Transaction	Description of Process/Transaction	Information Object Name	Information Object Description	Transport Method	Network Protocols	Interface Standard	Standard Msg Name
11.a.4	DDC	Field DAD	DAD Control Signal Transfer	DDC sends DAD Control Signal to all relevant Field DADs via DAN	DAD Control Signal	Updated configuration settings for one or more Field DADs as determined by VVC.	DAN	DNP3	IEEE 1815	Various
11.a.5	DDC	Field DAD	DAD Control Signal Transfer	DDC sends DAD Control Signal to a Field DAD via DAN to initiate load reduction	Field DAD Control Signal	Configuration settings for a Field DAD sent from DCADA to the Field DAD.	DAN	DNP3	IEEE 1815	Various
11.b.1	Field DAD	DDC	DAD Status Response Transfer	Field DAD sends DAD Status Response to DDC via DAN	DAD Status Response	A Msg sent from a Field DAD to DDC containing the configuration settings of the Field DAD.	DAN	DNP3	IEEE 1815	Various
11.b.2	Field DAD	DDC	DAD Status Update Transfer	Field DAD sends DAD Status Update to DDC via DAN	DAD Status Update	A Msg sent from a Field DAD to DAC containing the configuration settings of the Field DAD.	DAN	DNP3	IEEE 1815	Various
11.b.3	Field DAD	DDC	DAD Status Response Transfer	Field DAD sends DAD Status Response to DDC via DAN	DAD Status Response	Response from a Field DAD to DCADA that DAD Status has been sent.	DAN	DNP3	IEEE 1815	Various
11.b.4	Field DAD	DDC	DAD Alarm Report	Field DAD sends DAD Alarm to DDC via DAN	Field DAD Alarm	An alarm Msg sent from a Field DAD to DCADA to report an alert condition that has occurred at the Field DAD.	DAN	DNP3	IEEE 1815	Various
11.b.5	Field DAD	DDC	DAD Status Report	DAD sends DAD Status Update to DDC via DAN	Field DAD Status	A Msg containing DAD status sent from a Field DAD to DCADA.	DAN	DNP3	IEEE 1815	Various
12.a.1	D-SCADA	DAC	Model Updates Transfer	D-SCADA sends Model Updates to DAC via the Backhaul WAN.	Model Updates	The message will contain any new Tags or Manual Updates. The message is triggered anytime DAC sends a request and after a new Tag or Manual Update is applied to the model via the OMS GUI otherwise.	Backhaul WAN	Siemens Proprietary	N/A	N/A
12.b.1	DAC	D-SCADA	Model Updates Request Transfer	DAC sends Model Updates Request to D-SCADA via the Backhaul WAN.	Model Updates Request	The message will contain a request for any available Tags, Manual Updates, and JCGs (Jumper Cuts and Grounds). The message is triggered when DAC services are starting up.	Backhaul WAN	Siemens Proprietary	N/A	N/A
12.b.2	DAC	D-SCADA	DNA Notification Transfer	DAC sends DNA Notification to D-SCADA via the Backhaul WAN to be displayed to distribution system operators via the OMS GUI.	DNA Notification	The message will contain the results of a DNA application that was run. The message is triggered anytime a DNA application is run for a certain portion of the electrical model while DAC is in control (the message is sent after the DNA application has finished running).	Backhaul WAN	Siemens Proprietary	N/A	N/A
12.c.1	DNA	DAC	Model Updates Transfer	DNA sends Model Updates to DAC via the Back Office Network.	Model Updates	The message will contain any new JCGs (Jumper Cuts and Grounds). The message is triggered anytime DAC sends a request and after a new JCG is applied to the model via the OMS GUI otherwise.	Backhaul WAN	Siemens Proprietary	N/A	N/A
13.a.1	GIS	OMS (DMS)	Map Migration	GIS sends current Map Data to the OMS (DMS sub-system) via the Back Office Network. This process mostly consists of manual steps.	Map Data	Current geographical data needed to build the OMS map is retrieved from GIS on an ad hoc basis and sent to OMS.	Back Office Network	TCP/IP	N/A	N/A
14.a.1	D-SCADA	DERM	Network Model Sync Response Transfer	D-SCADA sends Network Model Sync Response to DERM via ESB.	Network Model Sync Response	The message contains a list of all the switches that currently in an abnormal state. It is a response to the GetDiscreteMeasurements message sent from DERM to D-SCADA.	ESB	HTTP(S) & JMS MQ	IEC 61968-3 with extenstions	ReplyDiscreteMeasurements (KCP&L Msg Name)
14.a.2	D-SCADA	DERM	DPF Results Response Transfer	D-SCADA sends DPF Results Response to DERM via ESB.	DPF Results Response	The message contains the requested set of DPF (Distribution Power Flow) results. It is a response to the GetDistributionPowerFlowLimitViolation message sent from DERM to D-SCADA.	ESB	HTTP(S) & JMS MQ	IEC 61968-3 with extenstions	ReplyDistributionPowerFlowLimitViolation (KCP&L Msg Name)
14.a.3	D-SCADA	DERM	DPF Limit Violations Modification Notification Transfer	D-SCADA sends DPF Limit Violations Modification Notification to DERM via ESB.	DPF Limit Violations Modification Notification	The message contains one or more existing DPF (Distribution Power Flow) limit violations that have been modified.	ESB	HTTP(S) & JMS MQ	IEC 61968-3 with extenstions	ChangedDistributionPowerFlowLimitViolation (KCP&L Msg Name)
14.a.4	D-SCADA	DERM	DPF Limit Violations Creation Notification Transfer	D-SCADA sends DPF Limit Violations Creation Notification to DERM via ESB.	DPF Limit Violations Creation Notification	The message contains the DPF (Distribution Power Flow) limit violations that have been created.	ESB	HTTP(S) & JMS MQ	IEC 61968-3 with extenstions	CreatedDistributionPowerFlowLimitViolation (KCP&L Msg Name)
14.a.5	D-SCADA	DERM	DPF Limit Violations Deletion Notification Transfer	D-SCADA sends DPF Limit Violations Deletion Notification to DERM via ESB.	DPF Limit Violations Deletion Notification	The message contains the DPF (Distribution Power Flow) limit violations that have been deleted.	ESB	HTTP(S) & JMS MQ	IEC 61968-3 with extenstions	DeletedDistributionPowerFlowLimitViolation (KCP&L Msg Name)
14.a.6	D-SCADA	DERM	DR Event List Request Transfer	DERM sends DR Event List Request to D-SCADA via ESB.	DR Event List Request	This message contains a request for the list of the currently scheduled DR (Demand Response) events.	ESB	HTTP(S) & JMS MQ	IEC 61968-3 with extenstions	GetDemandResourceControls (KCP&L Msg Name)
14.a.7	D-SCADA	DERM	Network Model Status Change Notification Transfer	D-SCADA sends Network Model Status Change Notification to DERM via ESB.	Network Model Status Change Notification	The message contains a list of all the spontaneous switch status changes.	ESB	HTTP(S) & JMS MQ	IEC 61968-3 with extenstions	ChangedDiscreteMeasurements (KCP&L Msg Name)
14.a.8	D-SCADA	DERM	DR Event Msg Response Transfer	D-SCADA sends DR Event Msg Response to DERM via ESB.	DR Event Msg Response	Msg from D-SCADA to DERM to acknowledge opt-in or opt-out disposition for a previously created DR (Demand Response) event for the Grid-Connected DER. It is a response to the oadrDistributeEvent message sent from DERM to D-SCADA.	ESB	HTTP(S) & JMS MQ	OpenADR	oadrCreatedEvent
14.a.9	D-SCADA	DERM	Network Static Model Transfer	D-SCADA sends Network Static Model to DERM.	Network Static Model	The file contains the current Network Static Model from D-SCADA. It is manually extracted and transferred after a new model is built in D-SCADA.	Internet	TCP/IP	IEC 61970-552	N/A

Msg ID	Producer (Actor 1)	Receiver (Actor 2)	Name of Process/Transaction	Description of Process/Transaction	Information Object Name	Information Object Description	Transport Method	Network Protocols	Interface Standard	Standard Msg Name
14.b.1	DERM	D-SCADA	Network Model Sync Request Transfer	DERM sends Network Model Sync Request to D-SCADA via ESB.	Network Model Sync Request	The message contains a request for DERM to synchronize its dynamic network model with the DMS. The message can be sent in real-time, after DERM re-starts following the creation of a new Study Case in DMS, or after a different set of dynamic data has been loaded into the DMS.	ESB	HTTP(S) & JMS MQ	IEC 61968-3 with extenstions	GetDiscreteMeasurements (KCP&L Msg Name)
14.b.2	DERM	D-SCADA	DPF Results Request Transfer	DERM sends DPF Results Request to D-SCADA via ESB.	DPF Results Request	The message enables DERM to query DMS for a specific set of DPF (Distribution Power Flow) results.	ESB	HTTP(S) & JMS MQ	IEC 61968-3 with extenstions	GetDistributionPowerFlowLimitViolation (KCP&L Msg Name)
14.b.3	DERM	D-SCADA	DR Event Creation Notification Transfer	DERM sends DR Event Creation Notification to D-SCADA via ESB.	DR Event Creation Notification	This message is a notification to D-SCADA that DERM has created a DR (Demand Response) event.	ESB	HTTP(S) & JMS MQ	IEC 61968-3 with extenstions	CreatedDemandResourceControls (KCP&L Msg Name)
14.b.4	DERM	D-SCADA	DR Event Modification Notification Transfer	DERM sends DR Event Modification Notification to D-SCADA via ESB.	DR Event Modification Notification	This message is a notification to D-SCADA that DERM has modified an existing DR (Demand Response) event.	ESB	HTTP(S) & JMS MQ	IEC 61968-3 with extenstions	ChangedDemandResourceControls (KCP&L Msg Name)
14.b.5	DERM	D-SCADA	DR Event Deletion Notification Transfer	DERM sends DR Event Deletion Notification to D-SCADA via ESB.	DR Event Deletion Notification	This message is a notification to D-SCADA that DERM has deleted an existing DR (Demand Response) event.	ESB	HTTP(S) & JMS MQ	IEC 61968-3 with extenstions	DeletedDemandResourceControls (KCP&L Msg Name)
14.b.6	DERM	D-SCADA	DR Event List Response Transfer	DERM sends DR Event List Response to D-SCADA via ESB.	DR Event List Response	This message includes a list of the currently scheduled DR (Demand Response) events. It is a response to the GetDemandResourceControls message sent from D-SCADA to DERM.	ESB	HTTP(S) & JMS MQ	IEC 61968-3 with extenstions	ReplyDemandResourceControls (KCP&L Msg Name)
14.b.8	DERM	D-SCADA	DR Event Msg Transfer	DERM sends DR Event Msg to D-SCADA via ESB.	DR Event Msg	Msg from DERM to D-SCADA to schedule a utility-managed DR (Demand Response) event for the Grid-Connected DER.	ESB	HTTP(S) & JMS MQ	OpenADR	oadrDistributeEvent
15.a.1	DERM	HEMP	DR Event Msg Transfer	DERM sends DR Event Msg to HEMP via ESB.	DR Event Msg	Msg from DERM to HEMP to schedule, modify, or cancel a utility-managed DR (Demand Response) event.	ESB	HTTP(S)	OpenADR	oadrDistributeEvent
15.b.1	HEMP	DERM	DR Event Msg Response Transfer	HEMP sends DR Event Msg Response to DERM via ESB, if required.	DR Event Msg Response	Msg from HEMP to DERM to acknowledge opt-in or opt-out disposition for a previously created DR (Demand Response) event. This Msg is only sent if the corresponding DR Event Msg required a response from HEMP.	ESB	HTTP(S)	OpenADR	oadrCreatedEvent
16.a.1	HEMP	IPI	Text Msg Transfer	HEMP sends Text Msg to IPI	Text Msg	Request from HEMP to CHR to send a text Msg to HAND. Contains text Msg, start time, duration and confirmation flag.	Internet	TCP/IP	Tendril - Aligns with SEP 1.0	N/A
16.a.3	HEMP	IPI	HEMP Settings Update Transfer	HEMP sends HEMP Settings Update to IPI	HEMP Settings Update	Msg from HEMP to CHR containing changes to the HEMP settings including set piont, fan operation and daily/weekly schedule.	Internet	TCP/IP	Tendril - Aligns with SEP 1.0	N/A
16.a.4	HEMP	IPI	HEMP Settings Update Transfer	HEMP sends HEMP Settings Update to IPI	HEMP Settings Update	Msg from HEMP to CHR containing changes to the HEMP settings. Includes schedule and on/off state.	Internet	TCP/IP	Tendril - Aligns with SEP 1.0	N/A
16.a.5	HEMP	IPI	HAND De-Provision Request Transfer	HEMP sends HAND De-Provision Request to IPI	HAND De-Provision Request	Request from HEMP to CHR to de-provision a HAND from the HANG.	Internet	TCP/IP	Aligns with ZigBee SEP 1.0	N/A
16.a.6	HEMP	IPI	Cancel Text Msg Request Transfer	HEMP sends Cancel Text Msg Request to IPI	Cancel Text Msg Request	Request from HEMP to CHR to cancel a previously sent text Msg. Includes ID of previously sent Msg and, optionally, requests and acknowledgement of receipt.	Internet	TCP/IP	Tendril - Aligns with SEP 1.0	N/A
16.b.1	IPI	HEMP	Text Msg Response Transfer	IPI sends Text Msg Response to HEMP	Text Msg Response	Confirmation from CHR to HEMP that CUST acknowledged receipt of text Msg. Requirement for this Msg is controlled by the Text Msg.	Internet	TCP/IP	Tendril - Aligns with SEP 1.0	N/A
16.b.2	HANG	HEMP	HANG Information Transfer	HANG sends HANG Information to HEMP	HANG Information	MAC Address and Install Code for the HANG. Provided by the HANG manufacturer and typically printed on a sticker applied to the device.	Internet	TCP/IP	Tendril - Aligns with SEP 1.0	MAC Address Install Code
16.b.5	IPI	HEMP	PCT Settings Update Transfer	IPI sends PCT Settings Update to HEMP	PCT Settings Update	Msg from CHR to HEMP containing changes to the PCT settings including set point, fan operation and daily/weekly schedule.	Internet	TCP/IP	Tendril - Aligns with SEP 1.0	N/A
16.b.7	IPI	HEMP	Cancel Text Msg Response Transfer	IPI sends Cancel Text Msg Response to HEMP	Cancel Text Msg Confirmation	Confirmation from CHR to HEMP indicating successful cancellation of a previously sent text Msg.	Internet	TCP/IP	Tendril - Aligns with SEP 1.0	N/A
18.a.1	DERM	VCMS	Shed Load Command Transfer	DERM sends Shed Load Command to VCMS.	Shed Load Command	This command is used to shed load for one or more EVCSs. The message can specify that either a certain percentage of an EVCS's current power output or the absolute maximum allowable load be shed.	Internet	HTTP(S)	ChargePoint Web Services API	shedLoad
18.a.2	DERM	VCMS	Clear Shed State Command Transfer	DERM sends Clear Shed State Command to VCMS.	Clear Shed State Command	This command is used to clear the shed state from one or more EVCSs.	Internet	HTTP(S)	ChargePoint Web Services API	clearShedState
19.a.1	VCMS	EVCS	Shed Load Command Transfer	VCMS sends Shed Load Command to EVCS.	Shed Load Command	This command is used to shed load for a specific EVCS. The message can specify that either a certain percentage of the EVCS's current power output or the absolute maximum allowable load be shed.	Hosted Cellular Network	OCPP	N/A	N/A

Msg ID	Producer (Actor 1)	Receiver (Actor 2)	Name of Process/Transaction	Description of Process/Transaction	Information Object Name	Information Object Description	Transport Method	Network Protocols	Interface Standard	Standard Msg Name
19.a.2	VCMS	EVCS	Clear Shed State Command Transfer	VCMS sends Clear Shed State Command to EVCS.	Clear Shed State Command	This command is used to clear the shed state from a specific EVCS.	Hosted Cellular Network	OCPP	N/A	N/A
21.a.1	DDC	Substation DAD	DAD Status Request Transfer	DDC sends DAD Status Request to a Substation DAD via SDPN	DAD Status Request	A Msg sent from DAC to DDC and a Substation DAD containing a request for the configuration settings of the Substation DAD.	SDPN	MMS	IEC 61850	Various
21.a.2	DDC	Substation DAD	Circuit Reconfiguration Transfer	DDC sends Circuit Reconfiguration to a Substation DAD via SDPN	Circuit Reconfiguration	A command sent from DAC to a Substation DAD containing the configuration settings of the Substation DAD.	SDPN	MMS	IEC 61850	Various
21.a.3	DDC	Substation DAD	DAD Status Request Transfer	DDC sends DAD Status Request to all Substation DADs within the area of control via SDPN	DAD Status Request	Monitor request sent by DCADA to one or more Substation DADs to determine optimal system parameters.	SDPN	MMS	IEC 61850	Various
21.a.4	DDC	Substation DAD	DAD Control Signal Transfer	DDC sends DAD Control Signal to all relevant Substation DADs via SDPN	DAD Control Signal	Updated configuration settings for one or more Substation DADs as determined by VVC.	SDPN	MMS	IEC 61850	Various
21.a.5	DDC	Substation DAD	DAD Control Signal Transfer	DDC sends DAD Control Signal to a Substation DAD via SDPN to initiate load reduction	Substation DAD Control Signal	Configuration settings for a Substation DAD sent from DCADA to the Substation DAD.	SDPN	MMS	IEC 61850	Various
21.b.1	Substation DAD	DDC	Fault Detected Msg Transfer	Substation DAD sends Fault Detected Msg to DDC via SDPN	Fault Detected Msg	A signal sent to DAC from a Substation DAD indicating the Substation DAD has detected a fault.	SDPN	MMS	IEC 61850	Various
21.b.2	Substation DAD	DDC	DAD Status Response Transfer	Substation DAD sends DAD Status Response to DDC via SDPN	DAD Status Response	A Msg sent from a Substation DAD to DDC containing the configuration settings of the DAD.	SDPN	MMS	IEC 61850	Various
21.b.3	Substation DAD	DDC	Recloser Open and Fault Detected Msg Transfer	RECL sends Recloser Open and Fault Detected Msg to DDC via SDPN	Recloser Open & Fault Detected Msg	A signal sent to DAC from a Substation DAD indicating the Recloser is open due to a fault that has occurred.	SDPN	MMS	IEC 61850	Various
21.b.4	Substation DAD	DDC	DAD Status Update Transfer	Substation DAD sends DAD Status Update to DDC via SDPN	DAD Status Update	A Msg sent from a Substation DAD to DAC containing the configuration settings of the Substation DAD.	SDPN	MMS	IEC 61850	Various
21.b.5	Substation DAD	DDC	Lock-Out Signal Transfer	Substation DAD sends Lock-Out Signal to DDC via SDPN	Lock-Out Signal	A signal sent to DAC from a Substation DAD indicating the CBR is locked due to the fault.	SDPN	MMS	IEC 61850	Various
21.b.6	Substation DAD	DDC	DAD Status Response Transfer	Substation DAD sends DAD Status Response to DDC via SDPN	DAD Status Response	Response from a Substation DAD to DCADA that DAD Status has been sent.	SDPN	MMS	IEC 61850	Various
21.b.7	Substation DAD	DDC	DAD Alarm Report	Substation DAD sends DAD Alarm to DDC via SDPN	Substation DAD Alarm	An alarm Msg sent from a Substation DAD to DCADA to report an alert condition that has occurred at the Substation DAD.	SDPN	MMS	IEC 61850	Various
21.b.8	Substation DAD	DDC	DAD Status Report	Substation DAD sends DAD Status Update to DDC via SDPN	Substation DAD Status	A Msg containing DAD status sent from a Substation DAD to DCADA.	SDPN	MMS	IEC 61850	Various
22.a.1	D-SCADA	DDC	DAD Status Request Transfer	D-SCADA begins Fault Isolation Calculation by sending DAD Status Request to DDC	DAD Status Request	A Msg sent from D-SCADA to DDC & a DAD containing a request for the configuration settings of a DAD.	Backhaul WAN	MMS	IEC 61850	Various
22.a.2	D-SCADA	DDC	Circuit Reconfiguration Transfer	D-SCADA sends Circuit Reconfiguration Command to DDC	Circuit Reconfiguration	A command sent from D-SCADA to DDC containing the configuration settings of a DAD.	Backhaul WAN	MMS	IEC 61850	Various
22.a.3	D-SCADA	DDC	DAD Status Request Transfer	D-SCADA sends a DAD Status Request to DDC	DAD Status Request	Monitor request sent by D-SCADA to DDC to determine optimal system parameters.	Backhaul WAN	MMS	IEC 61850	Various
22.a.4	D-SCADA	DDC	DAD Control Signal Transfer	D-SCADA creates and sends a DAD Control Signal to DDC	DAD Control Signal	Updated configuration settings for a Substation or Field DAD as determined by VVC.	Backhaul WAN	MMS	IEC 61850	Various
22.a.5	D-SCADA	DDC	DAD Control Signal Transfer	D-SCADA sends DAD Control Signal to DDC	DAD Control Signal	Configuration settings for a Substation or Field DAD sent from D-SCADA to DDC.	Backhaul WAN	MMS	IEC 61850	Various
22.a.6	D-SCADA	DDC	DAD Control Signal Transfer	D-SCADA sends DAD Control Signal to DDC	Field DAD Control Signal	Configuration settings for a Field DAD sent from D-SCADA to DDC.	Backhaul WAN	MMS	IEC 61850	Various
22.b.1	DDC	D-SCADA	Fault Detected Msg Transfer	DDC sends Fault Detected Msg to D-SCADA	Fault Detected Msg	A signal sent to D-SCADA from DDC indicating a DAD has detected a fault.	Backhaul WAN	MMS	IEC 61850	Various
22.b.2	DDC	D-SCADA	DAD Status Response Transfer	DDC sends DAD Status Response to D-SCADA	DAD Status Response	A Msg sent from DDC to D-SCADA containing the configuration settings of a DAD.	Backhaul WAN	MMS	IEC 61850	Various
22.b.3	DDC	D-SCADA	Recloser Open and Fault Detected Msg Transfer	DDC sends Recloser Open and Fault Detected Msg to D-SCADA	Recloser Open & Fault Detected Msg	A signal sent to D-SCADA from DDC indicating a Recloser is open due to a fault that has occurred.	Backhaul WAN	MMS	IEC 61850	Various
22.b.4	DDC	D-SCADA	DAD Status Update Transfer	DDC sends DAD Status Update to D-SCADA	DAD Status Update	A Msg sent from DDC to D-SCADA containing the configuration settings of a DAD.	Backhaul WAN	MMS	IEC 61850	Various
22.b.5	DDC	D-SCADA	Lock-Out Signal Transfer	DDC sends Lock-Out Signal to D-SCADA	Lock-Out Signal	A signal sent to D-SCADA from DDC indicating a CBR is locked due to the fault.	Backhaul WAN	MMS	IEC 61850	Various
22.b.6	DDC	D-SCADA	DAD Status Response Transfer	DDC sends DAD Status Response to D-SCADA	DAD Status Response	Response from DDC to D-SCADA that a DAD Status has been sent.	Backhaul WAN	MMS	IEC 61850	Various
22.b.7	DDC	D-SCADA	DAD Alarm Transfer	DDC sends DAD Alarm to D-SCADA	Substation DAD Alarm	An alarm Msg sent from DDC to D-SCADA to report an alert condition that has occurred at a Substation DAD.	Backhaul WAN	MMS	IEC 61850	Various
22.b.8	DDC	D-SCADA	DAD Alarm Transfer	DDC sends DAD Alarm to D-SCADA	Field DAD Alarm	An alarm Msg sent from DDC to D-SCADA to report an alert condition that has occurred at a Field DAD.	Backhaul WAN	MMS	IEC 61850	Various
22.b.9	DDC	D-SCADA	DAD Status Transfer	DDC sends DAD Status Update to D-SCADA	Substation DAD Status	A Msg containing a Substation DAD status sent from DDC to D-SCADA.	Backhaul WAN	MMS	IEC 61850	Various
22.b.10	DDC	D-SCADA	DAD Status Transfer	DDC sends DAD Status Update to D-SCADA	Field DAD Status	A Msg containing a Field DAD status sent from DDC to D-SCADA.	Backhaul WAN	MMS	IEC 61850	Various
23.a.1	AHE	DERM	Meter Interval and Register Reads Transfer	AHE sends Meter Interval and Register Reads to DERM.	Meter Interval and Register Reads	The file contains day-behind meter reads (interval and register).	Private Connection	SFTP	CMEP	N/A
24.a.1	DAC	DDC	DAD Status Request Transfer	DAC begins Fault Isolation Calculation by sending DAD Status Request to DDC	DAD Status Request	A Msg sent from DAC to DDC & a DAD containing a request for the configuration settings of the DAD.	SDAN	MMS	IEC 61850	Various

Msg ID	Producer (Actor 1)	Receiver (Actor 2)	Name of Process/Transaction	Description of Process/Transaction	Information Object Name	Information Object Description	Transport Method	Network Protocols	Interface Standard	Standard Msg Name
24.a.2	DAC	DDC	Circuit Reconfiguration Transfer	DAC sends Circuit Reconfiguration Command to DDC	Circuit Reconfiguration	A command sent from DAC to a DAD containing the configuration settings of the DAD.	SDAN	MMS	IEC 61850	Various
24.a.3	DAC	DDC	DAD Status Request Transfer	DCADA sends a DAD Status Request to DDC	DAD Status Request	Monitor request sent by DCADA to a DAD to determine optimal system parameters.	SDAN	MMS	IEC 61850	Various
24.a.4	DAC	DDC	DAD Control Signal Transfer	DAC creates and sends a DAD Control Signal to DDC	DAD Control Signal	Updated configuration settings for a Substation or Field DAD as determined by VVC.	SDAN	MMS	IEC 61850	Various
24.a.5	DAC	DDC	DAD Control Signal Transfer	DAC sends DAD Control Signal to DDC	DAD Control Signal	Configuration settings for a Substation or Field DAD sent from DCADA to a Substation DAD.	SDAN	MMS	IEC 61850	Various
24.a.6	DAC	DDC	DAD Control Signal Transfer	DAC sends DAD Control Signal to DDC	Field DAD Control Signal	Configuration settings for a Field DAD sent from DCADA to a Field DAD.	SDAN	MMS	IEC 61850	Various
24.b.1	DDC	DAC	Fault Detected Msg Transfer	DDC sends Fault Detected Msg to DAC	Fault Detected Msg	A signal sent to DAC from a DAD indicating the DAD has detected a fault.	SDAN	MMS	IEC 61850	Various
24.b.2	DDC	DAC	DAD Status Response Transfer	DDC sends DAD Status Response to DAC	DAD Status Response	A Msg sent from a DAD to DAC containing the configuration settings of the DAD.	SDAN	MMS	IEC 61850	Various
24.b.3	DDC	DAC	Recloser Open and Fault Detected Msg Transfer	DDC sends Recloser Open and Fault Detected Msg to DAC	Recloser Open & Fault Detected Msg	A signal sent to DAC from a DAD indicating the Recloser is open due to a fault that has occurred.	SDAN	MMS	IEC 61850	Various
24.b.4	DDC	DAC	DAD Status Update Transfer	DDC sends DAD Status Update to DAC	DAD Status Update	A Msg sent from a DAD to DAC containing the configuration settings of the DAD.	SDAN	MMS	IEC 61850	Various
24.b.5	DDC	DAC	Lock-Out Signal Transfer	DDC sends Lock-Out Signal to DAC	Lock-Out Signal	A signal sent to DAC from a DAD indicating the CBR is locked due to the fault.	SDAN	MMS	IEC 61850	Various
24.b.6	DDC	DAC	DAD Status Response Transfer	DDC sends DAD Status Response to DAC	DAD Status Response	Response from DAD to DCADA that DAD Status has been sent.	SDAN	MMS	IEC 61850	Various
24.b.7	DDC	DAC	DAD Alarm Transfer	DDC sends DAD Alarm to DAC	Substation DAD Alarm	An alarm Msg sent from a Substation DAD to DCADA to report an alert condition that has occurred at the DAD.	SDAN	MMS	IEC 61850	Various
24.b.8	DDC	DAC	DAD Alarm Transfer	DDC sends DAD Alarm to DAC	Field DAD Alarm	An alarm Msg sent from a Field DAD to DCADA to report an alert condition that has occurred at the DAD.	SDAN	MMS	IEC 61850	Various
24.b.9	DDC	DAC	DAD Status Transfer	DDC sends DAD Status Update to DAC	Substation DAD Status	A Msg containing DAD status sent from a Substation DAD to DCADA.	SDAN	MMS	IEC 61850	Various
24.b.10	DDC	DAC	DAD Status Transfer	DDC sends DAD Status Update to DAC	Field DAD Status	A Msg containing DAD status sent from a Field DAD to DCADA.	SDAN	MMS	IEC 61850	Various
25.a.4	HEMP	AHE	HAND Info Request Transfer	HEMP sends HAND Info Request to AHE via ESB	HAND Info Request	Request from HEMP (or other Utility back-office system) to AHE for HAND information.	ESB	HTTP(S)	IEC 61968-9	GET(HANDeviceAssets)
25.a.8	HEMP	AHE	DR Event Msg Transfer	HEMP sends DR Event Msg Transfer to AHE	DR Event Msg	Msg from HEMP to AHE that contains the load curtailment details for a specific MTR. Details are based upon the type of DR event and user defined preferences in the HEMP.	ESB	HTTP(S)	IEC 61968-9	CREATE(HANDeviceControls)
25.b.5	AHE	HEMP	HAND Info Response Transfer	AHE sends HAND Info Response to HEMP via ESB	HAND Info Response	Response from AHE to HEMP (or originating Utility back-office system) containing HAND information. Response includes MAC Address, Device Type, Installation Code, Installation Date and Pair ID.	ESB	HTTP(S)	IEC 61968-9	REPLY(HANDeviceAssets)
25.b.9	AHE	HEMP	DR Event Received Acknowledgement Transfer	AHE sends DR Event Received Acknowledgement to HEMP via ESB	DR Event Received Acknowledgement	Response Msg from AHE to HEMP indicating that the demand response event has been scheduled at the PCT.	ESB	HTTP(S)	IEC 61968-9	CREATED(HANDeviceEvents)
25.b.14	AHE	HEMP	Meter Interval and Register Reads Transfer	AHE sends Meter Interval and Register Reads to HEMP via Legacy MQ.	Meter Interval and Register Reads	The file contains day-behind meter reads (interval and register). Legacy MQ process used to re-format the file received from AHE (converted each meters' interval reads to register reads) before being sent to HEMP.	Legacy MQ	SFTP	N/A	N/A
26.a.1	RTAC	DDC	Grid-Connected DER Status Update Transfer	RTAC sends Grid-Connected DER Status Update to DDC via DAN.	Grid-Connected DER Status Update	The message will contain the current value for either a digital or analog status point that is associated with the Grid-Connected DER. Depending on the point, the message is trigged by any change in value or by the defined polling period configured in DDC.	DAN	DNP3	IEEE 1815	Various
26.b.1	DDC	RTAC	Grid-Connected DER Control Signal Transfer	DDC sends Grid-Connected DER Control Signal to RTAC via DAN.	Grid-Connected DER Control Signal	The message will contain the desired value for either a digital or analog control point that is associated with the Grid-Connected DER. The message is triggered anytime the DDC receives a Grid-Connected DER Control Signal from the upstream system (D-SCADA).	DAN	DNP3	IEEE 1815	Various
29.a.1	ALINK	HEMP	Single Sign-On Authentication Assertion Response Transfer	Customer logged into ALNK portal clicks on button to navigate to HEMP. After HEMP sends Assertion Request to ALNK, ALNK sends Assertion Response to HEMP to finish Single Sign-On process.	Single Sign-On Authentication Assertion Response	Only Customers that are enrolled in HEMP program can see button from their ALNK session. Customers aren't allowed access to the HEMP until ALNK sends the Assertion Response to HEMP.	Internet	TCP/IP	SAML	N/A
29.b.1	HEMP	ALINK	Single Sign-On Authentication Assertion Request Transfer	After Customer navigates to HEMP, HEMP sends Assertion Request to ALNK to verify Customer already has an active ALNK session.	Single Sign-On Authentication Assertion Request	Customers aren't allowed access to the HEMP until ALNK responds to the Assertion Request sent by ALNK.	Internet	TCP/IP	SAML	N/A
30.a.1	CIS	GIS	Customer Status Transfer	CIS sends current Customer Status Data to GIS via the Back Office Network.	Customer Status Data	A shadow database containing the current status for each customer is extracted from CIS and sent to GIS to synchronize all of the customers on each Point of Service in GIS. This database includes Service Point ID, Point of Service, and Transformer for each customer.	Back Office Network	SFTP	N/A	N/A

Msg ID	Producer (Actor 1)	Receiver (Actor 2)	Name of Process/Transaction	Description of Process/Transaction	Information Object Name	Information Object Description	Transport Method	Network Protocols	Interface Standard	Standard Msg Name
30.b.1	GIS	CIS	Customer Connectivity Status Change Transfer	GIS sends current Customer Connectivity Data to CIS via the Back Office Network. A portion of this process involves manual interaction.	Customer Connectivity Data	Current mapping between Service Point ID, Point of Service, and Transformer is retrieved from GIS and sent to CIS via a daily batch process. This data ensures CIS stays in sync with GIS after a customer is added to a Point of Service, removed from a Point of Service, or moved to a different Point of Service.	Back Office Network	SFTP	N/A	N/A
31.a.1	CIS	HEMP	Customer Account Information Transfer	CIS sends Customer Account Information to HEMP.	Customer Account Information	This information includes customers' enrollment status, rates, and daily price true-ups.	Private Connection	SFTP	N/A	N/A
32.a.1	CIS	DERM	Customer Status Transfer	CIS sends current Customer Status Data to DERM.	Customer Status Data	A shadow database containing the the current status for each customer is extracted from CIS and sent to DERM. This database includes Service Point ID, Point of Service, and Transformer for each customer.	Private Connection	SFTP	N/A	N/A
34.a.1	EVCS	PEV	Internal Process Communication from EVCS to PEV	These messages are used for internal application logic to enable the EVCS to safely charge a PEV at the proper rate.	Internal Process Data	This data is used for internal application logic for a given EVCS to charge a PEV.	SAE J1772 Level II Connector	SAE J1772	SAE J1772	N/A
34.b.1	PEV	EVCS	Internal Process Communication from PEV to EVCS	These messages are used for internal application logic to enable the EVCS to safely charge a PEV at the proper rate.	Internal Process Data	This data is used for internal application logic for a given EVCS to charge a PEV.	SAE J1772 Level II Connector	SAE J1772	SAE J1772	N/A
36.a.1	DAC	DAC	Internal Process Communication	These messages are used for internal processes.	Internal Process Data	This data is used for internal control processes.	DAC Internal	Siemens Proprietary	N/A	N/A
37.a.1	CIS	OMS (DMS)	Customer Status Transfer	CIS sends current Customer Status Data to OMS (DMS sub-system) via the Back Office Network.	Customer Status Data	A shadow database containing the the current status for each customer is extracted from CIS and sent to OMS on a weekly basis. This database includes Service Point ID, Point of Service, and Transformer for each customer.	Back Office Network	SFTP	N/A	N/A
40.a.1	AHE	DMAT	Meter Interval and Register Reads Transfer	AHE sends Meter Interval and Register Reads to DMAT.	Meter Interval and Register Reads	The files contain day-behind meter reads (interval and register).	Private Connection & Internet	SFTP	N/A	N/A
50.a.1	MFR	MMB	On-Demand Meter Read Request Transfer	MFR sends On-Demand Meter Read Request to MMB	On-Demand Meter Read Request	Request from AHE to MMB's internal reading table for current meter usage data.	Meter Internal	L+G Proprietary	L+G Proprietary	Command(OnDemandRead)
50.a.2	MFR	MMB	Gap-Filling Meter Read Request Transfer	MFR sends Gap-Filling Meter Read Request to MMB	Gap-Filling Meter Read Request	Request from AHE to MMB for a specific set of interval and/or register MTR data.	Meter Internal	L+G Proprietary	L+G Proprietary	GET(MeterReading)
50.a.3	MFR	MMB	On-Demand Meter Status Request Transfer	MFR sends On-Demand Meter Status Request to MMB	On-Demand Meter Status Request	Request from AHE to MMB's internal reading table for current meter reading data. This data is used to determine meter status.	Meter Internal	L+G Proprietary	L+G Proprietary	Command(OnDemandRead)
50.a.5	MFR	MMB	MTR Configuration Update Transfer	MFR sends MTR Configuration Update to MMB	MTR Configuration Update	Msg from AHE to MMB that contains a modification to the MTR Configuration.	Meter Internal	L+G Proprietary	L+G Proprietary	N/A
50.a.6	MFR	MMB	MMB Firmware Update Transfer	MFR sends MMB Firmware Update to MMB	MMB Firmware Update	Msg from AHE to MMB that contains a new version of firmware.	Meter Internal	L+G Proprietary	L+G Proprietary	N/A
50.b.1	MMB	MFR	On-Demand Meter Read Data Transfer	MMB sends On-Demand Meter Read Data to MFR	On-Demand Meter Read Data	Current meter usage data retrieved from MMB's internal reading table and sent to AHE.	Meter Internal	L+G Proprietary	L+G Proprietary	Response(Readings)
50.b.2	MMB	MFR	Interval Meter Read Data Transfer	MMB sends Interval Meter Read Data to MFR	Interval Meter Read Data	ANSI C12.19 formatted interval usage data generated and stored in the MMB's reading table and sent to MFR.	Meter Internal	L+G Proprietary	L+G Proprietary	IntervalReadings
50.b.3	MMB	MFR	Register Meter Read Data Transfer	MMB sends Register Meter Read Data to MFR	Register Meter Read Data	ANSI C12.19 formatted total daily usage reading generated and stored in the MMB's register and sent to MFR.	Meter Internal	L+G Proprietary	L+G Proprietary	RegisterReadings
50.b.4	MMB	MFR	Advisory Event Msg Transfer	ESI, MMB, or MFR sends Advisory Event Msg to MFR	Advisory Event Msg	Msg generated in a MTR sub-device and sent to the MFR. Contains any MTR events defined as "advisory".	Meter Internal	L+G Proprietary	L+G Proprietary	Various. See AMI-06 for details.
50.b.5	MMB	MFR	Log Only Event Msg Transfer	ESI, MMB, or MFR sends Log Only Event Msg to MFR	Log Only Event Msg	Msg generated in a MTR sub-device and sent to the MFR. Contains any MTR events defined as "log only".	Meter Internal	L+G Proprietary	L+G Proprietary	Various. See AMI-07 for details.
50.b.6	MMB	MFR	Alarm Event Msg Transfer	ESI, MMB, or MFR sends Alarm Event Msg to MFR	Alarm Event Msg	Msg generated in a MTR sub-device and sent to the MFR. Contains any MTR events defined as "alarm".	Meter Internal	L+G Proprietary	L+G Proprietary	Various. See AMI-05 for details.
50.b.7	MMB	MFR	On-Demand Meter Status Response Transfer	MMB sends On-Demand Meter Status Response to MFR	On-Demand Meter Status Response	Current meter reading data retrieved from MMB's internal reading table and sent to AHE. This data is used to determine meter status.	Meter Internal	L+G Proprietary	L+G Proprietary	Response(Readings)
50.b.9	MMB	MFR	MTR Configuration Update Confirmation Transfer	MMB sends MTR Configuration Update Confirmation to MFR	MTR Configuration Update Confirmation	Response Msg from MMB to AHE to confirm that MTR Configuration Update was made successfully.	Meter Internal	L+G Proprietary	L+G Proprietary	N/A
50.b.10	MMB	MFR	MMB Firmware Update Confirmation Transfer	MMB sends MMB Firmware Update Confirmation to MFR	MMB Firmware Update Confirmation	Response Msg from MMB to AHE to confirm that firmware update was installed successfully.	Meter Internal	L+G Proprietary	L+G Proprietary	N/A
50.b.11	MMB	MFR	Gap-Filling Meter Read Data Transfer	MMB sends Gap-Filling Meter Read Data to MFR	Gap-Filling Meter Read Data	Interval and/or register MTR data for a specific period of time that is retrieved from MMB and sent to AHE.	Meter Internal	L+G Proprietary	L+G Proprietary	REPLY(MeterReadings)
50.f.1	MFR	ESI	Commission HAN Command Transfer	MFR sends Commission HAN Command to ESI	Commission HAN Command	Command from the AHE to the MTR to turn on the ESI and enable the UHAN.	Meter Internal	L+G Proprietary	L+G Proprietary	Command(CommissionHAN)
50.f.2	MFR	ESI	Provision HAND Command Transfer	MFR sends Provision HAND Command to ESI	Provision HAND Command	Request from AHE to MTR for HAND provisioning. Contains Meter ID, HAND MAC Address and HAND Install Code, and Allow Joining duration.	Meter Internal	L+G Proprietary	L+G - Aligns with SEP 1.0	Command(ProvisionHANDevice)

Msg ID	Producer (Actor 1)	Receiver (Actor 2)	Name of Process/Transaction	Description of Process/Transaction	Information Object Name	Information Object Description	Transport Method	Network Protocols	Interface Standard	Standard Msg Name
50.f.3	MFR	ESI	Text Msg Transfer	MFR sends Text Msg to ESI	Text Msg	Request from AHE to ESI to send a text Msg to HAND. Contains text Msg, start time, duration and confirmation flag.	Meter Internal	L+G Proprietary	L+G - Aligns with SEP 1.0	Command(HANMsg)
50.f.5	MFR	ESI	Pricing Signals Transfer	MFR sends Pricing Signals to ESI	Pricing Signals	Pricing information sent from AHE to ESI. Contains flat, time-of-use, or critical peak pricing.	Meter Internal	L+G Proprietary	L+G - Aligns with SEP 1.0	Command(HANPricing)
50.f.6	MFR	ESI	HAND Pairing Info Request Transfer	MFR sends HAND Pairing Info Request to ESI	HAND Pairing Info Request	Request from AHE to ESI for HAND pairing information.	Meter Internal	L+G Proprietary	L+G - Aligns with SEP 1.0	Command(GetPairingDetails)
50.f.7	MFR	ESI	HAND De-Provision Request Transfer	MFR sends HAND De-Provision Request to ESI	HAND De-Provision Request	Request sent from AHE to ESI for the de-provisioning of a HAND.	Meter Internal	L+G Proprietary	L+G - Aligns with SEP 1.0	Command(DeprovisionHANDevice)
50.f.8	MFR	ESI	UHAN De-Commission Request Transfer	MFR sends UHAN De-Commission Request to ESI	UHAN De-Commission Request	Request from AHE to ESI for de-commissioning of the UHAN.	Meter Internal	L+G Proprietary	L+G Proprietary	Command(DecommissionHAN)
50.f.9	MFR	ESI	DR Event Msg Transfer	MFR sends DR Event Msg to ESI	DR Event Msg	Msg from AHE to ESI, through MFR, that contains the load curtailment details for a specific MTR. Details are based upon the type of DR event and user defined preferences in the HEMP.	Meter Internal	L+G Proprietary	L+G - Aligns with SEP 1.0	Command(LoadControl)
50.f.10	MFR	ESI	ESI Firmware Update Transfer	MFR sends ESI Firmware Update to ESI	ESI Firmware Update	Msg from AHE to ESI that contains a new version of firmware.	Meter Internal	L+G Proprietary	L+G Proprietary	N/A
50.f.11	MFR	ESI	Daily Bill TrueUp Msg Transfer	MFR sends Daily Bill TrueUp Msg to ESI	Daily Bill TrueUp Msg	Tunnel Text Msg from AHE to ESI that contains Daily Bill TrueUp data.	Meter Internal	L+G Proprietary	L+G - Aligns with SEP 1.0	Command(HANMsg)
50.g.1	ESI	MFR	HAN Commissioned Response Transfer	ESI sends HAN Commissioned Response to MFR	HAN Commissioned Response	Response from the ESI to the AHE indicating that the ESI has been enabled and the UHAN has been established. Contains Meter ID and HAN Network ID.	Meter Internal	L+G Proprietary	L+G Proprietary	Response(HANCommissioned)
50.g.2	ESI	MFR	Ready-to-Pair Response Transfer	ESI sends Ready-to-Pair Response to MFR	Ready-to-Pair Response	Response from MTR to AHE indicating UHAN is commissioned and ESI is ready to begin the pairing process.	Meter Internal	L+G Proprietary	L+G - Aligns with SEP 1.0	Response(Ready-to-Pair)
50.g.3	ESI	MFR	Provision Complete Response Transfer	ESI sends Provision Complete Response to MFR	Provision Complete Response	Response from MTR to AHE indicating that HAND has been provisioned to ESI.	Meter Internal	L+G Proprietary	L+G - Aligns with SEP 1.0	Response(PairingComplete)
50.g.4	ESI	MFR	Advisory Event Msg Transfer	ESI, MMB, or MFR sends Alarm Event Msg to MFR	Advisory Event Msg	Msg generated in a MTR sub-device and sent to the MFR. Contains any MTR events defined as “advisory”.	Meter Internal	L+G Proprietary	L+G Proprietary	Various. See AMI-06 for details.
50.g.5	ESI	MFR	Log Only Event Msg Transfer	ESI, MMB, or MFR sends Log Only Event Msg to MFR	Log Only Event Msg	Msg generated in a MTR sub-device and sent to the MFR. Contains any MTR events defined as “log only”.	Meter Internal	L+G Proprietary	L+G Proprietary	Various. See AMI-07 for details.
50.g.6	ESI	MFR	Alarm Event Msg Transfer	ESI, MMB, or MFR sends Alarm Event Msg to MFR	Alarm Event Msg	Msg generated in a MTR sub-device and sent to the MFR. Contains any MTR events defined as “alarm”.	Meter Internal	L+G Proprietary	L+G Proprietary	Various. See AMI-05 for details.
50.g.7	ESI	MFR	Text Msg Response Transfer	ESI sends Text Msg Respone to MFR	Text Msg Response	Confirmation from ESI to AHE that CUST acknowledged receipt of text Msg. Requirement for this Msg is controlled by the Text Msg.	Meter Internal	L+G Proprietary	L+G - Aligns with SEP 1.0	Response (TextMsgCreated)
50.g.9	ESI	MFR	Pricing Signals Acknowledgement Transfer	ESI sends Pricing Signals Acknowledgement to MFR	Pricing Signals Acknowledgement	Acknowledgement from ESI to AHE that Pricing Signals were received. Requirement for this Msg is controlled by the Pricing Signals.	Meter Internal	L+G Proprietary	L+G - Aligns with SEP 1.0	Response(HANPricing)
50.g.10	ESI	MFR	HAND Pairing Info Response Transfer	ESI sends HAND Pairing Info Response to MFR	HAND Pairing Info Response	Response from ESI to AHE containing HAND pairing information. Response includes MAC Address, Device Type and Pair ID.	Meter Internal	L+G Proprietary	L+G - Aligns with SEP 1.0	Response(PairingDetails)
50.g.11	ESI	MFR	HAND De-Provision Confirmation Transfer	ESI sends HAND De-Provision Confirmation to MFR	HAND De-Provision Confirmation	Confirmation from ESI to AHE that the HAND has been de-provisioned.	Meter Internal	L+G Proprietary	L+G - Aligns with SEP 1.0	Response(HANDeviceDeprovisioned)
50.g.12	ESI	MFR	UHAN De-Commission Confirmation Transfer	ESI sends UHAN De-Commission Confirmation to MFR	UHAN De-Commission Confirmation	Response from ESI to AHE confirming that the UHAN has been de-commissioned.	Meter Internal	L+G Proprietary	L+G Proprietary	Response(HANDecommissioned)
50.g.13	ESI	MFR	DR Event Received Acknowledgement Transfer	ESI sends DR Event Received Acknowledgement to MFR	DR Event Received Acknowledgement	Response Msg from ESI to AHE, through MFR, indicating that the demand response event has been scheduled at the PCT.	Meter Internal	L+G Proprietary	L+G - Aligns with SEP 1.0	Response(LoadControl)
50.g.14	ESI	MFR	ESI Firmware Update Confirmation Transfer	ESI sends ESI Firmware Update Confirmation to MFR	ESI Firmware Update Confirmation	Response Msg from ESI to AHE to confirm that firmware update was installed successfully.	Meter Internal	L+G Proprietary	L+G Proprietary	N/A
50.g.16	ESI	MFR	DR Event Started Msg Transfer	ESI sends DR Evnet Started Msg to MFR	DR Event Started Msg	Msg from ESI to AHE, through MFR, indicating that the demand response event has started.	Meter Internal	L+G Proprietary	L+G - Aligns with SEP 1.0	Response(LoadControl)
50.g.17	ESI	MFR	DR Event Completed Msg Transfer	ESI sends DR Evnet Completed Msg to MFR	DR Event Completed Msg	Msg from ESI to AHE, through MFR, indicating that the demand response event has ended.	Meter Internal	L+G Proprietary	L+G - Aligns with SEP 1.0	Response(LoadControl)
51.a.1	IPI	CHR	Text Msg Transfer	IPI sends Text Msg to CHR	Text Message	Request from HEMP to CHR to send a text Msg to HAND. Contains text Msg, start time, duration and confirmation flag.	HANG Internal	Tendril Proprietary	Tendril - Aligns with SEP 1.0	N/A
51.a.3	IPI	CHR	HEMP Settings Update Transfer	IPI sends HEMP Settings Update to CHR	HEMP Settings Update	Msg from HEMP to CHR containing changes to the HEMP setings including set point, fan operation and daily/weekly schedule.	HANG Internal	Tendril Proprietary	Tendril - Aligns with SEP 1.0	N/A
51.a.4	IPI	CHR	HEMP Settings Update Transfer	IPI sends HEMP Settings Update to CHR	HEMP Settings Update	Msg from HEMP to CHR containing changes to the HEMP settings. Includes schedule and on/off state.	HANG Internal	Tendril Proprietary	Tendril - Aligns with SEP 1.0	N/A
51.a.5	IPI	CHR	HAND De-Provision Request Transfer	IPI sends HAND De-Provision Request to CHR	HAND De-Provision Request	Request from HEMP to CHR to de-provision a HAND from the HANG.	HANG Internal	Tendril Proprietary	Aligns with ZigBee SEP 1.0	N/A
51.b.1	CHR	IPI	Text Msg Response Transfer	CHR sends Text Msg Response to IPI	Text Msg Response	Confirmation from CHR to HEMP that CUST acknowledged receipt of text Msg. Requirement for this Msg is controlled by the Text Msg.	HANG Internal	Tendril Proprietary	Tendril - Aligns with SEP 1.0	N/A
51.b.4	CHR	IPI	PCT Settings Update Transfer	CHR sends PCT Settings Update to IPI	PCT Settings Update	Msg from CHR to HEMP containing changes to the PCT settings including set point, fan operation and daily/weekly schedule.	HANG Internal	Tendril Proprietary	Tendril - Aligns with SEP 1.0	N/A

Msg ID	Producer (Actor 1)	Receiver (Actor 2)	Name of Process/Transaction	Description of Process/Transaction	Information Object Name	Information Object Description	Transport Method	Network Protocols	Interface Standard	Standard Msg Name
51.b.5	CHR	IPI	HAND De-Provision Confirmation Transfer	CHR sends HAND De-Provision Confirmation to IPI	HAND De-Provision Confirmation	Confirmation from CHR to HEMP that HAND has been de-provisioned from HANG.	HANG Internal	Tendril Proprietary	Aligns with ZigBee SEP 1.0	N/A
52.a.1	ESI	HAND	Text Msg Transfer	ESI sends Text Msg to HAND via UHAN	Text Msg	Request from ESI to HAND to display a text Msg. Contains text Msg, start time, duration and confirmation flag.	UHAN	IEEE 802.15.4	ZigBee SEP 1.0	Display Msg
52.a.3	ESI	HAND	Pricing Signals Transfer	ESI sends Pricing Signals to HAND via UHAN	Pricing Signals	Pricing information sent from ESI to HAND. Contains flat, time-of-use, or critical peak pricing.	UHAN	IEEE 802.15.4	ZigBee SEP 1.0	Publish Price
52.a.4	ESI	HAND	HAND Pairing Info Request Transfer	ESI sends HAND Pairing Info Request to HAND via UHAN	HAND Pairing Info Request	Request from ESI to HAND for HAND pairing information.	UHAN	IEEE 802.15.4	ZigBee SEP 1.0	Device Discovery
52.a.5	ESI	HAND	HAND De-Provision Request Transfer	ESI sends HAND De-Provision Request to HAND via UHAN	HAND De-Provision Request	Request from ESI to HAND for the HAND to leave the UHAN.	UHAN	IEEE 802.15.4	ZigBee SEP 1.0	Leave Command
52.a.6	ESI	PCT	DR Event Msg Transfer	ESI sends DR Event Msg to PCT via UHAN	DR Event Msg	Msg from ESI to PCT that contains the load curtailment details for a specific MTR. Details are based upon the type of DR event and user defined preferences in the HEMP.	UHAN	IEEE 802.15.4	ZigBee SEP 1.0	Load Control Event
52.a.7	ESI	IHD	Daily Bill TrueUp Msg Transfer	ESI sends Daily Bill TrueUp Msg to IHD via UHAN	Daily Bill TrueUp Msg	Tunnel Text Msg from ESI to IHD that contains Daily Bill TrueUp data.	UHAN	IEEE 802.15.4	ZigBee SEP 1.0	Display Msg
52.a.8	ESI	IHD	Real-Time Energy Usage Response Transfer	ESI sends Real-Time Energy Usage Response to IHD via UHAN	Real-Time Energy Usage Response	Response from ESI to IHD containing real-time energy usage.	UHAN	IEEE 802.15.4	ZigBee SEP 1.0	Instantaneous Demand
52.a.9	ESI	IHD	Current Price Response Transfer	ESI sends Current Price Response to IHD via UHAN	Current Price Response	Response from ESI to IHD containing current energy prices.	UHAN	IEEE 802.15.4	ZigBee SEP 1.0	Publish Price
52.a.10	ESI	IHD	Text Msg Response Transfer	ESI sends Text Msg Response to IHD via UHAN	Text Msg Response	Response from ESI to IHD containing the latest utility-generated text Msg.	UHAN	IEEE 802.15.4	ZigBee SEP 1.0	Display Msg
52.a.13	ESI	HAND	ZigBee Command Transfer	ESI sends ZigBee Command to HAND via UHAN	ZigBee Command	Generic ZigBee compliant command originating from either the ESI or a HAND. The destination could be a HAND or the ESI.	UHAN	IEEE 802.15.4	ZigBee SEP 1.0	Various
52.b.1	HAND	ESI	Text Msg Resonse Transfer	HAND sends Text Msg Response to ESI via UHAN	Text Msg Response	Confirmation from HAND to ESI that CUST acknowledged receipt of text Msg. Requirement for this Msg is controlled by the Text Msg.	UHAN	IEEE 802.15.4	ZigBee SEP 1.0	Msg Confirmation
52.b.3	HAND	ESI	Pricing Signals Acknowledgement Transfer	HAND sends Pricing Signals Acknowledgement to ESI via UHAN	Pricing Signals Acknowledgement	Acknowledgement from HAND to ESI that Pricing Signals were received. Requirement for this Msg is controlled by the Pricing Signals.	UHAN	IEEE 802.15.4	ZigBee SEP 1.0	Publish Price Response
52.b.4	HAND	ESI	HAND Pairing Info Response Transfer	HAND sends HAND Pairing Info Response to ESI via UHAN	HAND Pairing Info Response	Response from HAND to ESI containing HAND pairing information. Response includes MAC Address, Device Type and Pair ID.	UHAN	IEEE 802.15.4	ZigBee SEP 1.0	Simple Descriptor Startup Parameters Attribute Set
52.b.5	PCT	ESI	DR Event Received Acknowledgement Transfer	PCT sends DR Event Received Acknowledgement to ESI via UHAN	DR Event Received Acknowledgement	Response from PCT to ESI indicating that the demand response event has been scheduled at the PCT.	UHAN	IEEE 802.15.4	ZigBee SEP 1.0	Report Event Status Command
52.b.6	IHD	ESI	Real-Time Energy Usage Request Transfer	IHD sends Real-Time Energy Usage Request to ESI via UHAN	Real-Time Energy Request	Request from IHD to ESI for real-time energy usage.	UHAN	IEEE 802.15.4	ZigBee SEP 1.0	Instantaneous Demand
52.b.7	IHD	ESI	Current Price Request Transfer	IHD sends Current Price Request to ESI via UHAN	Current Price Request	Request from IHD to ESI for current energy prices.	UHAN	IEEE 802.15.4	ZigBee SEP 1.0	Get Current Price
52.b.8	IHD	ESI	Text Msg Request Transfer	IHD sends Text Msg Request to ESI via UHAN	Text Msg Request	Request from IHD to ESI for latest utility-generated text Msg.	UHAN	IEEE 802.15.4	ZigBee SEP 1.0	Get Last Msg
52.b.10	HAND	ESI	ZigBee Command Transfer	HAND sends ZigBee Command to ESI via UHAN	ZigBee Command	Generic ZigBee compliant command originating from either the ESI or a HAND. The destination could be a HAND or the ESI.	UHAN	IEEE 802.15.4	ZigBee SEP 1.0	Various
52.b.11	PCT	ESI	DR Event Started Msg Transfer	PCT sends DR Event Started Msg to ESI via UHAN	DR Event Started Msg	Msg from PCT to ESI indicating that the demand response event has started.	UHAN	IEEE 802.15.4	ZigBee SEP 1.0	Report Event Status Command
52.b.12	PCT	ESI	DR Event Completed Msg Transfer	PCT sends DR Evnet Completed Msg to ESI via UHAN	DR Event Completed Msg	Msg from PCT to ESI indicating that the demand response event has ended.	UHAN	IEEE 802.15.4	ZigBee SEP 1.0	Report Event Status Command
52.c.1	HAND	HAND	ZigBee Command Transfer	HAND sends ZigBee Command to another HAND via UHAN	ZigBee Command	Generic ZigBee compliant command originating from either the ESI or a HAND. The destination could be a HAND or the ESI.	UHAN	IEEE 802.15.4	ZigBee SEP 1.0	Various
53.a.1	CHR	HAND	Text Msg Transfer	CHR sends Text Msg to HAND via CHAN	Text Msg	Request from CHR to HAND to display a text Msg. Contains text Msg, start time, duration and confirmation flag.	CHAN	IEEE 802.15.4	ZigBee SEP 1.0	Display Msg
53.a.2	CHR	LCS	HEMP Settings Update Transfer	CHR sends HEMP Settings Update to LCS via CHAN	HEMP Settings Update	Msg from CHR to LCS containing changes to the HEMP settings. Includes schedule and on/off state.	CHAN	IEEE 802.15.4	ZigBee SEP 1.0	Demand Response and Load Control Cluster
53.a.3	CHR	HAND	HAND De-Provision Request	CHR sends HAND De-Provision Request to HAND via CHAN	HAND De-Provision Request	Request from CHR to HAND to de-provision a HAND from the HANG.	CHAN	IEEE 802.15.4	ZigBee SEP 1.0	Leave Command
53.a.4	CHR	HAND	ZigBee Command Transfer	CHR sends ZigBee Command to HAND via CHAN	ZigBee Command	Generic ZigBee compliant command originating from either the CHR or a HAND. The destination could be a HAND or the CHR.	CHAN	IEEE 802.15.4	ZigBee SEP 1.0	Various
53.a.6	CHR	PCT	HEMP Settings Update Transfer	CHR sends HEMP Settings Update to PCT via UHAN	HEMP Settings Update	Msg from CHR to PCT containing changes to the HEMP settings including set point, fan operation and daily/weekly schedule.	CHAN	IEEE 802.15.4	ZigBee SEP 1.0	Thermostat Settings Attribute Cluster
53.b.1	HAND	CHR	Text Msg Response Transfer	HAND sends Text Msg Response to CHR via CHAN	Text Msg Response	Confirmation from HAND to CHR that CUST acknowledged receipt of text Msg. Requirement for this Msg is controlled by the Text Msg.	CHAN	IEEE 802.15.4	ZigBee SEP 1.0	Msg Confirmation
53.b.2	HAND	CHR	ZigBee Command Transfer	HAND sends ZigBee Command to CHR via CHAN	ZigBee Command	Generic ZigBee compliant command originating from either the CHR or a HAND. The destination could be a HAND or the CHR.	CHAN	IEEE 802.15.4	ZigBee SEP 1.0	Various

Msg ID	Producer (Actor 1)	Receiver (Actor 2)	Name of Process/Transaction	Description of Process/Transaction	Information Object Name	Information Object Description	Transport Method	Network Protocols	Interface Standard	Standard Msg Name
53.b.4	PCT	CHR	PCT Settings Update Transfer	PCT sends PCT Settings Update to CHR via CHAN	PCT Settings Update	Msg from PCT to CHR containing changes to the PCT settings including set point, fan operation and daily/weekly schedule.	CHAN	IEEE 802.15.5	ZigBee SEP 1.0	Thermostat Settings Attribute Cluster
53.c.1	HAND	HAND	ZigBee Command Transfer	HAND sends ZigBee Command to another HAND via CHAN	ZigBee Command	Generic ZigBee compliant command originating from either the CHR or a HAND. The destination could be a HAND or the CHR.	CHAN	IEEE 802.15.4	ZigBee SEP 1.0	Various
54.a.1	Substation DAD	Substation DAD	GOOSE Broadcast Message Transfer	Feeder Relay (Substation DAD) sends GOOSE Broadcast Message out to all other Substation DADs via SPDN.	GOOSE Broadcast Message	Each GOOSE message broadcasted by a Feeder Relay contains a trip indicator, breaker position, event record indicator, average total load, average sheddable load, and ground fault indicator. The relay sends out a message anytime its status changes and on a 1-second interval otherwise.	SDPN	GOOSE	IEC 61850	Various
54.a.2	Substation DAD	Substation DAD	GOOSE Broadcast Message Transfer	Main Bus Relay (Substation DAD) sends GOOSE Broadcast Message out to all other Substation DADs via SPDN.	GOOSE Broadcast Message	Each GOOSE message broadcasted by a Main Bus Relay contains a trip indicator, breaker position, event record indicator, load shed indicator, feeder shed indicator, load scheme status, and fault indicator. The relay sends out a message anytime its status changes and on a 1-second interval otherwise.	SDPN	GOOSE	IEC 61850	Various
54.a.3	Substation DAD	Substation DAD	GOOSE Broadcast Message Transfer	Bus Tie Relay (Substation DAD) sends GOOSE Broadcast Message out to all other Substation DADs via SPDN.	GOOSE Broadcast Message	Each GOOSE message broadcasted by a Bus Tie Relay contains a trip indicator, breaker position, event record indicator, close-from-main indicator, load values, lockout contacts, and fault indicator. The relay sends out a message anytime its status changes and on a 1-second interval otherwise.	SDPN	GOOSE	IEC 61850	Various
54.a.4	Substation DAD	Substation DAD	GOOSE Broadcast Message Transfer	Bus Differential Relay (Substation DAD) sends GOOSE Broadcast Message out to all other Substation DADs via SPDN.	GOOSE Broadcast Message	Each GOOSE message broadcasted by a Bus Differential Relay contains a trip indicator for each bus feeder, event record indicator, and lockout contact. The relay sends out a message anytime its status changes and on a 1-second interval otherwise.	SDPN	GOOSE	IEC 61850	Various
54.a.5	Substation DAD	Substation DAD	GOOSE Broadcast Message Transfer	Transformer Differential Relay (Substation DAD) sends GOOSE Broadcast Message out to all other Substation DADs via SPDN.	GOOSE Broadcast Message	Each GOOSE message broadcasted by a Transformer Differential Relay contains a trip indicator, breaker position, event record indicator, average available load for both downstream buses, and transformer lockout contact. The relay sends out a message anytime its status changes and on a 1-second interval otherwise.	SDPN	GOOSE	IEC 61850	Various
54.b.1	Substation DAD	Substation DAD	Internal Process Communication	These messages are used for internal application logic to enable a Substation DAD to analyze and/or operate based upon its local protection scheme.	Internal Process Data	This data is used for internal application logic for a given Substation DAD's local protection scheme.	Substation DAD Internal	SEL Proprietary	N/A	N/A
55.a.1	Field DAD	Field DAD	Internal Process Communication	These messages are used for internal application logic to enable a Field DAD to analyze and/or operate based upon its local configuration profile or protection scheme.	Internal Process Data	This data is used for internal application logic for a given Field DAD's local configuration profile or protection scheme.	Field DAD Internal	Proprietary	N/A	N/A
56A.a.1	SMS	RTAC	Grid-Connected DER Status Update Transfer	SMS sends Grid-Connected DER Status Update to RTAC.	Grid-Connected DER Status Update	The message will contain the current value for either a digital or analog status point that is associated with the Grid-Connected DER. Depending on the point, the message is trigged by any change in value or by the defined polling period configured in RTAC.	DER Internal	DNP3	IEEE 1815	Various
56A.b.1	RTAC	SMS	Grid-Connected DER Control Signal Transfer	RTAC sends Grid-Connected DER Control Signal to SMS.	Grid-Connected DER Control Signal	The message will contain the desired value for either a digital or analog control point that is associated with the Grid-Connected DER. The message is triggered anytime the RTAC receives a Grid-Connected DER Control Signal from the upstream system (DDC).	DER Internal	DNP3	IEEE 1815	Various
56B.a.1	DESS	SMS	Grid-Connected DER Status Update Transfer	DESS sends Grid-Connected DER Status Update to SMS.	Grid-Connected DER Status Update	The message will contain the current value for either a digital or analog status point that is associated with the Grid-Connected DER. The message is trigged by any change in value for the status point.	DER Internal	MODBUS	N/A	N/A
56B.b.1	SMS	DESS	Grid-Connected DER Control Signal Transfer	SMS sends Grid-Connected DER Control Signal to DESS.	Grid-Connected DER Control Signal	The message will contain the desired value for either a digital or analog control point that is associated with the Grid-Connected DER. The message is triggered anytime the SMS receives a Grid-Connected DER Control Signal from the upstream system (RTAC).	DER Internal	MODBUS	N/A	N/A
56C.a.1	DESS	DESS	Internal Process Communication	These messages are used for internal processes.	Internal Process Data	This data is used for internal control processes.	DER Internal	Kokam Proprietary	N/A	N/A
58.a.1	Residential DER	Residential DER	Internal Process Communication	These messages are used for internal processes.	Internal Process Data	This data is used for internal control processes.	DER Internal	Sunverge Proprietary	N/A	N/A

Appendix M KCP&L SmartGrid Risk Assessment Master Report

Report on the

KCP&L SmartGrid
Demonstration Project
Risk Assessment

for

Kansas City Power & Light
Kansas City, MO

Project Number 58645

2011

Burns & McDonnell
SINCE 1898

Burns & McDonnell
SINCE 1898

November 18, 2011

Edward T. Hedges, P.E.
Mgr, SmartGrid Technology Planning
Kansas City Power & Light
P.O. Box 418679
Kansas City, MO 64141-9679

KCP&L SmartGrid Demonstration Project - Risk Assessment Report - B&McD Project No. 58645

Dear Mr. Hedges:

We are pleased to submit the final version of the Risk Assessment Report for the KCP&L SmartGrid Demonstration Project.

We based the risk assessment on the guidelines provided by the National Institute of Standards and Technology (NIST) in their Special Publication 800-30: Risk Management Guide for Information Technology Systems. We measured all SmartGrid systems on a common risk model, which covered the following risk components: Threats, Vulnerabilities, Likelihoods, Impacts, and Mitigations. We developed methodologies for each risk component and applied them to each SmartGrid system to assess its risk. The methodologies and their outcomes are detailed in different sections of the report. The report includes the analysis of the applicability (to the KCP&L SmartGrid systems) of the security controls recommended by NIST in their Interagency Report 7628. The report also provides a list of security controls to mitigate risks from these systems.

Our recommendations outline actionable technical and procedural steps towards securing the SmartGrid systems. While developing the recommendations, the risk assessment team was careful to include U.S. Department of Energy and industry suggested best practices. This report is intended to be a guide for the Information Security, WAN Services, Physical Security, IT Strategy & Management, and SmartGrid Project Management Office departments to design a secure KCP&L SmartGrid program.

Sincerely,

Rahul Chhabra
Cyber Security Compliance Consultant

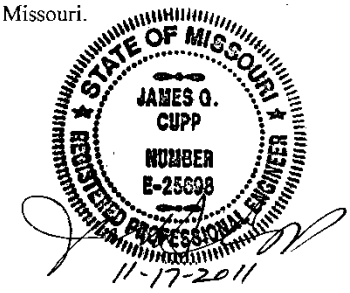
9400 Ward Parkway • Kansas City, MO 64114-3319
Tel: 816 333-9400 • Fax: 816 333-3690 • www.burnsmcd.com

INDEX AND CERTIFICATION

KCP&L SmartGrid Demonstration Project
Risk Assessment Report
Project 58645
Report Index

Certification

I hereby certify, as a Professional Engineer in the state of Missouri, that the information in the document was assembled under my direct personal charge. This report is not intended or represented to be suitable for reuse by Kansas City Power & Light or others without specific verification or adaptation by the Engineer. This certification is made in accordance with the provisions of the laws and rules of the State of Missouri.



James G. Cupp, PE Missouri License # 25698
Date: 11-17-11
(Reproductions are not valid unless signed, dated, and embossed with Engineer's seal)

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Page No.

LIST OF ACRONYMS

ACL	Access Control List
AES	Advanced Encryption Standard
AHE	Advanced Metering Infrastructure Head-End
ALNK	AccountLink
AMI	Advanced Metering Infrastructure
ASIS	American Society for Industrial Security
BMS	Building Management System
CIA	Confidentiality, Integrity, and Availability
CIS	Customer Information System
DAC	Distribution Automation Controller
DAD	Distribution Automation Device
DCADA	Distributed Control and Data Acquisition
DDC	Distribution Data Concentrator
DDoS	Distributed Denial of Service
DER	Distributed Energy Resources
DERM	Distributed Energy Resources Management System
DHS	Department of Homeland Security
DMAT	Data Mining & Analysis Tool
DMS	Distribution Management System
DOE	Department of Energy
DR	Demand Response or Disaster Recovery
EAVF	Ease of Access Vulnerability Factor
EMS	Energy Management System
EVSE	Electric Vehicle Supply Equipment
GIS	Geographic Information System
GUI	Graphical User Interface
HAN	Home Area Network
HAND	Home Area Network Device
HANG	Home Area Network Gateway
HEMP	Home Energy Management Portal
HVAC	Heating, Ventilation, and Air Conditioning
HTTP	Hypertext Transfer Protocol
ICSJWG	Industrial Control Systems Joint Working Group
IEC	International Electrotechnical Commission
IHD	In-Home Display
IP	Internet Protocol
ISA	International Society of Automation
KPI	Key Performance Indicator
L+G	Landis+Gyr
MAC	Media Access Control
MDM	Meter Data Management System
MTR	SmartMeter
MWFM	Mobile Workforce Management System
NERC	North American Electric Reliability Organization
NESCO	National Electric Sector Cybersecurity Organization
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency Report
NIST SP	National Institute of Standards and Technology Special Publication

NVD	National Vulnerability Database
OATI	Open Access Technology International
OMS	Outage Management System
OWASP	Open Web Application Security Project
PEV	Plug-in Electric Vehicle
PII	Personally Identifiable Information
RF	Radio Frequency
RSA	Rivest, Shamir, and Adleman (an algorithm for public key cryptography)
RTO	Regional Transmission Organization
RVR	Relative Vulnerability Rating
SDLC	Software Development Life Cycle
SDT	Standard Drafting Team
SGIP	Smart Grid Interoperability Panel
SGMM	Smart Grid Maturity Model
SIA	Security Industry Association
SME	Subject Matter Expert
SSL	Secure Sockets Layer
SSN	Social Security Number
TEVF	Tech Ease Vulnerability Factor
UCA	Utility Communications Architecture
UCAIug	UCA International Users Group
UTC	Utilities Telecom Council
VEMS	Vehicle Energy Management System
VPN	Virtual Private Network

Executive Summary

Kansas City Power & Light Company (KCP&L) chose to conduct a comprehensive risk assessment of all the systems within their SmartGrid Demonstration Project (hereafter called the "project"). KCP&L made this decision to meet the requirement set forth in both their SmartGrid Cyber Security Plan[1] and the U.S. Department of Energy (DOE) Smart Grid Demonstration funding announcement[2] that states implementing sound cyber security controls for all SmartGrid systems.

According to the KCP&L SmartGrid Cyber Security Plan, the risk assessment performed for the project was primarily based on the guidelines provided in the National Institute of Standards and Technology (NIST) in their Special Publication 800-30 – Risk Management Guide for Information Technology Systems (NIST SP 800-30)[3]. The NIST Interagency Report 7628 Volumes I-III (NISTIR-7628)[4] along with the UCA[5] International Users Group's Advanced Metering Infrastructure and Distribution Management (UCAIug AMI and UCAIug DM) security profiles were also used to conduct the analysis and provide cyber security suggestions for the KCP&L project. Several additional resources were used where applicable. Any references not included in the footnotes throughout the report are provided in Appendix I.

The risk assessment team used a mathematical model to assess the risk of each system. Using a model ensures that an identical method is used to evaluate risk for each system. The model is expressed using the following equation:

$$Risk = Threat + Vulnerability + Likelihood + Impact - Mitigation$$

Separate methodologies were developed to calculate the values of the variables: Threat, Vulnerability, Likelihood, Impact and Mitigation. Each methodology was applied uniformly to all systems to determine values of the risk rating model variables.

---

[1] KCP&L Green Impact Zone SmartGrid Demonstration, *SmartGrid Cyber Security Plan*, Version v1.0 - November 18, 2010
[2] U.S. Department of Energy, National Energy Technology Laboratory, Funding Opportunity Number: DE-FOA-0000036, CFDA Number: 81.122 Electricity Delivery and Energy Reliability Research, Development and Analysis, *Financial Assistance Funding Opportunity Announcement*, June 25, 2009
[3] NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems. http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
[4] National Institute of Standards and Technology Interagency Report 7628. http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf
[5] UCA International Users Group http://www.ucaiug.org/default.aspx
[5] UCA International Users Group (UCAIug) http://www.ucaiug.org/default.aspx

As a prerequisite to the risk assessment, all systems within the KCP&L SmartGrid portfolio were identified along with their respective interfaces. This step formed the boundaries of the scope and created a foundation for the assessment. The resultant scope of the risk assessment was identified to include the following SmartGrid systems:

SmartGrid Systems included in the Risk Assessment	Commonly Referred as:
Advanced Metering Infrastructure Head-End	AHE
AccountLink	ALNK
Building Management System	BMS
Customer Information System	CIS
Distributed Control and Data Acquisition	DCADA
Distributed Energy Resources – Commercial & Industrial	DER – C&I
Distributed Energy Resources – Grid-Connected	DER – Grid-Connected
Distributed Energy Resources Management System	DERM
Distributed Energy Resources – Residential	DER – Residential
Data Mining and Analysis Tool	DMAT
Distribution Management System	DMS
Energy Management System	EMS
Field Distribution Automation Devices	Field DADs
Geographic Information System	GIS
Home Area Network Device	HANDs
Home Area Network Gateway	HANG
Home Energy Management Portal	HEMP
Meter Data Management System	MDM
SmartMeter	MTR
Mobile Workforce Management System	MWFM
Substation Distribution Automation Devices	Substation DADs

Table ES 1 SmartGrid Systems included in the Risk Assessment

The systems that were in the early stages of definition and planning were not included in this assessment. Also excluded were the systems whose integration with the SmartGrid program at the time of assessment was planned but not completely defined. The assessment relied heavily upon analyzing the functionalities of each system and creating a rating for each of the risk components. The exclusions were required so as not to lessen the overall integrity of the results.

Following is the list of systems identified as part of the project that were excluded from the risk assessment:

SmartGrid Systems excluded from the Risk Assessment	Commonly Referred as:
Electric Vehicle Supply Equipment	EVSE
Outage Management System	OMS
Plug-in Electric Vehicle	PEV
Integration with Regional Transmission Organization	RTO
Vehicle Energy Management System	VEMS

Table ES 2 SmartGrid Systems Excluded from the Risk Assessment

For the systems that were included in the scope, several methods were used to develop a deeper understanding of KCP&L's implementation of SmartGrid technologies. These methods included the review of system documents such as use cases, interface diagrams, and vendor software specifications. The interactive methods included focus group interviews with the Subject Matter Experts (SMEs) using a set of targeted questions. The result was a grouping of SmartGrid systems in several business function domains that were later used as one of the criteria to recommend creation of security zones. The collaborative work with the SMEs also resulted in classification of all system interfaces in one of the NIST specified logical interface categories. This classification was later used to determine the security controls that will be required to secure the systems.

In order to assess the value of the Threat variable in the risk model, several internal and external threat sources were identified. The general perception is that a threat source is a malicious computer user with an intention to harm the organization. However this is not completely true. Threat can be defined as the intent and method targeted at the exploitation of a vulnerability, or a situation and method that may accidentally trigger a vulnerability[1]. This assessment also included threats resulting from unintentional acts and natural occurrences. Once the threat sources were identified, a listing of motivations and possible threat actions taken by each threat source was produced. In order to determine threat rating to be used in the risk rating model, each threat source was evaluated to determine if it could impact a given system. A threat rating was thus assigned to each system equating to the count of the number of threat sources identified to pose a risk to that system. The results of the threat determination calculation are shown in the following table on a scale of 0-10.

[1] U.S. Department of Commerce, Computer Security Division, National Institute of Standards and Technology, *Federal Information Processing Standards Publication 200, Minimum Security Requirements for Federal Information and Information Systems*, March 2006

System	Total Number of Potential Threat Sources
AHE	8
ALNK	8
BMS	7
CIS	7
DADs (Field and Substation)	6
DCADA	8
DER – C&I	6
DER – Grid-Connected	6
DERM	6
DER - Residential	6
DMAT	5
DMS	8
EMS	8
GIS	7
HAND/HANG	6
HEMP	7
MDM	8
MTR	8
MWFM	7

Table ES 3 Threat Ratings for the SmartGrid Systems

Vulnerability is defined as the susceptibility of a system to attacks. Numerous vulnerabilities are discovered every week. To evaluate a large program like KCP&L for every potential vulnerability at a single point-in-time is a large undertaking. Furthermore, the validity of vulnerabilities four to six months after the assessment is done is difficult to determine. To overcome these issues, systems were evaluated for the broader categories of vulnerabilities: System and Operational. The system vulnerabilities included were the ones that directly affect one of the three cyber security goals of Confidentiality, Integrity and Availability. The operational vulnerabilities were categorized into People, Policy and Procedural vulnerabilities. To provide a numerical value to the vulnerability of a system, an approach was used to quantify two of the fundamental reasons that make a system vulnerable. The resulting two variables were the relative technical ease of coordinating an attack and the relative ease of access to parts of the system. Table ES 4 lists each system along with the calculated vulnerability rating on a scale of 0-10.

System	Technical Ease	Ease of Access	Vulnerability Rating
AHE	3	3	6
ALNE	4	4	8
BMS	2	3	5
CIS	3	3	6
DCADA	2	3	5
DER – C&I	2	3	5
DER – Grid-Connected	2	3	5
DERM	3	4	7
DER – Residential	3	4	7
DMAT	2	3	5
DMS	2	2	4
EMS	2	2	4
Field DADs	2	3	5
GIS	3	2	5
HAND	4	4	8
HANG	4	4	8
HEMP	4	4	8
MDM	2	3	5
MTR	3	5	8
MWFM	2	2	4
Substation DADs	2	3	5

Table ES 4 Vulnerability Ratings for the SmartGrid Systems

Several measuring criteria were used to assess the *Likelihood* of an attack. These criteria included the evaluation of a potential threat source's motivation and capabilities, as well as the nature and frequency of existing vulnerabilities. The assessment was done to determine the likelihood of an attack, not represent the likelihood of a successful attack. Similar to other risk model components, a rating methodology was developed to assign a likelihood number to all systems. Each threat sources was applied to each system and its likelihood of an attack was given a rating. The highest assigned likelihood rating of a threat source for a system was then used as that system's overall likelihood rating on a scale of 0-10. The results of the likelihood assessment are shown in the following table, Table ES 5.

System	Likelihood Rating
AHE	8
ALNE	10
BMS	4
CIS	8
DADs	6
DCADA	6
DER - C&I	6
DER – Grid-Connected	6
DERM	6
DER - Residential	6
DMAT	6
DMS	8
EMS	10
GIS	6
HAND/HANG	8
HEMP	10
MDM	6
MDR	10
MWFM	6

Table ES 5 Likelihood Ratings for the SmartGrid Systems

Impact can be defined as the effect or influence a successful attack may have on a system and/or the organization. Some of the big impacts include: significant monetary damage, compromised consumer privacy, loss of important business operations for long periods, national-level damage to company reputation and/or years of litigation. For the risk rating model, a quantifying approach was developed to estimate the effects a cyber compromise of confidentiality, integrity, and/or availability will have on the system and the organization. The confidentiality impact was judged based on the qualitative assessment of sensitivity of the data and the effects of a data leak event. The integrity impacts were assessed in terms of cost impacts of fixing an integrity issue. Lastly, the losses due to unavailability of each system were estimated taking into account the loss in productivity. The assessment results in the form of each system's impact rating (on a scale 0-10) are listed in the following table, Table ES 6

System	Confidentiality Impact Level	Integrity Impact Level	Availability Impact Level	Overall Impact Level
ARE	8	8	6	7.33
ALNE	8	6	8	7.33
BMS	4	6	4	4.67
CIS	10	4	10	8.00
DADs (Field & Substation)	4	4	6	4.67
DCADA	4	6	8	6.00
DER – C&I	4	4	4	4.00
DER – Grid-Connected	4	6	4	4.67
DER – Residential	4	6	2	4.00
DERM	8	10	8	7.33
DMAT	6	4	4	4.67
DMS	4	10	10	8.00
EMS	6	10	10	8.67
GIS	4	6	6	5.33
HAND/HANG	6	4	6	5.33
HEMP	8	6	8	7.33
MDM	8	6	6	6.67
MTR	8	6	6	6.67
MWFM	4	6	4	4.67

Table ES 6 Impact Ratings for the SmartGrid Systems

Mitigations are defined as the risk reducing efforts or controls commissioned to moderate the vulnerability, impact, or likelihood of an attack on a system. To assess the mitigations, first the cyber controls suggested by NISTIR-7628 and the UCAIug AMI & DM profiles were studied for their applicability to the KCP&L SmartGrid systems. Once the applicable sets of controls were identified, they were matched with the security controls mandated in the KCP&L policies, standards and processes. A methodology was created to quantify the existing mitigation so that it can be used in the risk rating model. The methodology was based on the assumption that all requirements stated in the KCP&L policies, standards and processes are enforced on all existing and new systems at KCP&L. The results of existing mitigation (with maximum possible rating of 30) are provided in the following table, Table ES 7.

System	Combined Mitigation Rating
AHE	13.00
ALNK	15.36
BMS	8.19
CIS	13.41
DADs (Field & Substation)	9.49
DCADA	10.33
DER – C&I	9.07
DER – Grid-Connected	9.49
DER – Residential	10.14
DERM	12.23
DMAT	9.49
DMS	12.35
EMS	14.51
GIS	9.93
HAND/HANG	12.81
HEMP	15.36
MDM	10.75
MTR	14.94
MWFM	8.96

Table ES 7 Combined Mitigation Ratings for the SmartGrid Systems

The primary purpose for this risk assessment, as stated earlier, was to identify the risk of each SmartGrid system so that KCP&L can strategize its efforts towards securing the project as a whole. The prioritization task becomes less complex with a risk rating available for each system. The final risk rating for each system was calculated using the model.

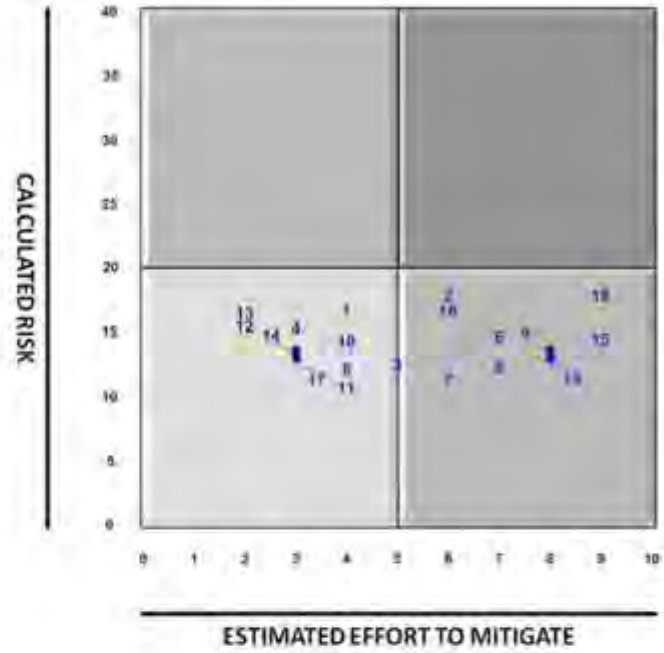
$$R = T + V + L + I - M$$

System ID	System	Threat Rating (T)	Relative Vulnerability Rating (V) ↓	Highest Likelihood Rating (L) ↓	System Impact Rating (I) ↓	Combined Mitigation Rating (M) ↑	Overall Risk Rating (R)
1	AHE	8	6	8	7.33	13.00	**16.34**
2	ALNK	8	8	10	7.33	15.36	**17.97**
3	BMS	7	5	4	4.67	8.19	**12.48**
4	CIS	7	6	8	8.00	13.41	**15.59**
5	DADs (Field & Substation)	6	5	6	4.67	9.49	**12.18**
6	DCADA	8	5	6	6.00	10.33	**14.67**
7	DER - C&I	6	5	6	4.00	9.07	**11.93**
8	DER - Grid-Connected	6	5	6	4.67	9.49	**12.18**
9	DER - Residential	6	7	6	4.00	10.14	**12.86**
10	DERM	6	7	6	7.33	12.23	**14.10**
11	DMAT	5	5	6	4.67	9.49	**11.18**
12	DMS	8	4	8	8.00	12.35	**15.65**
13	EMS	8	4	10	8.67	14.51	**16.15**
14	GIS	7	5	6	5.33	9.91	**13.42**
15	HAND/HANG	6	8	8	5.33	12.81	**14.53**
16	HEMP	7	8	10	7.33	15.36	**16.97**
17	MDM	8	5	6	6.67	10.75	**14.92**
18	MTR	8	8	10	6.67	14.04	**17.72**
19	MWFM	7	4	6	4.67	8.96	**12.71**

Table ES 8 Overall Risk Ratings for the SmartGrid Systems

↓ - Denotes that lowering the component rating will lower the Overall Risk Rating
↑ - Denotes that raising the component rating will lower the Overall Risk Rating

Based on the risk ratings calculated above, the systems were plotted against an estimate of the effort required to further mitigate the threats, likelihoods and impacts. The following figure, Figure ES 1, shows the system IDs plotted against calculated overall risk rating and estimated effort to mitigate.



System ID	System
1	AHE
2	ALNK
3	BMS
4	CIS
5	DADs (Field & Substation)
6	DCADA
7	DER - CAI
8	DER - Grid-Connected
9	DER - Residential
10	DERM
11	DMAT
12	DMS
13	EMS
14	GIS
15	HAND-HANG
16	HEMP
17	MDM
18	MTR
19	MWFM

Figure ES 1 Risk Rating Categories

There is not, nor should there be, an "ideal" level of risk, or a static "target" level of risk at which to aim. These calculated risk ratings should be used to prioritize efforts to reduce overall system risk. Risk may be reduced by mitigations and controls applied at the policy, network, or system level.

There are ten major recommendations given in this report. Some are technical in nature, such as assessing and implementing recommended security controls, or designing and implementing recommended network security zones. Others are more policy- and process-based, such as updating policies and documenting mitigation activities. The following list is an overview of the ten major recommendations:

- Implement the provided sets of security controls in a phased approach.
- Implement the recommended conceptual security zones using network design techniques.
- Create an implementation plan that covers the recommended security controls and security zones.
- Update the KCP&L SmartGrid Cyber Security Plan to maintain focus on security and to meet DOE expectations.

- Create security requirements for all systems to convert the security controls from concept to implementation.
- Develop minimum security requirements for any SmartGrid system externally hosted by a third-party.
- Update KCP&L policies, standards, and/or processes to include protection of SmartGrid systems based upon the provided set of procedural controls.
- Create and execute test cases to verify the placement and functionality of the security controls.
- Perform periodic security assessments to identify and mitigate new risks.
- Participate in working groups to learn and create best practices and standards for securing the grid.

These recommendations cover the entire project, but specifically target the systems evaluated as being the most at risk, or the most impactful, and should be evaluated and considered for inclusion in the project moving forward.

Introduction

The successful demonstration of SmartGrid capabilities at KCP&L includes achieving the three cyber security goals: Confidentiality, Integrity, and Availability (CIA) of the data being processed, stored, and transmitted by the SmartGrid systems. These goals can be attained with a strategic and carefully crafted risk management program. As one of the first steps of a successful risk management program, a good risk assessment provides a realistic risk rating utilizing a uniform, repeatable process and measurable criteria.

To obtain useful risk ratings, the same measurement criteria must be applied consistently for every system without partiality or influence added to any one aspect. In this way, decision makers may be confident that an assessed risk rating is an accurate measure relative to all systems within scope of the risk assessment, and can be used to evaluate and prioritize mitigation actions.

In order to present somewhat subjective criteria in a quantifiable and measurable manner, this assessment utilized a uniform series of evaluation criteria. These criteria were used to evaluate five variables of a risk rating model: Threat Sources, Vulnerabilities, Likelihood, Impact, and Existing Mitigations. The output of each preliminary evaluation was passed through the risk rating model shown below and calculated to produce the final risk rating.

$$Risk = Threat + Vulnerability + Likelihood + Impact - Mitigation$$

$$R = T + V + L + I - M$$

Sections 2.0, 3.0, 4.0, 5.0, and 6.0 of this report describe in detail how the risk assessment team arrived at the values used in the risk rating model. Each of those sections provides evaluation criteria for each SmartGrid system to be input into the risk rating model. Although the assessment used a formula to calculate relative overall risk to each SmartGrid system, it is important to understand that the risk rating model is not necessarily a mathematical problem to be solved. It is merely a template for consistently applying the chosen criteria in order to provide measurable and reliable risk ratings.

In strict mathematical terms, it is evident from the model that increasing mitigations or decreasing threats, vulnerabilities, likelihood, or impact will decrease the level of risk. In other words, a higher mitigation rating lowers a system's risk. Similarly, lowering the threat, vulnerability, likelihood, or impact ratings lowers a system's risk. However in practical terms, mitigations are applied to systems to guard vulnerabilities, decrease the likelihood of an attack, or minimize the overall impact of an attack. The

model also conveys that applying more mitigations will always lead to less risk, but a balance is required to ensure that adding more mitigations does not result in diminishing returns.

In order to properly understand the contents and output of sections 2.0 through 6.0, the criteria and rating systems used to arrive at the variable values for each SmartGrid system must first be understood.

Threat Source (T): The value for T was measured on a scale of 0-10, with 0 being no relevant threats and 10 being all identified threats.

Vulnerabilities (V): The value for V was calculated as an aggregate total of Technical Ease and Ease of Access. Those sub criteria were evaluated and given values between 0-10.

Likelihood (L): The value for L was measured on a scale of 0-10, with 0 being negligible likelihood of a threat source exercising any vulnerability on a system, and 10 being a very high likelihood.

Impact (I): The value for I was measured on a scale of 0-10, with 2 being very low impact to the system if a vulnerability were to be successfully exploited, and 10 being very high impact.

Existing Mitigations (M): The value for M was calculated (with maximum possible rating of 30) based on percentage of proposed security controls believed to be already met by the KCP&L Policies, Standards, and/or Processes, in one of risk model components: V, L, or I.

The risk assessment performed for the KCP&L SmartGrid Demonstration Project is primarily based on the National Institute of Standards and Technology (NIST) specified guidelines in NIST SP 800-30[1]. The evaluations of security controls were performed based on the guidelines presented in the NIST Interagency Report, NISTIR-7628, Volume-1.[2] Assessors used several other federal government and public sources throughout the process and such sources are appropriately cited in the report.

[1] NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems.
http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
[2] National Institute of Standards and Technology Interagency Report 7628.
http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf

A risk assessment provides limited value without a comprehensive plan to address the risks identified. In standard Governance, Risk, and Compliance management, there are four common ways to deal with identified risk: Avoidance, Transference, Mitigation, and Acceptance.

Risk Avoidance: Avoiding risk involves removing vulnerabilities or ceasing the vulnerable or otherwise risky behavior.

Risk Transference: Transference, in this instance, refers to shifting the burden of loss to another party, as in the purchase of an insurance policy.

Risk Mitigation: Mitigating risk is the process of systematically reducing the likelihood or impact of vulnerabilities.

Risk Acceptance: Accepting risk is an informed and conscious decision to accept the consequences and likelihood of a particular vulnerability or risk.

Of the four, Mitigation is by far the most common reaction to identified risks. The term "mitigation" can cover a broad range of actions, including: the creation of policies and procedures, identifying and applying system patches and updates, performing regular backups of critical data, developing robust configuration and change management processes, and any number of similar actions.

The assessment produced a number of additional recommended security controls and other recommendations for consideration. The final sections outline high level plans for prioritizing and implementing those recommendations.

The risk management lifecycle is a continuous loop of evaluating risk, implementing appropriate policies and controls, educating users and promoting risk awareness, and monitoring and evaluating the effectiveness of implemented controls. This risk assessment is the just the first step in the risk management lifecycle for the SmartGrid systems.

1.0 SYSTEM CHARACTERIZATION

The first step for a comprehensive risk assessment is to ensure that all the information system components are clearly identified and the system boundaries are carefully delineated. As evident, the KCP&L SmartGrid Demonstration Project (hereafter called the "project") is a collection of several smart systems that belong to different "Smart Grid Domains", thereby making the project a "system of systems". Thus the activity of accurately identifying the systems and their interfaces is crucial in defining the real boundaries of the project.

1.1 SYSTEM-RELATED INFORMATION

The widely accepted NIST Special Publication 800-30 was used as the guiding document for collecting information and performing the risk assessment for the project. A complete review of the project documentation was performed, which was followed by targeted questionnaires sent to the Subject Matter Experts (SMEs) to lay the foundation of the risk assessment effort. The SMEs' responses were studied and then discussed in focus group interviews. In parallel, the use cases of all the systems were studied and business functions were discussed with the SMEs. The results of the process led to classification of each application into one of the several "Smart Grid Domains"[1]. These domains can be best viewed as logical groupings of systems based on either the similarity of business functions they perform or their implementation. These logical groupings are primarily based on the guidelines provided in the NIST Interagency Report 7628 (commonly referred as the NISTIR-7628). The "Smart Grid Domains" suggested in the NISTIR-7628 are Transmission, Distribution, Operations, Bulk Generation, Markets, Customer, and Service Provider. However, as every implementation of the SmartGrid suite is unique, it is important to take NIST guidelines and tailor them to best fit KCP&L's implementation.

After studying the KCP&L SmartGrid systems, it was determined that the NISTIR-7628 domains would need to be extended to accomplish this. As such the Operations domain was divided to represent two classes of SmartGrid operations: Energy Management and Consumer Management. In addition, it was determined that the Transmission, Bulk Generation, and Markets domains were not applicable to any systems in the project.

[1] Smart Grid Domains are elaborately defined in the National Institute of Standards and Technology Interagency Report 7628. http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf

The following list provides a brief description of the extended SmartGrid domains unique to KCP&L's implementation.

Customer Facing Operations: All systems that aide or perform the business functions of managing energy consumption. These systems can be accessed* either by the consumer or the utility.

Examples: AccountLink (ALNK) and Home Energy Management Portal (HEMP)

*Access – Can be either through a Graphical User Interface (GUI) or a Data Interface.

Utility Operations: All systems contributing towards the supply, control, and management of energy from the utility to the consumer. Access to these systems is limited only to the utility.

Examples: Distribution Management System (DMS) and Customer Information System (CIS)

Field Distribution: The collection of systems that typically reside in the field and provide measurements or asset locations. Access to these systems is limited only to the utility.

Examples: SmartMeter (MTR) and Distributed Control and Data Acquisition (DCADA)

Customer: The collection of systems and devices that reside at the customer location and aide in usage management. These systems can be accessed either by the consumer or the utility.

Examples: Building Management System (BMS), Home Area Network Gateway (HANG), and Home Area Network Devices (HANDs)

Service Provider: The collection of systems that provide aggregation services or third-party analysis to the consumer(s) or the utility. These systems can be accessed either by the consumer, an authorized third-party, or the utility.

Example: Data Mining and Analysis Tool (DMAT)

Table 1-1 lists the classifications of all KCP&L SmartGrid systems according to the extended SmartGrid domains. A brief description of each system is provided in Appendix C.

System	Utility Operations	Customer Facing Operations	Field Distribution	Customer	Service Provider
AHE			X		
ALNR		X			
BMS				X	
CIS	X				
DCADA			X		
DER – C&I				X	
DER – Grid-Connected			X		
DERM	X				
DER – Residential				X	
DMAT					X
DMS	X				
EMS	X				
Field DADs			X		
GIS	X				
HANDs				X	
HANG				X	
HEMP		X			
MDM	X				
MTR			X		
MWFM	X				
Substation DADs			X		

Table 1-1 System Classifications in the Extended Smart Grid Domains

Before threats, vulnerabilities, impacts, likelihood, and risks of each system could be assessed, the next logical step was to classify the communication paths (interfaces) between the SmartGrid systems. The classification of interfaces is necessary, as the security profile and requirements of the grouped interfaces are likely to have a common set of controls. The guidelines provided in NISTIR-7628 Volume-I for "Logical Interface Categories"[10] are extremely helpful in this respect. With aid from KCP&L SMEs, all the known project interfaces were mapped to these Logical Interface Categories. This mapping is shown in Appendix B. The mapping includes the following for each project interface:

- KCP&L interface number
- Systems involved
- Applicable NISTIR-7628 Logical Interface
- Applicable NISTIR-7628 Logical Interface Category and Description

Of the twenty-two NISTIR-7628 Volume-I Logical Interface Categories, thirteen were found to be applicable to the project. This can be seen in the following table, Table 1-2.

[10] National Institute of Standards and Technology Interagency Report 7628. http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf

NISTIR-7628 Logical Interface Category	NISTIR-7628 Logical Interface Category Description
1	Interface between control systems and equipment with high availability, and with compute and/or bandwidth constraints
2	Interface between control systems and equipment without high availability, but with compute and/or bandwidth constraints
3	Interface between control systems and equipment with high availability, without compute nor bandwidth constraints
5	Interface between control systems within the same organization
7	Interface between back office systems under common management authority
8	Interface between back office systems not under common management authority
9	Interface with B2B connections between systems usually involving financial or market transactions
10	Interface between control systems and non-control/corporate systems
11	Interface between sensors and sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analog measurements
13	Interface between systems that use the AMI network
14	Interface between systems that use the AMI network with high availability
15	Interface between systems that use customer (residential, commercial, and industrial) site networks
16	Interface between external systems and the customer site

Table 1-2 Applicable NISTIR-7628 Volume-I Logical Interface Categories

2.0 THREAT IDENTIFICATION

The purpose of this section is to identify the various threats which may pose a risk to the KCP&L SmartGrid Demonstration Project systems, data, or network and communication infrastructure. NIST SP 800-30 defines a threat as:

> *"... the potential for a particular threat source to successfully exercise a particular vulnerability."*[1]

Because a Likelihood value was added to the Risk Rating Model for this assessment, the definition of a threat was modified. For this risk assessment, a threat, by itself, was not presumed to indicate the presence of risk to a system or network. Looking again at the risk calculation model, a threat requires the presence of a system or network vulnerability in order to present any level of risk. As such, only the threat sources that were determined to have the capability to exploit one or more system vulnerabilities were considered in this assessment. A threat can be internal or external, but generally cannot be influenced by KCP&L actions. The security controls discussed later in this report are intended to mitigate the risk posed by specific threat sources, vulnerabilities, or impacts—not to directly influence threats.

2.1 THREAT SOURCE IDENTIFICATION

A threat source, sometimes referred to as a threat vector, can be defined as:

> *"... a path or a tool that a Threat Actor uses to attack the target."*[2]

An attack on a target is not necessarily an intentional action, nor is the Threat Actor always a human. An attack, in this instance, is any event which has the potential to impact the confidentiality, integrity, or availability of a system, or the data generated, stored, or transmitted by that system. A Threat Actor is the source of any event, be it a human, an object, or the force of nature. Often, threats are viewed as strictly malicious or intentional. This report uses a broad definition of a threat, to include unintentional acts and natural occurrences.

Threats are commonly grouped into three categories: natural, human, and environmental. Each category contains possible threat sources which must be identified and evaluated to determine if there is opportunity and likelihood for that threat source to exercise an existing or potential vulnerability. In

---

[1] U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology, *Special Publication 800-30, Risk Management Guide for Information Technology Systems*, July 2002.
[2] Phil Withers, "Information Security Threat Vectors", http://isaca-va.org/Threat%20Vectors.pdf

practical terms, it is not possible to determine every possible threat or vulnerability. KCP&L should perform further periodic risk analyses as new threats or vulnerabilities are discovered. This section will describe the current threat sources identified during the risk assessment. To prevent the implication that one threat source is more likely or serious than another, the following threat sources are listed in alphabetical order.

2.1.1 Acts of Nature

An Act of Nature can threaten facilities, systems, personnel, vital utility infrastructure, and physical operations of SmartGrid systems. The assessment determined that the project is susceptible to a variety of natural disturbances. The likelihood of any individual occurrence impacting the SmartGrid systems is detailed in Section 4.0 of this report, but the most common sources pertaining to an Act of Nature for the area in and around Kansas City include:

Wind Damage: This threat includes damaging winds and flying debris. An occurrence of this threat may also include additional threat sources such as Dependency Failures (personnel or system), Physical Intrusion and/or Theft (looting), or System and Environmental Failures (power failure).

Floods: This threat primarily concerns large scale flooding from nearby streams and rivers. On a smaller scale, this threat may also include localized flash flooding from non-tornadic severe thunderstorms.

Lightning: The largest threat posed by lightning are cloud-to-ground flashes, however, intra-cloud and inter-cloud lighting may also cause brief interference on radio frequency (RF) communications.

Ice: The ice threat refers to both large-scale ice producing storms which may cause damage to infrastructure, as well as localized ice formation which may injure personnel.

2.1.2 Autonomous Systems and Malicious Code

This threat source is most commonly identified with viruses or self-replicating malware such as the recent Stuxnet worm. However, any cyber asset connected to a network may be subjected to a wide range of threats in this category, including such things as:[1]

Viruses: A program or programming code that replicates by being copied or initiating its copying to another program, computer boot sector, or document.

[1] All definitions courtesy of http://searchsecurity.techtarget.com/.

Worms: A self-replicating virus that does not alter files but resides in active memory and duplicates itself.

Trojan Horses: A program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do some intended form of damage.

Spyware: Programming that is put in someone's computer to secretly gather information about the user and relay it to advertisers or other interested parties.

2.1.3 Dependency Failures

An often overlooked threat source is the failure of another system or service outside the direct control of the system owner, which harms or interferes with its ability to function. Events included in dependency failures also include personnel dependencies. The assessment determined the systems within the project may be susceptible to the following dependency failure threats:

Power Failures: This threat may be localized or wide-spread and affect multiple areas of the project.

Downstream Processing Failures: Downstream threats may interfere with data processing, communications, or reporting and may have a negative impact on a system.

System Administrator or SME Job Termination or Reassignment: Loss of key personnel may reduce efficiency of operations and potentially impact system performance.

Failure of a Service or Control Owned by Another Entity Within KCP&L: Loss of processing, data storage, or communications required for optimal operation of a system.

2.1.4 Errors and Omissions

A common internal threat source is an authorized individual performing an inadvertently disruptive or even destructive action. These actions are sometimes difficult to prevent, even with robust change management and quality control programs. Errors can and do happen, even in the most robust environments. Some threats of this source which may impact the project are:

Network Configuration Errors: Mis-configured Network Infrastructure which produces an unintentional vulnerability.

Security Configuration Errors: Poorly written or implemented firewall or other security boundary rules.

Improper Change Management: Performing maintenance on the wrong system (primary instead of secondary, for example).

Improper Configuration Management: Poorly written administration scripts or batch files which create an adverse condition.

Incomplete System Identification: Mislabeling systems or neglecting to update system documentation resulting in confusion or a potential outage situation.

2.1.5 External Attack

This is the threat source most often referenced in the media and identified with cyber security. Threats in this category bring to mind the classic hacker image and are nearly universally applicable for any system connected to an external network, either directly or through intermediate systems. An external network most often refers to the Internet, however, any network outside an existing security boundary, especially those not managed by KCP&L, qualifies as an untrusted external network. The most common examples of external attack which may affect the project are:

System Compromise: This is the classic hacking attack which provides an intruder with elevated privileges, unauthorized access to processes and data, or complete control of a system.

Data and Account Harvesting: This threat is usually an attempt to crack passwords in order to gain unauthorized access, but can also lead to an intruder impersonating a legitimate user in an effort to gain access to more sensitive data or systems.

Website Defacement: Public websites are the online face of KCP&L. Malicious or prank alterations of those public websites may cause damage to the reputation or public image of KCP&L.

Computer Crime: The primary goal of a computer criminal is usually monetary gain. This is one threat in which identity theft may be categorized.

Password Guessing: This threat is related to Data and Account Harvesting, although much less sophisticated and often easier to detect.

Denial of Service: This attack attempts to deny access to a cyber asset or assets. It can often be used as a form of blackmail, but can also be a sign of an attempted spoofing attack on another system.

Social Engineering: This threat can be defined as "…the act of manipulating a person to accomplish goals that may or may not be in the "target's" best interest. This may include obtaining information, gaining access, or getting the target to take certain action."[8]

2.1.6 Insider Abuse and Unauthorized Acts

Although not intentionally malicious in nature, abusing company resources to perform unauthorized, illegal, or inappropriate actions may have unintended consequences which may cause disruption or harm. This threat source can be difficult to detect without active monitoring of employee activities. Threats in this source which may adversely impact the project include:

Sharing or Distribution of Copyrighted Material: Downloading unauthorized copies of music, movies, or other copyrighted material for personal gain, or utilizing file sharing applications on corporate IT systems.

Invasion of Privacy: Unauthorized attempts to access personally identifiable information, defined as "…any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual."[9]

Unauthorized Exploration of Computer Systems: Reconnaissance or mapping of networks without express written consent of the network or system owner(s).

Use of Computing Resources to Harass Others: Threatening or demeaning electronic communication which creates "…an unpleasant or hostile situation for especially by uninvited and unwelcome verbal or physical conduct."[10]

Disregard for or Actively Circumventing Security Controls: Refusing to implement or comply with required security controls, disabling active security controls, or performing actions intended to work around required security controls.

---

[8] Chris Hadnagy, http://www.social-engineer.org/
[9] Executive Office of the President, Office of Management and Budget, M-06-19 Memorandum for Chief Information Officers, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, July 12, 2006
[10] Merriam-Webster Online Dictionary, 2011. http://www.merriam-webster.com

Use of Computing Resources to Perform Illegal Acts: Accessing or attempting to access information or locations which violate local ordinances, state, or Federal law, such as online gambling, child pornography, seditious or anarchist websites, or sites espousing or financing threats against the government.

2.1.7 Insider Attack

Although sometimes overlooked, the insider attack threat source is the most common and most difficult to defend against. Similar in nature to the external attack threat source, an inside attacker has many advantages, possibly including authorized access, with which to perform and hide the attack. The KCP&L SmartGrid Demonstration Project systems, as with any systems, provide many opportunities for insider attack, including:

System Compromise: This is the classic hacking attack which provides an intruder with elevated privileges, unauthorized access to processes and data, or complete control of a system.

Escalation of Privileges: Attempts to gain access to information, systems, technical capabilities, or physical locations to which the individual is not authorized.

Electronic Eavesdropping: Unauthorized access or installation of surveillance devices or software for the purpose of obtaining information which would otherwise be unavailable.

Password Guessing: This threat is usually an attempt to ascertain another user's login credentials in order to gain unauthorized access, but can also lead to an intruder impersonating a legitimate user in an effort to gain access to more sensitive data or systems.

Denial of Service: This attack attempts to deny access to a cyber asset or assets. It can often be used as a form of blackmail, but can also be a sign of an attempted spoofing attack on another system.

Social Engineering: This threat can be defined as "...the act of manipulating a person to accomplish goals that may or may not be in the "target's" best interest. This may include obtaining information, gaining access, or getting the target to take certain action."[1]

[1] Chris Hadnagy, http://www.social-engineer.org/

2.1.8 Legal and Administrative Actions

This threat source is usually the result of failure to comply with regulatory requirements, or unauthorized or illegal actions performed on systems, including the activation of malicious software. Law enforcement or administrative measures in response to those actions may result in an adverse effect on the KCP&L SmartGrid Demonstration Project systems. Threats from legal or administrative actions may include:

Regulatory Findings and Penalties: Internal or external audit findings which result in significant changes to a system which may temporarily impact performance or availability.

Law Enforcement Proceedings Resulting in System Seizure: Investigative measures resulting in the complete loss of a system for forensic analysis or evidential material.

2.1.9 Physical Intrusion and/or Theft

The compromise of a facility or theft of physical resources can pose a significant threat to both the operational capability of the KCP&L SmartGrid systems and the reputation of the company. In this instance, a physical resource refers to more than systems. Theft may also affect items such as proprietary or confidential hard-copy printouts, employee access badges or tokens, and copper or other metals.

Theft can also include non-physical resources such as company data, personal customer information, or passwords.

2.1.10 System and Environmental Failures

This threat source is one of the most commonly recognized and mitigated, and is only occasionally the result of human actions. There are many threats associated with this source, but they can be condensed into generic types. Some of the most common types of threats in this source which may affect the project are:

System Hardware Failures: Malfunction or interruption of hardware devices essential to the function of the system.

Environmental Control Failures: Disruption of systems or devices managing the local environment which houses the system, such as HVAC, humidity, or electronic emissions control.

Software or Data Corruption: Inadvertent altering of system applications, local or offsite system information, or system firmware.

2.1.11 Violent Acts of Man

The violence indicated by this threat source includes not only violence directed against KCP&L personnel or systems, but also violence on a regional or local level that results in indirect harm or dependency failure. Examples of violent threats which may affect the project include:

Riots: Violent public disorder or widespread disturbance of the peace

Gang-Related Violence: Planned or spontaneous incidents involving members of criminal gangs, which result in damage or disruption to systems.

Domestic Incidents: Violent disturbances within or around a household which damage or disrupt a system.

Random Acts of Violence: Unplanned and unaccountable violence perpetrated with no apparent or logical pattern or motivation.

In order to determine a consistent threat rating for the risk calculation model, each threat source was evaluated to determine if it had a chance to impact a given system. The value for this variable is a total number of potential threat sources which may affect the system. The exception is the Acts of Nature threat source, which is assumed to affect every system, and is therefore omitted from the risk calculations. The results of the threat determination calculation are shown in Table 2-1.

System	Identified Threat Sources	Total Number of Potential Threat Sources
AHE	2, 3, 4, 5, 6, 7, 8, 10	8
ALNK	2, 3, 4, 5, 6, 7, 8, 10	8
BMS	2, 3, 4, 5, 6, 8, 10	7
CIS	3, 4, 5, 6, 7, 8, 10	7
DADs (Field and Substation)	3, 4, 5, 7, 9, 11	6
DCADA	3, 4, 5, 6, 7, 8, 10, 11	8
DER – C&I	3, 4, 5, 9, 10, 13	6
DER – Grid-Connected	3, 4, 5, 9, 10, 13	6
DERM	2, 4, 5, 7, 8, 10	6
DER - Residential	3, 4, 5, 9, 10, 11	6
DMAT	3, 4, 6, 7, 10	5
DMS	2, 3, 4, 5, 6, 7, 8, 10	8
EMS	2, 3, 4, 5, 6, 7, 8, 10	8
GIS	2, 3, 4, 6, 7, 8, 10	7
HAND/HANG	3, 5, 8, 9, 10, 11	6
HEMP	2, 3, 4, 5, 7, 8, 10	7
MDM	2, 3, 4, 5, 6, 7, 8, 10	8
MTR	3, 4, 5, 6, 8, 9, 10, 11	8
MWFM	3, 4, 5, 7, 8, 9, 11	7

Table 2-1 Threat Determination Calculation Results

Likelihood and impact levels are discussed later in this report, so it is important to note that this threat rating is only indicating the presence of a threat source with the potential to exercise system vulnerabilities, not the presence of any vulnerability, or the likelihood or impact of such an event.

2.2 MOTIVATION AND THREAT ACTIONS

To assist in determining if a threat source may pose a risk to a specific system, it is important to determine what motivation, if any, a threat source may have to exploit one or more vulnerabilities on that system.

Determining threat motivations is restricted to intentional human threats, since natural, environmental, and inadvertent threats are not premeditated and have no motivation to assess. The motivation for a human threat will vary depending upon the type of threat source. For example, a hacker will have a different motivation to attempt to penetrate the KCP&L SmartGrid Demonstration network than a computer criminal (challenge or ego vs. profit).

Table 2-2 lists the intentional human threat sources described above and assigns potential motivations for each. This table is not intended to imply that these are the only possible motivations, only to give examples of common possible motivations in order to provide guidance in determining if a threat source may pose a risk to a selected system.

As can be seen in Table 2-2, many of the motivations are similar for various threat sources; however, different sources will use varying threat actions to achieve a goal, even if their motivations are the same.

Threat Source	Potential Motivations	Possible Threat Actions
Autonomous Systems and Malicious Code	• Ego/Notoriety • Destruction or Unauthorized Disclosure of Data • Unauthorized Data Alteration • Profit • Blackmail • Revenge	• Broad-Reaching, Self-Replicating Malware (i.e. Code Red) • Targeted Malware (i.e. Stuxnet) • Spyware & Adware Promulgation • System Control Malware (i.e. Win32/Winwebsec)
External Attack	• Challenge • Ego/Notoriety • Destruction or Unauthorized Disclosure of Data • Unauthorized Data Alteration • Industrial Espionage • Blackmail • Revenge	• Hacking • Social Engineering • Unauthorized Privilege Escalation • Spoofing • System Attack (DDoS) • Terrorism
Insider Abuse and Unauthorized Acts	• None (Poorly Trained Personnel) • Ego • Harassment/Stalking • Curiosity	• Computer Abuse • Bypassing Security Controls • Browsing Proprietary or Confidential Data • Pirating Software
Insider Attack	• Challenge • Ego/Notoriety • Curiosity • Profit • Destruction or Unauthorized Disclosure of Data • Unauthorized Data Alteration • Blackmail • Revenge	• Hacking • Social Engineering • Spoofing • Assault • Malicious Code • Unauthorized Privilege Escalation
Legal and Administrative Actions	• Law Enforcement Investigation • Audit Findings • Litigation	• System Seizure • Overly Stringent Security Controls • Legal Hold
Physical Intrusion and/or Theft	• Challenge • Ego/Notoriety • Curiosity • Profit • Destruction of Systems • Blackmail • Revenge	• Jumping or Cutting Fences • Picking or Destroying Physical Locks • Assault • Terrorism
Violent Acts of Man	• Ego • Protest • Territory Infighting	• Assault • Looting • Random Gunfire

Table 2-2 Threat Source Motivations and Threat Actions

3.0 VULNERABILITY ASSESSMENT

For a large program like the KCP&L SmartGrid Demonstration Project, measuring each system's relative weakness for sets of vulnerabilities was the taken approach for the risk assessment. The goal of this assessment was to identify the relative risk level of all SmartGrid systems. As the established model suggests, the vulnerabilities of each system play a large role in the relative risk level determination. For this report, the risk assessment team analyzed the vulnerabilities for each system using a high level approach. Each application was evaluated for broad sets of vulnerabilities that range from system to operational. This approach worked well and produced credible results, especially for several systems that needed to be evaluated whose implementation was still in the early stages at the time this risk assessment was performed.

3.1 VULNERABILITY SOURCES

Vulnerability sources primarily lie in two categories: systems or operations. Within the systems category, it is beneficial to look at generic vulnerabilities that threaten one of the three cyber security goals: Confidentiality, Integrity, and Availability. Operational vulnerabilities, on the other hand, are internal to the organization, and as such, are better assessed in the categories of People, Policy, and Procedures.

The system set of vulnerabilities are either inherited from the original equipment manufacturer (operating systems, firewalls, firmware, third-party software, etc.) or from security oversight during the in-house Software Development Life Cycle (SDLC) process. Unfortunately, the eventual user (in this case, KCP&L) has little or no control in eliminating the threats, but many actions can be taken to guard the vulnerable points. System vulnerabilities can be guarded by placing a combination of security controls like hardening the operating system, utilizing Access Control Lists (ACLs) or firewalls, and implementing secure networks such as Virtual Private Networks (VPNs).

Operational vulnerabilities can be controlled by existing policies enhancement, managerial enforcement, and close monitoring. A list of all known system and operational vulnerabilities that could adversely affect the organization can be found through many credible agencies like the National Labs, Department of Homeland Security (DHS), National Domestic Preparedness Coalition, and vulnerability databases like the National Vulnerability Database (NVD) and Open Web Application Security Project (OWASP)[9]. Their applicability to the KCP&L project, however, should be looked at on a case-by-case basis. The

[9] NISTIR-7628 Volume-III http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol3.pdf

intent of this section is to provide a high-level understanding of the types of vulnerabilities that exists in each category.

3.1.1 Confidentiality Vulnerabilities

This set of vulnerabilities directly threatens the confidentiality of the data stored or processed in the systems. Insufficient authentication and authorization mechanisms give an attacker easy access to classified data. Inadequate data encryption during data transmission provides attackers the means to "sniff" through sensitive material. Insufficient logging and auditing procedures allow an attacker to learn about the system settings and clear its traces once the "intrusion" is over. Holes in the password protection processes provide an attacker access to otherwise restricted areas.

3.1.2 Integrity Vulnerabilities

Vulnerabilities that directly threaten the integrity of a system or its data usually arise from negligence in the SDLC process. Attackers often use this set of vulnerabilities when their motive is not to steal but to create disruption to normal business operations. For such attackers, poorly coded systems or unprotected code repositories are gold mines to be exploited. Inadequate input data ranges and counters are often seen as attack vectors, which can lead to the systems being unreliable. Protocols and communication mediums that do not provide enough protection during data transfer give attackers mechanisms to compromise data integrity. Network devices that do not verify the integrity of data packets against the implemented protocol provide weaker openings that are more susceptible to attacks.

3.1.3 Availability Vulnerabilities

Vulnerabilities exploited in this set result in unavailability of the information system or its data for several hours or in extreme cases, several days. Networks not designed with the philosophy of creating protection zones allow an attacker to inundate applications with rouge requests, resulting in system unavailability and crashes. A type of unavailability attack common to Internet-facing applications is referred to as a Denial-of-Service (DoS) attack. Applications deployed without adequate system redundancy result in complete unavailability during times of forced (attacks) or planned (maintenance) outage events.

3.1.4 Policy Vulnerabilities

The security policy of an organization provides the foundation for protecting information systems against potential threats. Up until the introduction of Advanced Metering Infrastructure (AMI), utilities' IT departments' touchpoints never entered consumer homes. A failure to adjust the security policy to provide protection related to the extended touchpoints may open doors for attackers to penetrate KCP&L

environments. In addition, new systems such as the AMI Head-End (AHE) will collect more granular data that could be used to draw inferences about the consumers' usage patterns. This data is considered private by many consumers. As such, a security policy that does not cover restricted access allows a malicious user to freely review private data.

3.1.5 People Vulnerabilities

New business offerings bring new cyber challenges, making the implementation of good security controls paramount to the success of the project. Further, any sound security implementation requires an equally sound training program. The annual training program for KCP&L employees covers the existing business processes and technologies. However, the introduction of several SmartGrid technologies at KCP&L requires enhancement to the training programs to cover consumer privacy, new standards, and industry best practices. The KCP&L SmartGrid system users and implementers should not be expected to keep systems secure without adequate cyber security training in the SmartGrid domain. An oversight in training may lead to accidental cyber compromise or suboptimal security infrastructure.

3.1.6 Procedural Vulnerabilities

The multi-vendor profile of the project creates opportunities for inconsistencies in configurations, code changes, and patches for system maintenance. Each vendor's development, testing, and implementation timelines for patches and functionality upgrades usually follow different paths, thus opening up windows of exploitations. One of the big challenges in a multi-vendor program such as the KCP&L demonstration project is the coordination of changes to the production environments. Mismatches and frequent releases in the production environment, if not controlled carefully, may result in either system and/or data unavailability or compromised integrity. SmartGrid systems also require additional attention during regression testing, as the patches and upgrades to one system may trigger functional issues in other system(s). An oversight in configuration documentation and disaster recovery processes may also leave systems vulnerable.

3.2 VULNERABILITY RATINGS

The intent of this section is first to introduce a vulnerability rating method and then to evaluate a rating for each of the KCP&L SmartGrid systems. The method was designed to evaluate a Relative Vulnerability Rating (RVR) of each system by looking at the project as a whole. As such, these RVRs should not be used in situations where the requirement is to find a system's stand-alone vulnerability level and not a relative vulnerability level with respect to the other KCP&L SmartGrid systems. To assign a RVR, the first question to answer for each system was, "Relative to other systems, how technically easy

is it to exploit a vulnerability?" For example, EMS and DMS require high technical skills to be exploited and hence their Tech Ease Vulnerability Factor (TEVF) is relatively low. The second question to be answered was, "Relative to other systems, how easy is it to gain access to parts of the assessed system?" Since HEMP is an Internet-facing application, its Ease of Access Vulnerability Factor (EAVF) is relatively high. These two questions were first answered on a qualitative scale ranging from Negligible to Very High and then converted to a numerical representation using a scale of 0 to 10 (0 = Negligible, 2 = Very Low, 4 = Low, 6 = Medium, 8 = High, 10 = Very High).

The overall relative vulnerability rating for each system was then calculated using the formula:

$$RVR = TEVF + EAVF$$

Where:

RVR = Relative Vulnerability Rating

TEVF = Technical Ease Vulnerability Factor

EAVF = Ease of Access Vulnerability Factor

Thus, the values for RVR for the SmartGrid systems ranged from 0 to 10.

3.3 VULNERABILITY ASSESSMENT

The following subsections list the assessment of each planned system in the KCP&L SmartGrid Demonstration Project.

3.3.1 AMI Head-End (AHE)

At the time that this report was developed, the AHE was planned to be hosted external to KCP&L's environment. To perform a thorough assessment, a full review of the vendor's security policy was conducted. The vendor has appropriate focus in securing systems it supports, but the implementation needs to be tested and verified. The TEVF was determined to be Medium (3) because the RF mesh network being utilized and its vulnerabilities are well understood and do not require a very skilled person to coordinate an attack. The EAVF was also found to be Medium (3) because the RF mesh network is physically accessible to the public.

3.3.2 AccountLink (ALNK)

Since ALNK has an Internet-facing customer interface and is implemented with very well-known internet technologies, its TEVF was determined to be High (4). The EAVF was also determined to be High (4) for two primary reasons. First, gaining access to customer account login information is relatively easy through the use of social engineering techniques. Second, the access point is available to anyone who has access to the World Wide Web.

3.3.3 Building Management System (BMS)

The BMS is envisioned to be third-party software installed at commercial and industrial customer sites to manage their Distributed Energy Resources (DER). A thorough vulnerability assessment was deferred because the technology, control mechanism, and protocols were not completely defined when this risk assessment was performed. However, from the little that was known, the TEVF was believed to be Low (2) due to the fact that the BMS (much like the EMS) requires highly technical skills to cause damage. The EAVF was believed to be Medium (3) because the control signals will likely be sent using VPN connections via the Internet.

3.3.4 Customer Information System (CIS)

Due to the many installations of CIS in the utility industry, the technology and the inner workings of the application are very well-known. As a result, the TEVF was determined to be Medium (3). The EAVF was also determined to be Medium (3) because the CIS is well-protected inside the KCP&L network.

3.3.5 Distributed Control and Data Acquisition (DCADA)

The DCADA system is comprised of highly technical information subsystems with complex engineering algorithms. An attacker would have to be very well-versed in engineering applications to cause any damage to these subsystems. As a result, the TEVF for DCADA was estimated to be Low (2). Since access to this application is both electronically and physically designed to be restricted, the only vulnerable points are the connection points between it and the Field and Substation Distribution Automation Devices (DADs). The resultant EAVF was therefore estimated to be Medium (3).

3.3.6 Distributed Energy Resources – Commercial & Industrial (DER – C&I)

The DER - C&I will be managed directly by commercial and industrial customers through their BMS. These resources and their technologies were not completely known at the time of writing this report. Therefore, a thorough risk assessment on DER - C&I could not be done. From the little that was known, the TEVF was estimated to be Low (2) as the technologies are less understood in the attacker community.

The EAVF was estimated to be Medium (3) since the number of implementations is expected to grow, creating new avenues to penetrate. Also, each implementation may not have stringent security measures in place.

3.3.7 Distributed Energy Resources – Grid-Connected (DER – Grid-Connected)

The DER – Grid-Connected will be owned and managed by KCP&L. The first installation will include a battery with a generation management system. The TEVF was determined to be Low (2) because it will require an attacker to understand not only the control logic of battery operations, but also the generation management system. The EAVF, however, was estimated to be Medium (3) because there is more than one communication interface planned for the battery: one from DCADA to send DR signals and the other from a remote location (battery vendor) to manage configurations.

3.3.8 Distributed Energy Resource Management System (DERM)

The DERM will be used to manage DR calculations and requests. This system is planned to be hosted at a vendor site. Any vulnerability at the vendor site could be exploited to affect KCP&L operations. A review of the vendor's security principles was conducted and the results were found to be focused in addressing security needs. However, testing and verification is needed to confirm the implementation. The TEVF was determined to be Medium (3) due to the known vulnerabilities in the communication channels. In addition, since the communication channels between the DERM and KCP&L is planned to be over external networks, the EAVF was determined to be High (4).

3.3.9 Distributed Energy Resources – Residential (DER – Residential)

The DER - Residential will be comprised of customer-managed demand response units and load curtailment units that will be directly managed by KCP&L. The TEVF was determined to be Medium (3) because the control signals will traverse through various systems and devices with a mix of TEVF ratings. The EAVF, on the other hand, was estimated to be High (4) since the attacker will have multiple avenues (several exposed communication channels, systems, and devices) to modify DR signals.

3.3.10 Data Mining and Analysis Tool (DMAT)

The DMAT application is a third-party data mining tool hosted at a vendor site. The answers provided by the vendor in the security questionnaire were found to adequately address the existing security issues. The TEVF was found to be Low (2) because the vendor controls were determined to be satisfactory. However, the EAVF was determined to be Medium (3) due to the existence of several data interfaces between KCP&L and DMAT.

3.3.11 Distribution Management System (DMS)

This suite of applications is the coordinator of energy distribution and is built using complex engineering algorithms. Superior technical skills are required to create and manage this type of application. Thus, an attacker breaking into this application is not a trivial task, which made the TEVF Low (2). The ease of access was estimated to be limited since the DMS will not have many external access points, which also made the EAVF Low (2).

3.3.12 Energy Management System (EMS)

The EMS application (like the DMS) is built upon highly technical principles requiring a highly skilled attacker to exploit system vulnerabilities. The TEVF was therefore estimated to be Low (2). The EAVF was also estimated to be Low (2) because this system resides deep inside KCP&L protection zones.

3.3.13 Field and Substation Distribution Automation Devices (Field-DADs and Substation DADs)

The Distribution Automation Devices have control modules that are used to remotely manage the device functions. It requires a high knowledge of embedded systems to break into such devices, and in many cases, it requires physical access to make changes to the control modules. Due to the relatively high technical knowledge required to break into a DAD, the TEVF was estimated to be Low (2). Since many of these devices will be deployed in the field with less physical security around them, the EAVF was estimated to be Medium (3).

3.3.14 Geographic Information System (GIS)

The GIS application has been in use in many industries for some time, and the inner workings of these applications are not relatively complex. If there are routes available, breaking into these kinds of applications is relatively easy. Therefore, the appropriate TEVF was estimated to be Medium (3). The EAVF was determined to be Low (2) because this system resides inside the KCP&L corporate network (external entities do not have direct connections to it).

3.3.15 Home Area Network Devices and Gateway (HAND and HANG)

The HAN Device(s) and Gateway technologies are still at their nascent stages. Although progress has been made in securing home area networks and the devices connected to them, much work still needs to be done. At the time this report, many cyber security questions remained unanswered for the proposed primary protocol (ZigBee 1.0). Within the protocol stack, different network layers are not cryptographically separated, so access policies are needed and correct design is assumed. ZigBee uses

128-bit keys to implement its security mechanisms, which means different services must use different one-way variations of the link key in order to avoid leaks and security risks. As a result, the TEVF assigned to HANDs and HANG was High (4). The EAVF was also determined to be High (4) because the HAN would exist in every participant's home and any one of those networks could become the target of an attack.

3.3.16 Home Energy Management Portal (HEMP)

The HEMP is the primary interface that KCP&L SmartGrid residential consumers will utilize to manage their HAN, participate in DR events, and view their energy usage. It is planned to be hosted at a vendor site. The TEVF was determined to be High (4) because HEMP is an internet application. The primary determinant of the rating was the attacker community's awareness of this application being very impactful to KCP&L's reputation. The fact that this application is hosted at a vendor site (making KCP&L's security mandate indirect) also supports the High TEVF rating. The EAVF was also determined to be High (4) for two reasons. First, social engineering attempts with consumers can result in easy access, and second, the Internet interface, along with several connections to other systems, opens up multiple avenues for an attack.

3.3.17 Meter Data Management System (MDM)

The MDM acts as the repository of meter inventory and individual consumer usage. This system is hosted at a well-secured vendor site. The TEVF was found to be Low (2) because the encryption and security measures will require a skilled person to coordinate an attack. The EAVF was found to be Medium (3) because the MDM will have interfaces with multiple KCP&L systems, each one requiring data transmission external to KCP&L's corporate network.

3.3.18 SmartMeter (MTR)

MTR refers to the physical SmartMeter that resides on the consumer's premise. The MTR will have capabilities to perform several smart functions like capturing and storing consumer usage and accepting and executing remote connect or disconnect signals. This device has drawn a lot of attention lately from energy theft enablers and hackers. Even though the MTR has embedded systems which require high skill levels to break into, the motivation and desire in the attacker community is large enough that the TEVF was determined to be Medium (3). The EAVF was determined to be Very High (5) because the MTR will be at every consumer location and will have its own broadcasting network (communicates with the consumer's HANG using ZigBee 1.0 protocol).

3.3.19 Mobile Work Force Management System (MWFM)

MWFM is the system used by the field service dispatchers to solve customer issues that require a technician to visit the site. None of the SmartGrid systems will directly interface with the MWFM. The TEVF was determined to be Low (2) because the technical difficulty will be high for an attacker to break into multiple applications to gain access to MWFM. The EAVF was also determined to be Low (2) since no direct access points were planned (at the time of this assessment) between MWFM and any of the SmartGrid systems. An assessment of other vulnerable routes was out of scope because this assessment only covered relative vulnerability ratings within the SmartGrid portfolio.

3.4 VULNERABILITY ASSESSMENT RESULTS

Table 3-1 is based on the assessment performed in the previous section. It provides a quick view of the relative vulnerabilities of the systems by comparing their RVR numbers.

System	TEVF	EAVF	RVR
AHE	3	3	6
ALNE	4	4	8
BMS	2	3	5
CIS	3	3	6
DCADA	2	3	5
DER – C&I	2	3	5
DER – Grid-Connected	2	3	5
DERM	3	4	7
DER – Residential	3	4	7
DMAT	2	3	5
DMS	2	2	4
EMS	2	2	4
Field DADs	2	3	5
GIS	3	2	5
HAND	4	4	8
HANG	4	4	8
HEMP	4	4	8
MDM	2	3	5
MTR	3	5	8
MWFM	2	2	4
Substation DADs	2	3	5

Table 3-1 Relative Vulnerability Ratings of SmartGrid Systems

A summary of the relative vulnerability rating results is graphically represented in Figure 3-1 where each system is placed in either the Low, Medium or High region.

Figure 3-1 Graphical Representation of Relative Vulnerability Ratings

4.0 LIKELIHOOD DETERMINATION

The likelihood of a threat source attempting to impact a system is determined by evaluating a potential threat source's motivation, the nature and frequency of existing vulnerabilities, and perhaps performing a level of statistical analysis for occurrences of common vulnerabilities and exploits.

For example, a disgruntled former employee may have a very high motivation, but the frequency of that sort of threat materializing against a vulnerability is very low. Alternatively, an act of nature has no motivation factor, but different geographic areas present a higher frequency of certain natural occurrences, e.g. severe thunderstorms and tornadoes in the Midwest, hurricanes along the Gulf Coast, and earthquakes in California.

Referencing the Risk Calculation Model, the likelihood of attack is one element of the risk calculation. When evaluating the likelihood of an attempted vulnerability exploit, it is important to realize that this determination does not indicate the likelihood of success, merely the likelihood that an attempt will be made by a threat source to exercise a vulnerability on a system. The following evaluation criteria will be used to assign a value to the likelihood that a potential vulnerability could be exercised by a given threat source.

Likelihood Level	Likelihood Definition	Assigned Value
Very High	The threat-source is highly motivated, capable and presents a targeted attack against KCP&L resources	10
High	The threat-source is highly motivated and sufficiently capable[19]	8
Medium	The threat-source is motivated or capable[20]	6
Low	The threat-source lacks motivation or capability[21]	4
Very Low	The threat-source lacks motivation and capability	2
Negligible	The threat-source poses no probability of exercising a vulnerability against KCP&L	0

Table 4-1 Likelihood Evaluation Criteria

The following sections list each system within the scope of this risk assessment of the KCP&L SmartGrid Demonstration. Each of these systems was deemed essential to the reliable operation and management of the project. Each system was evaluated to determine the event likelihood for each threat source. The overall likelihood rating for each system is the highest value determined for any threat source that may target that system.

---

[19] U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology, *Special Publication 800-30, Risk Management Guide for Information Technology Systems*, July 2002.
[20] Phil Withers, "Information Security Threat Vectors", http://isaca-va.org/Threat%20Vectors.pdf

4.1 ANALYSIS OF THREAT LIKELIHOOD

4.1.1 Common Likelihood Ratings

Some threat sources are common across all the systems within the scope of the SmartGrid risk assessment. To avoid repetition within the report, these common threat sources are listed here. These common values will be used in the event that a common threat source represents the highest likelihood of a vulnerability being exercised on a given system.

4.1.1.1 Acts of Nature

HIGHEST LIKELIHOOD RATING: 6

There is, of course, no motivating factor to consider for this threat source, and with the randomness of Acts of Nature, it is difficult to assign a likelihood value without extensive statistical analysis beyond the scope of this assessment. The following are the most likely Acts of Nature to affect the Kansas City area.

Wind Damage: Damage from straight line winds or tornados is a slight risk for the Kansas City metro area. The potential of a strong tornado (F2 or greater) striking the Kansas City area is less than .025%[9]. Although this ranks as the 35th highest likelihood in the nation, it still represents a very low possibility of this event affecting any of the systems within scope of this assessment.

Likelihood Rating: 4

Floods: Kansas City frequently experiences flooding along rivers and lakes, however, significant flooding which may affect the SmartGrid systems are much less common. In order to require closing levees along the Missouri River in Kansas City, river levels must be forecast to reach 39 feet[10]. Since 1900, there have been 9 instances of flooding significant enough to reach this level.[11] This presents a very low probability of this event affecting any of the systems within scope of this assessment. Although localized or flash flooding is more common, it is not deemed a significant threat to the data centers housing the SmartGrid systems, the communications network, or the Midtown Substation itself.

Likelihood Rating: 2

---

[9] Climatological Threat Potential, National Oceanic and Atmospheric Administration (NOAA), http://www.src.noaa.gov/climo/online/rda/EAX.html
[10] NOAA, National Weather Service, Advanced Hydrologic Prediction Service, *Missouri River at Kansas City, Flood Impacts*. http://water.weather.gov/ahps2/hydrograph.php?wfo=eax&gage=kcdm7&view=1,1,1,1,1,1,1&toggles=10,7,8,2,9,15,6
[11] NOAA, National Weather Service, Advanced Hydrologic Prediction Service, *Historical Crests for Missouri River at Kansas City*, http://water.weather.gov/ahps2/crests.php?wfo=eax&gage=kcdm7

Ice: The primary danger posed from this threat source is loss of power, or inability of support personnel to physically access the SmartGrid systems. Statistics for ice storms are difficult to come by, but a review of local weather patterns indicates this is a real, but relatively low likelihood event.

Likelihood Rating: 4

Lightning: Cloud-to-Ground Lightning flashes average over 995,000 occurrences per year in Missouri and over 899,000 per year in Kansas. Those numbers equate to 14.3 strikes per square mile in Missouri and 11 strikes per square mile in Kansas.[24] These numbers rank in the top thirty percent of lightning strikes per square mile in the United States, indicating the frequency and severity of thunderstorms in Kansas City and throughout the region, making this threat the most likely Act of Nature to impact the systems of the SmartGrid Demonstration.

Likelihood Rating: 6

4.1.1.2 Autonomous Systems and Malicious Code

The likelihood of a malware vulnerability being exploited is more dependent upon the platform being attacked than the specific application or system function. While instances of malware targeting applications are becoming more prevalent, vulnerabilities to those applications are still primarily dependent upon the operating system on which they are deployed.

For this reason, the Autonomous Systems and Malicious Logic threat source is split into two possible likelihood ratings, based upon the system platform and operating system. Threats to mobile computing devices are not considered in this risk assessment. If mobile computing is deployed within the KCP&L SmartGrid environment in the future, another risk assessment should be performed which includes an evaluation of those threats.

4.1.1.2.1 Microsoft Windows-Based Cyber Assets

The Windows-Based likelihood rating assumes some common applications and utilities are not present or active on the Windows cyber asset. These common applications include; Java and JavaScript, Adobe Acrobat, and any application from the Microsoft Office Suite. Although Internet Explorer is integral to

[24] NOAA, National Weather Service, Weather Forecast Office, Central Region Headquarters, *Rank of Cloud-to-Ground Flash Densities by State from 1996 to 2008, http://www.crh.noaa.gov/Image/lsx/wcm/96-08Cloud_to_Ground.pdf*

any installation of Microsoft Windows, an additional assumption is that HTTP connections are not permitted to untrusted networks from the cyber assets in the KCP&L SmartGrid demonstration.

Vulnerabilities and exploits targeting Windows-based applications, although generally declining, still represent a far larger percentage of the overall reported vulnerabilities in 2010, as opposed to operating system or browser vulnerabilities.[2] For that reason, if any of the assumptions stated above prove incorrect, the likelihood rating would potentially be much higher.

Although Windows operating system vulnerabilities and exploits are smaller in number relative to those for Windows-based applications, there are still a large number of reported exploits against the Windows operating system, perhaps due to its large installation base around the world. Exploits detected by Microsoft numbered just under 200,000 in each of the first two quarters of 2010.[1]

An additional consideration for this likelihood rating is the version of Microsoft Windows installed on each cyber asset. Newer versions such as Windows Server 2003 or the Windows 7 Desktop obtain better and more up to date support, and were developed with more security built in than older versions of the Windows operating system. Due to the range of operating systems and versions in the KCP&L SmartGrid demonstration, this report maintains a "highest likelihood rating" approach.

Likelihood Rating: 8

4.1.1.2.2 Unix-Based and Linux-Based Cyber Assets

The likelihood rating for Unix and Linux-based systems is predicated on existing data indicating fewer identified vulnerabilities for those operating systems.[3] As with the Windows-based likelihood rating, prior to assigning a likelihood rating for this threat source, the assumption was made that certain applications were not present or active on the system. These common applications include; Java and Javascript, Adobe Acrobat, and web browsers such as Mozilla.

Likelihood Rating: 6

---

[2] Microsoft Corporation, *Microsoft Security Intelligence Report, Volume 10*, July 11, 2011
[3] GFI Software, *Top Most Vulnerable Applications and Operating Systems in 2010*, February 17, 2011, http://www.gfi.com/blog/top-vulnerable-applications-operating-systems-2010/

4.1.1.3 Errors and Omissions:

The likelihood of this threat source being exercised is nearly random. The execution of errors and omissions is almost exclusively inadvertent human interaction, so it may be influenced to a degree if there is more human interaction with a cyber asset. However, it is impossible to assign a realistic figure to the likelihood rating for Errors and Omissions without a thorough statistical analysis of related events at KCP&L. Such an in depth analysis is outside the scope of this risk assessment.

For the purposes of this assessment, beginning with a global average likelihood rating of 3 will provide a baseline for the evaluation of risk for this threat source.

Likelihood Rating: 6

4.1.1.4 Insider Abuse and Unauthorized Acts:

This likelihood rating is similar to Errors and Omissions, in that it is a nearly random occurrence with little evidence to support a quantitative likelihood rating, outside of an exhaustive statistical analysis.

For that reason, and also similar to Errors and Omissions, Insider Abuse and Unauthorized Acts is given a global average likelihood rating of 3 to provide a baseline for risk evaluation.

Likelihood Rating: 6

4.1.1.5 Legal and Administrative Actions:

Any system may be affected by audit findings or become involved in a criminal investigation. Although it may seem that systems with fewer security controls would be more apt to incur attacks and negative audit results, this is not always the case. Due to the unpredictable nature of this threat source, a global average likelihood rating of 3 is provided as a baseline for risk evaluation.

Likelihood Rating: 6

4.1.2 System-Specific Likelihood Ratings

4.1.2.1 AMI Head End (AHE)

HIGHEST LIKELIHOOD RATING: 8

Dependency Failures: The AHE system collects data from meters and interfaces with the MDM, CIS, DERM, and HEMP systems. The loss of a small number of meters is more likely than losing connectivity with any of the primary systems which interface with AHE.

Likelihood Rating: 4

External Attack: The AHE System is hosted outside the physical control of KCP&L in a secure Landis+Gyr datacenter. Although this fact is not common knowledge outside the SmartGrid demonstration project, neither is it classified as Restricted information. As a known collection point for the most visible elements of the SmartGrid network, namely the meters, the AHE system presents a higher profile target than many systems of the SmartGrid. Therefore, the likelihood of an external threat source targeting this system is elevated.

Likelihood Rating: 6

Insider Attack: Access to the AHE becomes much easier and knowledge of the importance of the AHE system more common from inside the KCP&L or Landis+Gyr environments. This makes an insider a more likely threat to the AHE system.

Likelihood Rating: 8

Physical Intrusion and/or Theft: The physical location of the Landis+Gyr datacenter is unknown, so an analysis of crime statistics for the area is unavailable. No national statistics are available for data center thefts but based on a cursory search of Internet information, it can be ascertained that datacenter theft, although rare, is not unprecedented.

Likelihood Rating: 4

System and Environmental Failures: The AHE system is hosted in an environmentally controlled Landis+Gyr data center outside the physical control of KCP&L. The environmental controls and equipment are managed and monitored continuously and regularly maintained, lessening the likelihood of a malfunction or other operational failure. However, even the best maintained equipment is occasionally

offline, whether planned or unplanned, making it possible albeit unlikely for this threat source to impact the AHE system.

Likelihood Rating: 4

Violent Acts of Man: Similar to the Physical Intrusion and/or Theft threat source, it is difficult to perform an analysis of crime statistics near the Landis+Gyr datacenter because the exact physical location is unknown. However, instances of random violence serious enough to threaten the AHE system do not seem likely.

Likelihood Rating: 2

4.1.2.2 AccountLink (ALNK)

*HIGHEST LIKELIHOOD RATING: **10***

Dependency Failures: The ALNK system accepts connections from the Internet and interfaces with the HEMP system to provide customers a portal into their energy usage and billing. The ALNK system does not rely upon external data for operations and while it is possible that all the network circuits may fail, the likelihood of that occurring is fairly low.

Likelihood Rating: 4

External Attack: As the Internet-facing customer portal for KCP&L, the ALNK system may be the highest profile system and therefore the most likely target in the SmartGrid environment. Realizing also that, according to some statistics, four of the top 10 external vulnerabilities target web services, the likelihood of this threat source being exercised is very high.

Likelihood Rating: 10

Insider Attack: The primary motivations for an insider attack would be monetary gain, blackmail, or revenge using the personal information stored on the system. These types of intrusions are fairly rare, lessening the likelihood of such an event occurring on the ALNK system. However, the presence of large amounts of personal customer information may provide additional motivation to exploit a vulnerability on this system.

Likelihood Rating: 8

Physical Intrusion and/or Theft: Other than the value of the hardware, there is little to gain from the theft of the ALNK system. Obtaining the system's data would be more likely accomplished through cyber means. A cursory examination of crime statistics in the area of the KCP&I. data center did not indicate a large concentration of break-ins or business-related crime.[9]

Likelihood Rating: 4

System and Environmental Failures: The ALNK system is hosted in an environmentally controlled data center, which is managed and monitored continuously and regularly maintained, lessening the likelihood of a malfunction or other operational failure. However, even the best maintained equipment is occasionally offline, whether planned or unplanned, making it possible albeit unlikely for this threat source to impact the ALNK system.

Likelihood Rating: 4

Violent Acts of Man: The most accurate method to determine this likelihood rating is a thorough investigation into the statistical probability of violence in the area around the datacenter, which is outside the scope of this risk assessment. However, a quick search of random violence in the North Kansas City area indicated that instances of random violence serious enough to threaten the ALNK system within a secured datacenter do not appear likely.

Likelihood Rating: 2

4.1.2.3 Building Management System (BMS)

HIGHEST LIKELIHOOD RATING: 4

Dependency Failures: The BMS system manages DER systems in commercial and industrial locations, and interfaces with the DERM system. The likelihood of these connections failing is low.

Likelihood Rating: 4

External Attack: The presence of the BMS system interface at customer locations increases the likelihood of curious or malicious individuals will attempt to penetrate the system from that location. However, the relatively low current profile of DER resources reduces that likelihood greatly.

Likelihood Rating: 4

[9] https://www.crimereports.com/

Insider Attack: The likelihood of an internal attacker exercising a vulnerability on the BMS is relatively low due to the presence of higher profile targets with greater opportunity to gain valuable data or disrupt operations.

Likelihood Rating: 4

Physical Intrusion and/or Theft: Other than the value of the hardware, there is little to gain from the theft of the BMS system. Obtaining the system's data would be more likely accomplished through cyber means. The likelihood of theft may increase in neighborhoods more prone to criminal activity, but such a determination cannot be made for the current KCP&L SmartGrid demonstration.

Likelihood Rating: 4

System and Environmental Failures: Unlike many of the systems in the KCP&L SmartGrid environment, the BMS system is not located in a controlled environment. The potential for weather-related interruptions increases the likelihood of a temporary failure of individual communication channels, or sections of wireless communication.

Likelihood Rating: 4

Violent Acts of Man: The most accurate method to determine this likelihood rating is a thorough investigation into the statistical probability of violence in the area around the datacenter, which is outside the scope of this risk assessment. As such, a more accurate determination cannot be made for the current KCP&L SmartGrid demonstration.

Likelihood Rating: 2

4.1.2.4 Customer Information System (CIS)

HIGHEST LIKELIHOOD RATING: 8

Dependency Failures: The CIS system interfaces with many other systems to send and receive data. The likelihood of failure for the most important interfaces to the AHE, MDM, or HEMP is greater due to the distance between the locally maintained CIS and those remotely hosted systems.

Likelihood Rating: 6

External Attack: The CIS is not a customer-facing system, nor does it directly interface with public networks. However, there are three interfaces to externally hosted systems. Moreover, the presence of

large amounts of personal customer information may provide additional motivation to exploit a vulnerability on this system.

Likelihood Rating: 8

Insider Attack: The primary motivations for an insider attack would be monetary gain, blackmail, or revenge using the personal information stored on the system. These types of intrusions are fairly rare, lessening the likelihood of such an event occurring on the CIS system. However, the presence of large amounts of personal customer information may provide additional motivation to exploit a vulnerability on this system.

Likelihood Rating: 8

Physical Intrusion and/or Theft: Other than the value of the hardware, there is little to gain from the theft of the CIS system. Obtaining the system's data would be more likely accomplished through cyber means. A cursory examination of crime statistics in the area of the KCP&L data center did not indicate a large concentration of break-ins or business-related crime.*

Likelihood Rating: 4

System and Environmental Failures: The CIS system is hosted in an environmentally controlled data center, which is managed and monitored continuously and regularly maintained, lessening the likelihood of a malfunction or other operational failure. However, even the best maintained equipment is occasionally offline, whether planned or unplanned, making it possible albeit unlikely for this threat source to impact the CIS system.

Likelihood Rating: 4

Violent Acts of Man: The most accurate method to determine this likelihood rating is a thorough investigation into the statistical probability of violence in the area around the datacenter, which is outside the scope of this risk assessment. However, a quick search of random violence in the North Kansas City area indicated that instances of random violence serious enough to threaten the CIS system within a secured datacenter are not likely.

Likelihood Rating: 2

* https://www.crimereports.com/

4.1.2.5 Distribution Automation Devices (DADs)

HIGHEST LIKELIHOOD RATING: 6

Dependency Failures: The DADs transmit system parameter data to the DMS and DCADA for processing. These systems are located in controlled and monitored environments and are considered critical to the operation of the distribution network, increasing the frequency of maintenance and reducing the potential for failure.

Likelihood Rating: 4

External Attack: The DADs use a wireless network to communicate, presenting an attractive attack vector for a potential intruder, and the large number of DADs presents a target-rich environment.

Likelihood Rating: 6

Insider Attack: Although an inside attacker would have access to the systems upstream from the DADs and potentially the ability to affect their operation, the only real motivation for an insider would be revenge or data leak from a disgruntled employee, reducing the likelihood of an internal intrusion.

Likelihood Rating: 4

Physical Intrusion and/or Theft: The distributed locations of the DADs presents a greater profile for theft, however, there is a limited market for resale. Since profit would be the most common motivation for theft of these devices, their limited appeal also limited their attractiveness to thieves. An attacker bent on destructive or disruptive motives would most likely target systems farther upstream in order to impact a larger area.

Likelihood Rating: 4

System and Environmental Failures: Unlike many of the systems in the KCP&L SmartGrid environment, the DADs are not located in a controlled environment. The potential for weather-related interruptions increases the likelihood of a temporary failure of individual DADs or sections of the wireless communication. In addition, due to the large number of DADs, a communication failure to any one of them becomes more likely.

Likelihood Rating: 6

Violent Acts of Man: The location of the DADs much closer to the general public makes them more susceptible to damage if there is an outbreak of violence in the area. Although the DADs are unlikely to be a direct target, their proximity alone increases the likelihood of public violence making an impact. However, a review of crime statistics in the area provides no indication of such widespread violence, reducing the likelihood of impact.[9]

Likelihood Rating: 4

4.1.2.6 Distribution Control and Data Acquisition (DCADA)

HIGHEST LIKELIHOOD RATING: 6

Dependency Failures: The DCADA accepts input from the DADs, and provided data to the DMS. The loss of individual DADs would not impact the ability of the DAC or DDC subsystems to function, but would impact the accuracy of their output to DMS, increasing the likelihood of a loss due to the large number of systems DCADA depends upon for information.

Likelihood Rating: 4

External Attack: Remote access to the DCADA system is primarily controlled via the DMS, but their connection to an IP network provides additional avenues of attack. The most likely motivation for this threat source would be revenge or espionage, meaning an attacker would need to have at least cursory knowledge of distribution automation, reducing the likelihood that either the DAC or DDC would be primary targets.

Likelihood Rating: 4

Insider Attack: The primary motivation for an insider to target the DCADA system would most likely be revenge, meaning unless the attacker had detailed knowledge of the DAC or DDC systems specifically, a higher profile target would be more appealing. However, any insider with access to the system would be able to cause extensive disruption, which may provide incentive to an insider bent upon causing damage to KCP&L's equipment or reputation.

Likelihood Rating: 6

[9] https://www.crimereports.com/

Physical Intrusion and/or Theft: The location of the DCADA systems within the perimeter of a substation reduces their availability for theft and the likelihood they would be targeted. Even if an intruder gained access to the substation, they would need to be directly targeting the DCADA system, further reducing the likelihood of this threat source impacting them.

Likelihood Rating: 4

System and Environmental Failures: Unlike many of the systems in the KCP&L SmartGrid environment, the DADs are not located in a controlled environment. The potential for weather-related interruptions increases the likelihood of a temporary failure of individual DADs and/or their communication network.

Likelihood Rating: 6

Violent Acts of Man: The location of the DCADA systems much closer to the general public makes them more susceptible to damage if there is an outbreak of violence in the area. Although DCADA is unlikely to be a direct target, its proximity alone increases the likelihood of public violence making an impact. However, a review of crime statistics in the area provides no indication of such widespread violence, reducing the likelihood of impact.[9]

Likelihood Rating: 4

4.1.2.7 Distributed Energy Management System (DERM)

HIGHEST LIKELIHOOD RATING: 6

Dependency Failures: The DERM system interfaces with many other systems both to provide and receive data. The likelihood of failure for the most important interfaces to the DMS, MDM, or HEMP systems is greater due to the distance and complexity of communication between remotely hosted systems.

Likelihood Rating: 6

External Attack: The use of a proprietary operating system means an external attacker would need direct knowledge of this specific product in order to successfully mount an attack other than denial of service. This fact limits the potential motivations to revenge or unauthorized data disclosure. Since the HEMP

[9] https://www.crimereports.com/

system contains customer load information and processes demand response schedules, it presents a more likely target for an external attacker wishing to cause damage to the local distribution network or KCP&L's reputation.

Likelihood Rating: 6

Insider Attack: The demand response functions of the DERM system could present an attractive target to an insider with knowledge of the environment and the motivation of causing disruption to the local distribution network.

Likelihood Rating: 6

Physical Intrusion and/or Theft: The physical location of the OATI datacenter is unknown, so an analysis of crime statistics for the area is unavailable. No national statistics are available for datacenter thefts but a cursory search of Internet information shows that datacenter theft, although rare, is not unprecedented.

Likelihood Rating: 4

System and Environmental Failures: The DERM system is hosted in an environmentally controlled OATI data center, which places it outside the physical control of KCP&L. The environmental controls and equipment are managed and monitored continuously and regularly maintained, lessening the likelihood of a malfunction or other operational failure. However, even the best maintained equipment is occasionally offline, whether planned or unplanned, making it possible albeit unlikely for this threat source to impact the DERM system.

Likelihood Rating: 4

Violent Acts of Man: Similar to the Physical Intrusion and/or Theft threat source, it is difficult to perform an analysis of crime statistics near the OATI datacenter because the exact physical location is unknown. However, instances of random violence serious enough to threaten the DERM system do not seem likely.

Likelihood Rating: 2

4.1.2.8 Distributed Energy Resources (DER - C&I, DER - Residential, Grid-Connected DER))

HIGHEST LIKELIHOOD RATING: 6

Dependency Failures: Various implementations of DER would have different interfaces within the SmartGrid environment. The common theme for dependencies is response for DR purposes. Most of these systems will be outside the immediate physical control of KCP&L, increasing the likelihood of this type of threat impacting them.

Likelihood Rating: 4

External Attack: Due to its limited capacity, the current plans for DER in the SmartGrid demonstration environment make it an unlikely target for an external attack. However, if an attacker were motivated by curiosity, the likelihood of this threat would increase.

Likelihood Rating: 6

Insider Attack: The limited capacity and impact of the various DER systems make it an unlikely target for an inside attacker. Widespread deployment or an increased impact on DR operations or decisions may increase the likelihood of an insider attack.

Likelihood Rating: 4

Physical Intrusion and/or Theft: The DER system is too large to steal, but could be used as blackmail if an event were leaked to the local media.

Likelihood Rating: 4

System and Environmental Failures: Implementation of the DER system is proposed for inside the substation of the SmartGrid demonstration. This limits the potential for an environmental or system failure.

Likelihood Rating: 4

Violent Acts of Man: The planned locations of the various DER systems in homes, businesses, and substations bring them closer to potential violence. However, instances of random violence serious enough to threaten the DER systems do not seem likely.

Likelihood Rating: 4

4.1.2.9 Data Mining and Analysis Tool (DMAT)

HIGHEST LIKELIHOOD RATING: 6

Dependency Failures: DMAT receives input and provides data to the MDM system. The likelihood of a dependency failure for any one communications circuit is relatively small.

Likelihood Rating: 4

External Attack: DMAT contains customer energy usage data, which may make it an attractive target for an attacker motivated by revenge, curiosity, or third party marketing.

Likelihood Rating: 6

Insider Attack: The information processed by DMAT is available for less effort from other systems accessible by an insider, making it unlikely an insider would use this avenue of compromise.

Likelihood Rating: 4

Physical Intrusion and/or Theft: The physical location of the DataRaker datacenter is unknown, so an analysis of crime statistics for the area is unavailable. No national statistics are available for datacenter thefts but a cursory search of Internet information shows that datacenter theft, although rare, is not unprecedented.

Likelihood Rating: 4

System and Environmental Failures: The DMAT system is hosted in an environmentally controlled DataRaker data center, which places it outside the physical control of KCP&L. The environmental controls and equipment are managed and monitored continuously and regularly maintained, lessening the likelihood of a malfunction or other operational failure. However, even the best maintained equipment is occasionally offline, whether planned or unplanned, making it possible albeit unlikely for this threat source to impact the DMAT system.

Likelihood Rating: 4

Violent Acts of Man: Similar to the Physical Intrusion and/or Theft threat source, it is difficult to perform an analysis of crime statistics near the DMAT datacenter because the exact physical location is unknown. However, instances of random violence serious enough to threaten the DMAT system do not seem likely.

Likelihood Rating: 2

4.1.2.10 Distribution Management System (DMS)

HIGHEST LIKELIHOOD RATING: 8

Dependency Failures: The DMS interfaces with at least six other systems, making the loss of any one communication path possible but unlikely.

Likelihood Rating: 4

External Attack: The DMS is the backbone of the SmartGrid distribution network, increasing the public profile and presenting a more attractive target for an attacker.

Likelihood Rating: 6

Insider Attack: If an insider wanted to do the most possible damage to the KCP&L SmartGrid demonstration, the DMS may be the system most likely to be attacked due to its high profile.

Likelihood Rating: 8

Physical Intrusion and/or Theft: Other than the value of the hardware, there is little to gain from the theft of the DMS system. Obtaining the system's data would be more likely accomplished through cyber means. A cursory examination of crime statistics in the area of the KCP&L data center did not indicate a large concentration of break-ins or business-related crime.[1]

Likelihood Rating: 4

[1] https://www.crimereports.com/

System and Environmental Failures: The DMS system is hosted in an environmentally controlled data center, which is managed and monitored continuously and regularly maintained, lessening the likelihood of a malfunction or other operational failure. However, even the best maintained equipment is occasionally offline, whether planned or unplanned, making it possible albeit unlikely for this threat source to impact the DMS system.

Likelihood Rating: 4

Violent Acts of Man: The most accurate method to determine this likelihood rating is a thorough investigation into the statistical probability of violence in the area around the datacenter, which is outside the scope of this risk assessment. However, a quick search of random violence in the North Kansas City area indicated that instances of random violence serious enough to threaten the DMS system within a secured datacenter are not likely.

Likelihood Rating: 4

4.1.2.11 Energy Management System (EMS)

HIGHEST LIKELIHOOD RATING: 10

Dependency Failures: Within the scope of the SmartGrid environment, the EMS interfaces with the DADs at the Substation. This line of communication is unlikely to be broken during normal operation.

Likelihood Rating: 4

External Attack: The EMS is a very visible part of KCP&L's transmission and distribution network. As such, it presents a larger attack profile than a lesser known system. An attacker could be motivated by a range of factors, including destruction or unauthorized disclosure of data, industrial espionage, blackmail, or revenge.

Likelihood Rating: 8

Insider Attack: A malicious insider could have multiple motives for attacking the EMS, and would understand its importance to the KCP&L mission, including the SmartGrid environment. This makes the EMS a very likely target.

Likelihood Rating: 10

Physical Intrusion and/or Theft: Other than the value of the hardware, there is little to gain from the theft of the EMS system other than disruption of KCP&L's transmission network. Obtaining the system's data would be more likely accomplished through cyber means. A cursory examination of crime statistics in the area of the KCP&L control center did not indicate a large concentration of break-ins or business-related crime.[5]

Likelihood Rating: 4

System and Environmental Failures: The EMS system is hosted in an environmentally-controlled control center, which is managed and monitored continuously and regularly maintained, lessening the likelihood of a malfunction or other operational failure. However, even the best maintained equipment is occasionally offline, whether planned or unplanned, making it possible albeit unlikely for this threat source to impact the EMS system.

Likelihood Rating: 4

Violent Acts of Man: The most accurate method to determine this likelihood rating is a thorough investigation into the statistical probability of violence in the area around the datacenter, which is outside the scope of this risk assessment. However, a quick search of random violence in the North Kansas City area indicated that instances of random violence serious enough to threaten the EMS system within a secured control center are not likely.

Likelihood Rating: 4

4.1.2.12 Geographical Information System (GIS)

HIGHEST LIKELIHOOD RATING: 6

Dependency Failures: The GIS system has two interfaces into the KCP&L SmartGrid environment, to the CIS and the DMS. The likelihood of these connections failing is fairly low.

Likelihood Rating: 4

[5] https://www.crimereports.com/

External Attack: The geographical data provided by GIS provides detailed hard copy maps of the distribution system that are kept in field vehicles. This information may focus an attacker's energy on discovering what other information is contained in GIS, or falsifying data to disrupt operations.

Likelihood Rating: 6

Insider Attack: A knowledgeable insider could attempt to alter GIS data to disrupt maintenance or repair efforts, among other things.

Likelihood Rating: 6

Physical Intrusion and/or Theft: Other than the value of the hardware, there is little to gain from the theft of the GIS system. Obtaining the system's data would be more likely accomplished through cyber means. A cursory examination of crime statistics in the area of the KCP&L data center did not indicate a large concentration of break-ins or business-related crime.[9]

Likelihood Rating: 4

System and Environmental Failures: The GIS system is hosted in an environmentally controlled data center, which is managed and monitored continuously and regularly maintained, lessening the likelihood of a malfunction or other operational failure. However, even the best maintained equipment is occasionally offline, whether planned or unplanned, making it possible albeit unlikely for this threat source to impact the GIS system.

Likelihood Rating: 4

Violent Acts of Man: The most accurate method to determine this likelihood rating is a thorough investigation into the statistical probability of violence in the area around the datacenter, which is outside the scope of this risk assessment. However, a quick search of random violence in the North Kansas City area indicated that instances of random violence serious enough to threaten the GIS system within a secured datacenter are not likely.

Likelihood Rating: 4

[9] https://www.crimereports.com/

4.1.2.13 Home Area Network Devices/Gateway (HAND/HANG)

HIGHEST LIKELIHOOD RATING: 8

Dependency Failures: The Home Area Network devices receive data from multiple sources to provide accurate information to the customer. Many of these interfaces may rely upon power line or wireless communications, increasing the likelihood of a disruption.

Likelihood Rating: 6

External Attack: As the devices closest to the customer, the HAN devices and gateway are a high profile target for attackers interested in how they work, or attempting to alter power usage data. The presence of these devices within customer's homes increases the likelihood of malicious or curious tampering with them.

Likelihood Rating: 6

Insider Attack: An insider would understand the importance of the HAN to individuals involved with the KCP&L SmartGrid environment, but would also understand the benefit of attacking further downstream in the data processing.

Likelihood Rating: 4

Physical Intrusion and/or Theft: The location of HAN devices and gateways within private residences creates an opportunity for customers to physically break into them for curiosity's sake, to attempt to alter their energy bill, or to sell them in an effort to make a profit.

Likelihood Rating: 8

System and Environmental Failures: Power failures in residential areas are common enough to be an issue for HAN devices. The physical environment is also outside the control of KCP&L, which may lead to overheating, water damage, fire damage, etc.

Likelihood Rating: 8

Violent Acts of Man: Domestic violence is a more likely scenario for causing damage or malfunction on Home Area Network devices. KCP&L has no impact or local authority to prevent or deter such violence from damaging or destroying HAN devices.

Likelihood Rating: 6

4.1.2.14 Home Energy Management Portal (HEMP)

*HIGHEST LIKELIHOOD RATING: **10***

Dependency Failures: The HEMP system interfaces with many other systems to provide and receive data for processing and/or display to customers. The system also accepts inputs from customers for their account. This amount of interaction provides many opportunities for failure.

Likelihood Rating: 6

External Attack: The HEMP is a web-based front-end into a customer's energy usage and efficiency. It is accessed via a link from another web-based portal (ALNK). The combination of a high-profile application and high-profile platform vulnerabilities leads to a very high likelihood of this threat source attempting to impact HEMP.

Likelihood Rating: 10

Insider Attack: The motivations an insider may have to affect the data or function of HEMP range from revenge to curiosity. In such cases, the HEMP provides a high-profile target for attempted penetration.

Likelihood Rating: 6

Physical Intrusion and/or Theft: The physical location of the Tendril datacenter is unknown, so an analysis of crime statistics for the area is unavailable. No national statistics are available for datacenter thefts but a cursory search of Internet information shows that datacenter theft, although rare, is not unprecedented.

Likelihood Rating: 4

System and Environmental Failures: The HEMP system is hosted in an environmentally controlled Tendril data center, which places it outside the physical control of KCP&L. The environmental controls and equipment is managed and monitored continuously and regularly maintained, lessening the likelihood of a malfunction or other operational failure. However, even the best maintained equipment is

occasionally offline, whether planned or unplanned, making it possible albeit unlikely for this threat source to impact the HEMP system.

Likelihood Rating: 4

Violent Acts of Man: Similar to the Physical Intrusion and/or Theft threat source, it is difficult to perform an analysis of crime statistics near the Tendril datacenter because the exact physical location is unknown. However, instances of random violence serious enough to threaten the HEMP system do not seem likely.

Likelihood Rating: 2

4.1.2.15 Meter Data Management System (MDM)

HIGHEST LIKELIHOOD RATING: 6

Dependency Failures: The MDM system interfaces with many other systems to process energy usage and information for customer billing. The number of inputs presents more opportunities for dependency failure.

Likelihood Rating: 6

External Attack: The MDM may present an attractive target for an attacker attempting to view or alter customer usage or billing information.

Likelihood Rating: 6

Insider Attack: The most likely scenario for an insider to attack the MDM is for revenge or curiosity. There is minimal personal information on the system, so an attack to find that data would focus on other systems.

Likelihood Rating: 4

Physical Intrusion and/or Theft: The physical location of the Siemens datacenter is unknown, so an analysis of crime statistics for the area is unavailable. No national statistics are available for datacenter thefts but a cursory search of Internet information shows that datacenter theft, although rare, is not unprecedented.

Likelihood Rating: 4

System and Environmental Failures: The MDM system is hosted in an environmentally controlled Siemens data center, which places it outside the physical control of KCP&L. The environmental controls and equipment are managed and monitored continuously and regularly maintained, lessening the likelihood of a malfunction or other operational failure. However, even the best maintained equipment is occasionally offline, whether planned or unplanned, making it possible albeit unlikely for this threat source to impact the MDM system.

Likelihood Rating: 4

Violent Acts of Man: Similar to the Physical Intrusion and/or Theft threat source, it is difficult to perform an analysis of crime statistics near the Siemens datacenter because the exact physical location is unknown. However, instances of random violence serious enough to threaten the MDM system do not seem likely.

Likelihood Rating: 2

4.1.2.16 SmartMeter (MTR)

*HIGHEST LIKELIHOOD RATING: **10***

Dependency Failures: Meters provide data upstream for processing and billing purposes and in some cases pass signals on to the HAN devices. These connections can be either wired or wireless, which increases the likelihood of interference or interruption.

Likelihood Rating: 6

External Attack: Smart meters have become the symbol of the SmartGrid for many consumers, and often in a negative light. Hackers have already demonstrated exploits against smart meters in public forums and will continue to do so, making the meters perhaps the highest likelihood point of attack in the environment.

Likelihood Rating: 10

Insider Attack: The lack of customer identifiable information reduces the likelihood of meters being a target for internal attack or compromise. No matter the motivation, an insider is more likely to target a system farther downstream.

Likelihood Rating: 4

Physical Intrusion and/or Theft: Meters are already subject to customer and criminal break-ins. Occasionally, the motivation is self-repair in order to avoid a visit fee from the utility, but most often the motive is criminal in nature, such as attempting to artificially lower reported energy usage.

Likelihood Rating: 6

System and Environmental Failures: Meters are designed to withstand power outages and data disruptions. However, the addition of wireless radio and smart functionality increases the likelihood of component failure.

Likelihood Rating: 4

Violent Acts of Man: The presence of meters on every building increases the likelihood of damage any time violence breaks out, no matter the cause or location.

Likelihood Rating: 6

4.1.2.17 Mobile Workforce Management System (MWFM)

HIGHEST LIKELIHOOD RATING: 6

Dependency Failures: The MWFM system receives input from and sends data to the CIS. Each mobile device communicates independently via wireless communication from the field. Individual loss of connectivity is more likely than widespread failure or disruption.

Likelihood Rating: 4

External Attack: The mobile laptops are located in each truck and communicate wirelessly, increasing their network footprint and attack profile.

Likelihood Rating: 6

Insider Attack: The lack of useful data or login credentials make MWFM an unattractive target for malicious insiders.

Likelihood Rating: 4

Physical Intrusion and/or Theft: The mobile laptops are located in each truck and visible from outside the vehicle, making them a tempting target for attackers.

Likelihood Rating: 6

System and Environmental Failures: The mobile laptops contain battery backup and are able to function without power for some time. On the other hand, the rigors of field use may reduce the life expectancy of the mobile laptops.

Likelihood Rating: 4

Violent Acts of Man: It is unlikely for a mobile laptop to become engaged in local or regional violence. Accidental damage during use is more likely.

Likelihood Rating: 6

4.2 LIKELIHOOD DETERMINATION RESULTS

The highest likelihood ratings for all the systems are summarized in Table 4-2.

System	Highest Likelihood (L) Rating
ABE	8
ALNK	10
BMS	4
CIS	8
DADs	6
DCADA	6
DER - C&I	6
DER – Grid-Connected	6
DERM	6
DER - Residential	6
DMAT	6
DMS	8
EMS	10
GIS	6
HAND/HANG	8
HEMP	10
MDM	6
MTR	10
MWFM	6

Table 4-2 Likelihood Ratings

5.0 IMPACT ANALYSIS

The next major step in the risk assessment is to carefully and methodically evaluate the impact of a threat exercising one or more vulnerabilities. An impact could go deep enough to damage public image, open up windows of potential litigations, cause significant operational disruptions or monetary damages, or any combination of the above. Mitigating or minimizing the impacts thus becomes a high priority. This can be achieved by careful selection and placement of control elements based on the criticality of a system. The criticality of a system is directly proportional to the impact a security compromise can cause:

$$\text{Criticality} \propto \text{Impact}$$

The magnitude of an impact depends on the depth of the security breach compromising one or more of the three security goals: Confidentiality, Integrity, and Availability. Clearly, a sound approach for impact determination takes all three security goals into account. Interviewing business users and system owners as well as studying system requirement documentation and use cases are some key methods used to assess impacts. As an example, if the business users' tolerance towards a system outage is very low and the loss of availability directly affects the organization's primary business functions, then the system undoubtedly becomes a high-impact, highly critical system. In most utilities, the Energy Management System (EMS) and Distribution Management System (DMS) are considered highly critical systems. Similarly, if a business function requires very high quality data and an integrity compromise is unacceptable, then the system belongs to the highly critical category. On the other hand, if a system's unavailability or a moderate loss of its data integrity does not adversely affect business operations, then the system can be placed in the medium or low criticality level. System criticality may also fluctuate based on the impact of an information leak to business operations. As such, the higher the confidentiality of a system's data, the higher the system criticality or impact level is.

Table 5-1 provides a guideline that could be used for criticality assignment. However, a more quantitative criticality assessment approach was used for this risk assessment effort and is covered in the following section.

Criticality Level	Result of Security Breach
Very High	Significant monetary damage, Compromised consumer privacy, Loss of important business operation for a long period, National level damage to the company reputation, Years of litigation
High	Consumers opting out of SmartGrid programs, Loss of large sums of money, Stained public image, Penalties by regulating authorities, Temporary loss of important business operation, Regional level damage to company reputation
Medium	Few hours loss of operations, Some loss of public trust, Inquiry from monitoring authorities, Localized level damage to company reputation
Low	Loss of business operations, Some damage to company reputation, Monitoring authorities attention, Strained consumer relationship
Very Low	Consumer complaints, Minor loss in productivity due to unavailability or data corruption

Table 5-1 Example Criticality Assignment Guideline

5.1 IMPACT ASSESSMENT APPROACH

The key to a successful impact assessment is development of a good approach to quantify the impact magnitude. The approach should result in a relative impact rating for each system, which can be used later to assess the relative risk level of the system. It is prudent to understand that the quantifying process requires the evaluators to make a sound qualitative judgment at some point in the analysis.

The security goal of confidentiality is the first such qualitative judgment, which can be converted into a numerical assignment as shown in the following table, Table 5-2. A straightforward way to judge the confidentiality of the data is to look at its sensitivity and the impact a leak will have on KCP&L's image and operations. Any system that processes information such as KCP&L's trade secrets, operational security, and consumer privacy should be considered highly sensitive. A system could be considered moderately sensitive if the data it owns could not be used by a threatening entity to compromise KCP&L's image and operations. A system that stores or processes data that is usually available in the public domain can be placed in relatively low sensitivity category.

Confidential / Sensitive Data Examples	Impact Level	Impact Numerical Assignment
KCP&L Trade Secrets (Delta Production Cost), Consumer Private Data (Social Security Numbers)	Very High	10
Financial Data (billing), Consumer Data (Credit Card Numbers, Bank Account Numbers)	High	8
Customer Usage Data, Control Signals	Medium	6
Equipment Location, Telemetry Data	Low	4
KCP&L Internet Site (Generic Outage Data)	Very Low	2

Table 5-2 Confidentiality Impact Level Definitions

The impact of an *integrity* compromise can be best assessed by looking at the cost of a security breach. A formula to assess the cost of an integrity compromise can be expressed as:

$$Cost(i) = (Number\ of\ work\ hours\ spent\ on\ a\ f(x) \times (Hourly\ rate)$$

In a simple scenario, an integrity compromise event results in ten operations and IT engineers spending a ten-hour day to fix the issue. If they are all paid at a rate of $100 per hour, the total cost would be $10,000. This cost could increase exponentially if the solutions are hosted at vendor sites and may require expensive specialized resources to resolve.

Table 5-3 can be used to quantify a system's integrity impact based upon the cost per day to resolve an integrity compromise.

Cost (i) per day	Impact Level	Impact Numerical Assignment
i > $100,000	Very High	10
$50,000 < i < $100,000	High	8
$10,000 < i < $50,000	Medium	6
$1,000 < i < $10,000	Low	4
i < $1,000	Very Low	2

Table 5-3 Integrity Impact Level Definitions

The impact of a security event affecting the availability (third security goal) of a system can be best assessed by calculating the overall cost caused by system unavailability. The cost calculation can be expressed as:

$$Cost(a) = Lost\ Productivity\ Cost + Lost\ Opportunity\ Cost + Cost\ of\ Lost\ Business\ Image + Increased\ Business\ Cost$$

In a scenario where the system unavailability results in twenty engineers losing productivity for a day, parts of power distribution being managed through manual processes, power being supplied through expensive routes (examples include turning on higher cost units or overusing power lines resulting in congestions), and customers losing power for an undefined amount of time, the total cost could easily reach hundreds of thousands of dollars. Since the intent of this report is to identify the relative IT risk level of each system, a complete economic impact assessment is out of scope. However, using the established Disaster Recovery (DR) priority list at KCP&L as an aide, an assessment can be made regarding the relative importance of systems based upon operational area similarities.

Table 5-4 provides the method to quantify each system's availability impact level with respect to the acceptable length of system unavailability.

Acceptable unavailability duration (Time)	Impact Level	Impact Numerical Assignment
1 to 60 minutes	Very High	10
1 Hour to 4 Hours	High	8
4 Hours to 12Hours	Medium	6
12 Hours to 48 hours	Low	4
Greater than 48 Hours	Very Low	2

Table 5-4 Availability Impact Level Definitions

Once the numerical assignment for each security goal is completed for each system, the criticality level is calculated by averaging the assigned impact numbers:

$$Criticality\ Level = \frac{Confidentiality\ Impact + Integrity\ Impact + Availability\ Impact}{3}$$

5.2 IMPACT ASSESSMENT

The following subsections include the relative impact assessment of each planned system in the KCP&L SmartGrid Demonstration Project.

5.2.1 AMI Head-End (AHE)

AHE will be processing control signals such as meter reads, connect/disconnect commands, and demand response (DR) signals. It will also be the hub for the collection of customer usage data, which affects billing. The impact of a confidentiality breach of such data was found to be High (8). A breach resulting in the release of several hundred consumers' usage data collectively will have a high negative impact on KCP&L's reputation. Since AHE is planned to be hosted and managed externally to KCP&L, the impact

of an integrity issue was found to be High (8). The primary contributing factor for this rating was the fact that any integrity fix will require a combination of internal (IT, Operations) and external (vendor) resources. Since the MTRs can store several days of usage data and the other communication between the AHE and the MTRs is not critical to overall operations, an unavailability of AHE for 4 to 12 hours (Medium - 6) was found to be acceptable.

5.2.2 AccountLink (ALNK)

Since ALNK is the repository of consumer financial data, any confidentiality breach could be very damaging to KCP&L's reputation. The confidentiality compromise in this application was thus assigned a High (8) value. Since the code and services are managed in-house, the integrity fix cost was determined to be Medium (6). The SMEs verified that any unavailability exceeding one hour may affect thousands of monetary transactions. Thus, ALNK was given a High (8) availability impact level.

5.2.3 Building Management System (BMS)

Since the BMS control signals only convey the DR signals, the confidentiality of this data was determined to be Low (4). The integrity factor, however, belonged to the Medium (6) category as any malicious modification to the control signals could discourage DR participation by larger consumers. The unavailability of a single instance of BMS would not affect KCP&L operations; thus, the impact was determined to be Low (4).

5.2.4 Customer Information System (CIS)

The CIS manages all aspects of KCP&L's relationship with its customers including the storage of sensitive information such as customer Social Security Number (SSN), bank account numbers, and credit card numbers. Any leak of such information will likely greatly decrease KCP&L's credibility and its consumers' trust level. The confidentiality impact was thus determined to be Very High (10). The cost of fixing an integrity issue in CIS was estimated to be Low (4) as the technology is well known and does not require highly technical resources. The availability of CIS is the highest priority according to the KCP&L IT disaster recovery plan. As such, the unavailability factor assigned to CIS for this assessment was Very High (10).

5.2.5 Distributed Control and Data Acquisition (DCADA)

Since the DCADA system primarily manages information that relates to energy distribution point-in-time, a leak of this information does not affect the confidentiality of the system. The resultant confidentiality factor was determined to be Low (4). The DCADA applications are designed to manage single instance

integrity issues. An integrity compromise; however, may require the time of skilled resources only if the issue is persistent over several cycles. As a result, the integrity impact factor for DCADA was determined to be Medium (6). The DCADA application will be the primary application to manage Midtown Substation. Its unavailability will cause operations to shift from automated to either manual or a less controlled mode. The resultant unavailability impact factor was estimated to be High (8).

5.2.6 Distributed Energy Resources – Commercial & Industrial (DER – C&I)

The DER - C&I are customer installations; a leak of information about these DERs will not have any effect on the confidentiality according to KCP&L. The confidentiality factor was therefore estimated to be Low (4). Similarly, an integrity issue at the customer end does not affect KCP&L. Thus, the integrity impact factor was also determined to be Low (4). The unavailability of a single customer's DER has minimal impact on KCP&L operations. However, if multiple customers' DER are out of commission, then the DR program can get paralyzed. Still, the overall impact was determined to be Low (4).

5.2.7 Distributed Energy Resources (DER – Grid-Connected)

The battery and other similar grid-connected DER do not contain confidential data other than configuration data, which would cause a relatively low impact should there be a data leak. The confidentiality impact factor was thus given a rating of Low (4). However, any integrity compromise will require expensive vendor resources to fix or rectify. Thus, the integrity impact factor was determined to be Medium (6). Unavailability of the battery would remove a large, inexpensive DER from the grid, but the impact will still be small relative to other systems, making the unavailability factor Low (4).

5.2.8 Distributed Energy Resource Management System (DERM)

The DERM is one of the key systems in the KCP&L SmartGrid project, as the overall success of the project is quite dependent on its secure deployment. The data and control signals generated by DERM were determined not to be sensitive in nature. Thus, the confidentiality rating was determined to be Low (4). However, an integrity issue could get costly as the fix would involve multiple resources from the various vendors (OATI, Tendril, Landis+Gyr), KCP&L, and in some cases, the customers. The resultant integrity factor was estimated to be Very High (10). The unavailability of the DERM could cost KCP&L a loss of DR participation during the time of greatest need (summer peaks). The impact of unavailability during these times could be very high. Unavailability during normal, off-peak business operations will have only a moderate impact. Based on that reasoning, the appropriate rating for unavailability was determined to be High (8).

5.2.9 Distributed Energy Resources – Residential (DER – Residential)

The DER - Residential will be a collection of load curtailment and small storage devices. These devices will not have any sensitive data, which resulted in a confidentiality impact rating of Low (4). A data integrity problem will be an easier fix, but identification could get expensive. Nevertheless, an incorrect or unnecessary load curtailment signal can impact customers in an adverse way. Therefore, an integrity impact rating of Medium (6) was justified. The impact of unavailability of residential DER will be minimal to KCP&L operations. Thus, a rating of Very Low (2) was suitable.

5.2.10 Data Mining and Analysis Tool (DMAT)

The DMAT system analyzes metering data, creates usage patterns, estimates missing metering data, and provides visualization of the analysis. The usage data was estimated to be moderately sensitive (Medium - 6) as the leak of this information may not adversely affect KCP&L or its customers. The system's integrity is also not a big concern as the data integrity issues are corrected by vendor processes. Therefore, a resultant rating of Low (4) was justified. DMAT's unavailability also does not affect KCP&L operations, as this system is not considered mission-critical, thereby resulting in a rating of Low (4).

5.2.11 Distribution Management System (DMS)

The DMS is the main computing resource behind the distribution operations. It does not manage confidential data (thus, the confidentially impact rating was determined to be Low (4)) but an integrity loss has the potential to be detrimental to KCP&L operations. The remedy will likely get expensive depending on the number of hours required and the resulting loss in productivity. Therefore, the impact rating of integrity compromise was determined to be Very High (10). The unavailability of this system will interrupt the automated operations for the length of time associated with a sustained outage. As a result, the suitable rating for unavailability of this system was determined to be Very High (10).

5.2.12 Energy Management System (EMS)

The EMS manages the generation and transmission of bulk energy. As such, the EMS does not contain or manage highly confidential data, but with some effort a knowledgeable attacker could deduce energy cost related data by understanding generation levels and transmission networks. On a confidentiality scale this information was estimated to be Medium (6). The integrity cost however can be Very High (10) depending on the depth of the issues. EMS resources are typically the most expensive, and the amount of time to fix issues can also be on the higher side. The unavailability impact (like the DMS) was also

determined to be Very High (10) as KCP&L operations are largely dependent on applications like the EMS.

5.2.13 Field and Substation Distribution Automation Devices (Field-DADs and Substation DADs)

The Distribution Automation Devices are used to remotely manage the distribution of energy and as such do not contain any sensitive data. For this reason, the confidentiality rating was considered to be Low (4). Since the automation devices operate on point-in-time control signals, an integrity compromise (unless repeated over several cycles) will not cause damage to KCP&L operations. The resultant rating was thus estimated to be Low (4). Individual or localized unavailability of the DADs will likely not affect operations. However, large-scale unavailability could hamper KCP&L distribution operations. For the purposes of the demonstration project, the unavailability impact rating of Medium (6) was more appropriate.

5.2.14 Geographic Information System (GIS)

The data contained in GIS helps designers and planners perform geographical analysis. The data managed inside the GIS system is not considered sensitive from an operational perspective. However, the locations of critical customers like hospitals, fire departments, and police departments are marked on the spatial files. The confidentiality rating was still determined to be Low (4) as most of this information is available in the public domain. An integrity compromise was estimated to be Medium (6) as the fixes are not expensive but the productivity lost due to incorrect field work locations may get high. The SMEs verified that the IT disaster recovery plan allows for six hours of unavailability. This system was thus assigned the unavailability impact rating of Medium (6).

5.2.15 Home Area Network Devices and Gateway (HAND and HANG)

The HAN Devices and Gateway will contain information such as device MAC addresses, installation code, device type, installation date, pair ID, etc. This information, by itself, is not considered sensitive, but if leaked could be manipulated to adversely affect the consumer. The resultant confidentiality impact rating was determined to be Medium (6). The integrity compromise cost, by itself, for these devices was determined to be Low (4); however a data integrity issue propagating into other systems could have a medium to high impact. Lastly, the unavailability impact of these devices for a single consumers or a small number of consumers is going to be low for KCP&L. However, impact could be high for the consumer if the appliances that these devices control become unavailable or malfunction. As a result, the unavailability rating was determined to be Medium (6).

5.2.16 Home Energy Management Portal (HEMP)

The HEMP is the primary interface that the KCP&L SmartGrid consumers will utilize to manage their HAN, participate in DR events, and view their usage. Information like usage data and billing levels has been determined by many consumer groups to be private. A leak of this information will be damaging for KCP&L's reputation and its SmartGrid program. The impact rating of a confidentiality compromise was thus determined to be High (8). The cost of a data integrity fix could be anywhere from low to medium depending on the number of consumers affected by the issue. The impact rating of Medium (6) was thus justified to cover for events that affect large numbers of consumers. Unavailability of HEMP for a few consumers is going to be insignificant. However, mass unavailability will affect many consumers and could result in a large number of complaints and trust issues with KCP&L's SmartGrid program. For this reason, the unavailability impact rating was determined to be High (8).

5.2.17 Meter Data Management System (MDM)

The MDM acts as the repository of meter inventory and individual consumer usage. Because of the sensitivity of the usage information contained in MDM, the most suitable category for this system was High (8). An integrity fix for this application may not get costly unless a large amount of consumer data gets affected, and the duration of the integrity issue is long. The resultant rating for this application was therefore evaluated to be Medium (6). After discussion with the SMEs, it was determined that the unavailability of MDM for up to six hours is not believed to cause major operational impacts. However, an unavailability lasting any longer could result in billing issues. As a result, the appropriate rating determined for MDM was Medium (6).

5.2.18 SmartMeter (MTR)

A breach resulting in an unauthorized entity getting access to the usage data stored in a MTR will be very damaging to the consumer and to KCP&L. Since this type of data is considered private by many consumer groups, it was reason enough to place MTR at High (8) on the sensitivity scale. A data integrity event for one MTR installation will not be costly for KCP&L, however any compromise to the control signals (a false disconnect command being sent for example) could have far-reaching effects. As a result, an integrity impact rating of medium (6) was suitable for this device. One instance of MTR unavailability will have minimal impact on KCP&L, but a large number of MTR outages could easily have a large impact on the KCP&L bottom line. Thus, the unavailability impact rating for MTR was determined to be Medium (6).

5.2.19 Mobile Work Force Management System (MWFM)

MWFM is the system used by the field service dispatchers to solve customer issues that require a technician visit to the site. This type of data was determined to be low in sensitivity and thus, a Low (4) confidentiality impact rating was given. Due to the high number of mobile client installations, the coordination of an integrity fix rollout, coupled with time spent on creating and testing the fix may require a large number of man-hours. Thus, an integrity fix cost for this system was determined to be Medium (6). The unavailability impact rating was determined to be Low (4) as an outage of this system is not considered critical to overall operations. To cover for lengthy outages, KCP&L has backup functionalities that involve manual business processes.

5.3 IMPACT ASSESSMENT RESULTS

Based on the assessment in the previous section, Table 5-5 was created to summarize the results in a tabular format. The table provides a quick view of the relative criticalities of the SmartGrid systems with respect to each other.

System	Confidentiality Impact Level	Integrity Impact Level	Availability Impact Level	Overall Impact Level
AHE	8	8	6	7.33
ALNK	8	6	8	7.33
BMS	4	6	4	4.67
CIS	10	4	10	8.00
DADs (Field & Substation)	4	4	6	4.67
DCADA	4	6	8	6.00
DER – C&I	4	4	4	4.00
DER – Grid-Connected	4	6	4	4.67
DER – Residential	4	6	2	4.00
DERM	8	10	8	7.33
DMAT	6	4	4	4.67
DMS	4	10	10	8.00
EMS	6	10	10	8.67
GIS	4	6	6	5.33
HAND/HANG	6	4	6	5.33
HEMP	8	6	8	7.33
MDM	8	6	6	6.67
MDS	8	6	6	6.67
MWFM	4	6	4	4.67

Table 5-5 Impact Assessment Results

A summary of the relative criticality results is graphically represented in Figure 5-1, where each system is placed in the Low, Medium or High region.

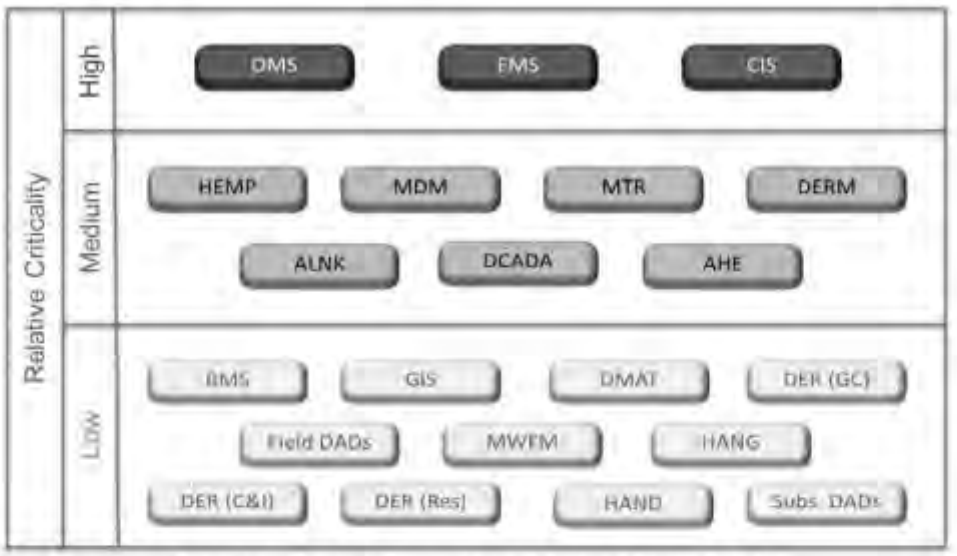


Figure 5-1 Graphical Representation of Relative Criticality Results

6.0 EXISTING MITIGATION

As described in the risk assessment model, the identification of existing controls (mitigation) plays an important role in evaluating the overall risk rating of the systems. To identify the existing controls several mechanisms are used, these include: interviewing the security implementation team, reviewing system documentation, and studying organization policies and procedures. The identification and analysis can then be used to create a method to quantify the mitigation and which can be used in the risk rating model.

6.1 MITIGATION ANALYSIS ASSUMPTIONS

This mitigation analysis relies heavily on the existing KCP&L policies, processes and the standards. Two assumptions are made while this assessment was conducted. First, all security requirements mandated in the said documents are enforced and are fully implemented in all existing and new systems at KCP&L. Second, all requirements mentioned in these documents are also mandated to the vendors for implementing (at the minimum) similar controls to KCP&L systems hosted by them.

6.2 MITIGATION ANALYSIS TECHNIQUE

The mitigation analysis technique consisted of a series of methodical steps. First, all data transfer interfaces between SmartGrid systems were identified. The interface scope included all interfaces that were planned or existed (at the time this risk assessment was performed) however limited to and/or from the SmartGrid systems. Second, all identified interfaces were mapped to one of the twenty-two NISTIR-7628 Volume-1 defined logical interface categories. This task was performed in collaboration with the KCP&L SMEs (the results of the mapping are provided in Appendix B). In the next step, controls recommended in the NISTIR-7628 Volume-1, UCAIug AM1, and the UCAIug DM Security Profiles were identified for each applicable interface category. As the final step, the identified controls were compared to the requirements that are mandated by KCP&L policies, standards, and processes for all new and existing systems. A control was considered "fulfilled" if there was a close match between the NISTIR control and the KCP&L requirement. The matching process resulted in a set of security controls that are applicable to SmartGrid systems and their implementation mechanisms already exist at KCP&L.

6.3 MITIGATION ANALYSIS RESULTS

It was determined that only thirteen of the twenty-two interface categories were applicable to KCP&L SmartGrid implementation. And based on the applicable categories, one hundred eighty-one out of one hundred ninety-seven (total recommended security controls in the NISTIR-7628) were found to be applicable to the project. Appendix D lists the applicable security requirements, along with the page

number(s) that each is defined on in the NISTIR-7628 Volume-1. The comparison of the applicable controls with the requirements in the KCP&L's policies, standards, and/or processes, confirmed that ninety-three of the one hundred eighty-one were mandated.

Table 6-1 lists the total number controls recommended by NISTIR-7628 Volume-1 and of that total, the number of controls currently mandated by KCP&L. These controls are grouped together by the NISTIR defined control families.

NISTIR-7628 SmartGrid Control Family	Total Number of Controls in each NISTIR 7628 Control Family	Number of Controls Mandated by the KCP&L Policies, Standards, and/or Processes
Access Control (SG.AC)	21	16
Awareness and Training (SG.AT)	7	5
Audit and Accountability (SG.AU)	16	4
Security Assessment and Authorization (SG.CA)	6	2
Configuration Management (SG.CM)	11	10
Continuity of Operations (SG.CP)	13	9
Identification and Authentication (SG.IA)	6	5
Information and Document Management (SG.ID)	5	4
Incident Response (SG.IR)	11	10
Smart Grid Information System Development and Maintenance (SG.MA)	7	5
Media Protection (SG.MP)	6	6
Physical and Environmental Security (SG.PE)	12	0*
Planning (SG.PL)	5	3
Security Program Management (SG.PM)	8	5
Personnel Security (SG.PS)	9	6
Risk Management and Assessment (SG.RA)	6	5
Smart Grid Information System and Services Acquisition (SG.SA)	11	10
Smart Grid Information System and Communication Protection (SG.SC)	30	7
Smart Grid Information System and Information Integrity (SG.SI)	9	5

Table 6-1 Fulfilled NISTIR-7628 Security Requirements by Family

*- The physical security requirements in the NISTIR-7628 are not currently mandated in KCP&L policies, standards, and processes for any of the systems except for the EMS. In the case of EMS, it is believed that all 12 physical security requirements are currently mandated by KCP&L. For more information regarding how the mitigation ratings were calculated for both EMS and all other systems, see section 6.4, Table 6-2, and Table 6-3

6.4 MITIGATION EVALUATION

The method developed to quantify the Mitigation takes into account the NISTIR-7628 listed security controls believed to be implemented for all systems at KCP&L, as well as the Impact, Likelihood and Vulnerability ratings calculated for each system.

The Mitigation calculation for each system can be expressed as:

$$M = (a \times I) + (b \times L) + (c \times V)$$

Where:

a is the Impact Coefficient

I is the Impact Rating

b is the Likelihood Coefficient

L is the Likelihood Rating

c is the Vulnerability Coefficient

V is the Vulnerability Rating

The coefficients are a numerical representation of the number of controls that are specifically put in place by KCP&L to minimize impacts, decrease likelihoods, or guard vulnerabilities. The Impact Coefficient ("a") was determined to be 0.627, which represents the 62.7% of the impact minimizing requirements that are believed to be implemented for all systems at KCP&L. The Likelihood Coefficient ("b") was calculated to be 0.650, which represents the 65.0% of the likelihood decreasing requirements covered by KCP&L policies, procedures, and standards. Similarly, the Vulnerability Coefficient ("c") was calculated to be 0.533, representing the 53.3% of the requirements that specifically address the protection of system vulnerabilities. Thus, the mitigation equation becomes:

$$M = 0.627I + 0.650L + 0.533V$$

To determine the percentages and eventually the coefficients, each of the NISTIR-7628 control families were first assigned a primary purpose: Minimize Impact, Decrease Likelihood, or Guard Vulnerability. The requirements (within each family) that are mandated by KCP&L were then counted, and a percentage was calculated using the total number of requirements in each NISTIR-7628 control family as a basis.

Table 6-2 shows the total requirements for each control family, the number of requirements in each currently mandated by KCP&L , and the calculated percentages for the three coefficients.

NISTIR-7628 SmartGrid Requirement Family	Total Number of Controls in each NISTIR 7628 Control Family	Number of Controls Fulfilled by KCP&L Policies, Standards, and/or Processes	Affect Assignment	Affect Coefficient
Audit and Accountability (SG.AU)	16	4	Impact	0.627
Continuity of Operations (SG.CP)	11	9	Impact	
Information and Document Management (SG.ID)	5	4	Impact	
Incident Response (SG.IR)	11	10	Impact	
Smart Grid Information System Development and Maintenance (SG.MA)	7	5	Impact	
Smart Grid Information System and Information Integrity (SG.SI)	9	5	Impact	
Awareness and Training (SG.AT)	7	5	Likelihood	0.650
Planning (SG.PL)	5	3	Likelihood	
Security Program Management (SG.PM)	8	5	Likelihood	
Access Control (SG.AC)	21	16	Vulnerability	0.5333
Security Assessment and Authorization (SG.CA)	6	2	Vulnerability	
Configuration Management (SG.CM)	11	10	Vulnerability	
Identification and Authentication (SG.IA)	6	5	Vulnerability	
Media Protection (SG.MP)	6	6	Vulnerability	
Physical and Environmental Security (SG.PE)	12	0*	Vulnerability	
Personnel Security (SG.PS)	9	6	Vulnerability	
Risk Management and Assessment (SG.RA)	6	5	Vulnerability	
Smart Grid Information System and Communication Protection (SG.SC)	30	7	Vulnerability	
Smart Grid Information System and Services Acquisition (SG.SA)	11	10	N/A	N/A

Table 6-2 Determination of Mitigation Equation Coefficients

* - A vulnerability coefficient of 0.645 was used to calculate the mitigation rating for EMS. The value of 0.645 was calculated based upon the belief that all 12 physical security requirements from the NISTIR-7628 are currently mandated by KCP&L for the EMS. Currently, KCP&L policies, standards, and processes do not mandate the same level of physical security for the other assessed systems. As implementation of SmartGrid technologies progresses from demonstration to enterprise-wide deployment, the physical security controls mandated by KCP&L policies, standards, and processes will need to be extended to include the other assessed systems to achieve a balanced security profile.

Table 6-3 provides the mitigation values determined for each of the KCP&L SmartGrid System.

System	Relative Vulnerability (V) Rating	Highest Likelihood (L) Rating	System Impact (I) Rating	Combined Mitigation (M) Rating*
AHE	6	8	7.33	13.00
ALNK	8	10	7.33	15.36
BMS	5	4	4.67	8.19
CIS	6	8	8.00	13.41
DADs	5	6	4.67	9.49
DCADA	5	6	6.00	10.33
DER – C&I	5	6	4.00	9.07
DER – Grid-Connected	5	6	4.67	9.49
DER – Residential	7	6	4.00	10.14
DERM	7	6	7.33	12.25
DMAT	5	6	4.67	9.49
DMS	4	8	8.00	12.35
EMS	4	10	8.67	14.07 + 0.44**
GIS	5	6	5.33	9.91
HAND/HANG	8	8	5.33	12.81
HEMP	8	10	7.33	15.36
MDM	5	6	6.67	10.75
MTE	8	10	6.67	14.94
MWFM	4	6	4.67	8.96

Table 6-3 Mitigation Rating for Systems

* - The maximum possible value of 30 for Combined Mitigation Rating is obtained if all security requirements are implemented to guard vulnerabilities, decrease likelihoods, and minimize impacts.
** - The Combined Mitigation Rating for EMS was calculated to be 14.51 (the sum of 14.07 and 0.44) using a vulnerability coefficient of 0.645. The value of 14.07 corresponds to the Combined Mitigation Rating for the EMS if none of the physical security requirements from the NISTIR-7628 were being mandated by KCP&L (i.e. using a vulnerability coefficient of 0.533). See note below Table 6-2 for additional information.

7.0 RISK DETERMINATION

The purpose of this step is to assess the level of risk to the IT system. The determination of risk for a particular threat/vulnerability pair can be expressed as a function of:

- The likelihood of a given threat-source's attempting to exercise a given vulnerability.
- The magnitude of the impact should a threat-source successfully exercise the vulnerability.
- The adequacy of planned or existing security controls for reducing or eliminating risk.[7]

The ultimate goal of a risk assessment is to determine the relative risk of all systems within the scope of the assessment. The risk rating model used in this assessment evaluates all the SmartGrid systems in the environment using common criteria in order to provide a scaled risk value for each. Since each system was evaluated using the same criteria, the resulting risk ratings may be used to prioritize mitigation actions.

There are many kinds of risk which may require different kinds of response or mitigation. For example, reliability risk to a substation would be given a different priority than reputational risk to the corporate website. Some examples of different types of risk are:

- Operational Risk: Risk that directly concerns the functions or operational state of systems
- Reliability Risk: Risk that directly impacts the local or regional reliability of power systems
- Financial Risk: Risk of lost revenue or reduced profit
- Reputational Risk: Risk of damage to corporate reputation or public goodwill
- Compliance Risk: Risk of failing to meet regulatory requirements

7.1 RISK-RATING MATRIX

The model used in this report to evaluate system risk is described in the Introduction section and referenced throughout the report. Values for the criteria used in the risk rating model have been evaluated and described earlier in this report. For each system, existing mitigating controls reduce the calculated risk rating in order to arrive at the Overall Risk Rating value. The output of those evaluations and calculations has been entered into Table 7-1 which shows the Overall Risk Rating for each system.

[7] U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology, *Special Publication 800-30: Risk Management Guide for Information Technology Systems*, July 2002

System	Threat Rating (T)	Relative Vulnerability Rating (V) ↓	Highest Likelihood Rating (L) ↓	System Impact Rating (I) ↓	Combined Mitigation Rating (M) ↑	Overall Risk Rating (R)
AHE	8	6	8	7.33	13.00	**16.34**
ALNK	8	8	10	7.33	15.36	**17.97**
BMS	7	5	4	4.67	8.19	**12.48**
CIS	7	6	8	8.00	13.41	**15.59**
DADs (Field & Substation)	6	5	6	4.67	9.49	**12.18**
DCADA	8	5	6	6.00	10.33	**14.67**
DER - C&I	6	5	6	4.00	9.07	**11.93**
DER – Grid-Connected	6	5	6	4.67	9.49	**12.18**
DER - Residential	6	7	6	4.00	10.14	**12.86**
DERM	6	7	6	7.33	12.23	**14.10**
DMAT	5	5	6	4.67	9.49	**11.18**
DMS	8	4	8	8.00	12.35	**15.65**
EMS	8	4	10	8.67	14.51	**16.15**
GIS	7	5	6	5.33	9.91	**13.42**
HAND/HANG	6	8	8	5.33	12.81	**14.53**
HEMP	7	8	10	7.33	15.36	**16.97**
MDM	5	5	6	6.67	10.75	**14.92**
MTR	8	8	10	6.67	14.94	**17.72**
MWFM	7	4	6	4.67	8.96	**12.71**

Table 7-1 Risk Rating Matrix

↓ - Denotes that lowering the component rating will lower the Overall Risk Rating
↑ - Denotes that raising the component rating will lower the Overall Risk Rating

7.2 RISK DETERMINATION

The calculated values for the Overall Risk Rating can be used to assist with prioritizing mitigation actions. An established level of acceptable risk must be determined for each individual system based on operational and business-level factors. These risk ratings will change over time and should be re-evaluated regularly in order to recalculate each system's overall risk.

To further prioritize mitigation actions, it was necessary to calculate a high-level estimate of effort necessary to mitigate each system. This estimate was based solely upon environmental considerations for each system; physical location, operating system, availability of updates, etc. The rating uses the criteria listed in Table 7-2 to calculate the estimate of effort required to apply mitigations to each system. The maximum value for the estimated mitigation effort is 10. With some SmartGrid systems still in the planning phases, and considering the complexity of the environment, certain aspects of the mitigation effort criteria have been estimated based on information gained during personal interviews. For example, the "No Remote Administration" criterion was only applied if that information was specifically identified for a particular system. Similarly, for systems hosted remotely, criteria were assigned based on

conversations and questionnaire responses. The criteria were carefully evaluated, however, it is possible that some criteria were missed, or have been incorrectly assigned.

Criteria #	Criteria	Effort Rating Modifier
1	System Hosted Locally	+1
2	System Hosted Remotely	+2
3	System Located at Customer or Field Location(s)	+3
4	Windows Operating System or applications	+1
5	Unix-based Operating System or applications	+1
6	Proprietary Operating System or Applications	+2
7	No Remote Administration	+2
8	No Regularly Scheduled Updates	+1
9	Public Access to System	+2
10	Greater than 20 Devices in System	+1
11	Virtual Server	+1
12	Unsupported Operating System	+2
13	System Contains PII	+1

Table 7-2 Mitigation Effort Criteria

Table 7-3 assigns estimated mitigation effort values to each KCP&L SmartGrid system within the scope of this assessment.

System	System ID	Assigned Mitigation Effort Criteria	Estimated Mitigation Effort
AHE	1	2, 4, 11	4
ALNE	2	1, 4, 9, 11, 13	6
BMS	3	3, 9	5
CIS	4	1, 5, 13	3
DADs (Field & Substation)	5	3, 6, 8, 10	7
DCADA	6	1, 6, 7, 8, 10	7
DER – C&I	7	3, 6, 8	6
DER – Grid-Connected	8	1, 6, 8	4
DER – Residential	9	3, 6, 8, 9	8
DERM	10	2, 6	4
DMAT	11	2, 6	4
DMS	12	1, 4	2
EMS	13	1, 4	2
GIS	14	1, 5, 8	3
HAND/HANG	15	3, 6, 8, 9, 10	9
HEMP	16	2, 5, 9, 13	6
MDM	17	2, 4,	3
MTB	18	3, 6, 7, 8, 10	9
MWFM	19	3, 6, 8, 10, 13	8

Table 7-3 Estimated Mitigation Effort for SmartGrid Systems

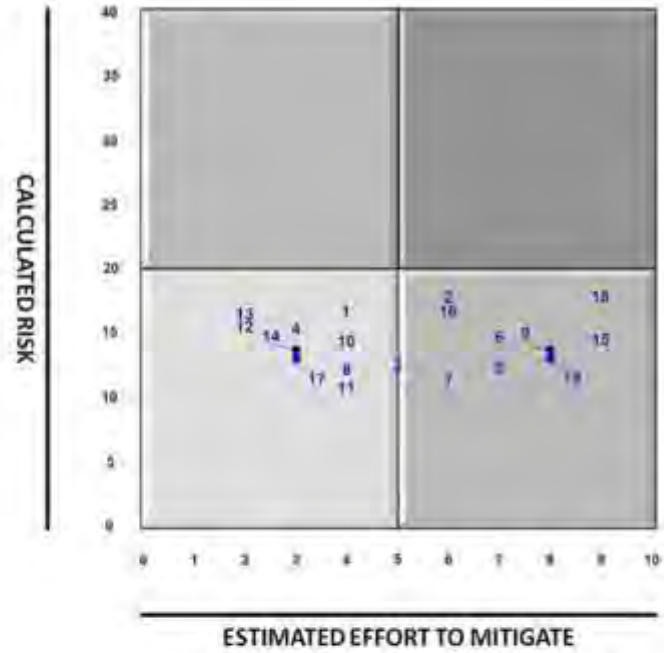
As stated in the Introduction, the most common action which can be taken in response to an evaluated threat is mitigation. The goal of applying mitigating security controls to systems is to reduce the level of

risk by eliminating vulnerabilities, or lessening the likelihood or impact of a threat exploiting vulnerabilities.

Figure 7-1 illustrates the distribution of KCP&L's SmartGrid systems within the risk rating and mitigation effort values. Each system was assigned a numeric identification number in Table 7-3, which is used to represent that system in Figure 7-1.

The first step in planning risk mitigation is to prioritize which systems and controls will be implemented first. When planning mitigations, reducing the risk of all systems should be a goal, but using Figure 7-1 as a guide, mitigations for each system can be prioritized to focus on those systems most at risk first, while still working to reduce the overall risk to all systems. Section 8.0 provides more risk mitigation recommendations and details.

Although the Risk Rating values can be used to prioritize mitigation actions, there is no ideal or static target Risk Rating. Since environments are always changing, new threats are always emerging, and new vulnerabilities are discovered every day, system risk is not a static point. Therefore, mitigation actions must not be static either. Risk must be regularly re-evaluated to ensure newly implemented mitigations and controls are functioning as expected, and new threats or vulnerabilities have not increased system risk.



System ID	System
1	AHE
2	ALMC
3	BMS
4	CIS
5	DADs (Field & Substation)
6	DCADA
7	DER - C&I
8	DER – Grid-Connected
9	DER - Residential
10	DERM
11	DMAT
12	DMS
13	EMS
14	GIS
15	HAND HANG
16	HEMF
17	MDM
18	MTR
19	MWFM

Figure 7-1 Risk Rating Categories

As shown in Figure 7-2, Risk Management is not a one-time process but rather a cycle of continuous improvement.

Figure 7-2 Risk Management Cycle

This report is the conclusion of the Assessment Phase of the cycle. In the Mitigation Phase, policy, procedure, and technical controls are implemented to reduce the factors of vulnerability, impact, or likelihood. In the Educate Phase, management, administrators, users, and customers are trained in or informed of the new controls, how they operate, and why they are in place. In the Evaluate Phase, the new controls are reviewed and monitored to assure they both function as expected and do not introduce any unexpected vulnerability.

8.0 RISK MITIGATION

The completion of a risk assessment should result in a set of actionable mitigation steps that can be taken by the organization to make its systems secure. The mitigation recommendations provided in this section are specific to the SmartGrid project at KCP&L and are primarily driven by the results from the end-to-end risk assessment. The KCP&L SmartGrid Trust Model[9] was also used as an important reference while creating these mitigation recommendations. The KCP&L Trust Model domains (*Secured, Restricted, Controlled,* and *Uncontrolled*) were used to develop recommended security zones for KCP&L SmartGrid systems and to determine the security controls for data stored and/or generated by the systems. The Trust Model transport classes (*Trusted, Managed,* and *Public*) were used to determine the security controls for data transmitted between systems.

The mitigation recommendations resulting from the risk assessment fall into one of the following two types of security control implementations:

Creation of Security Zones and Implementation of Tailored Control Sets: A security zone is defined as a group of SmartGrid systems that have the same criticality level and perform similar business functions. A tailored control set is a collection of security requirements that are applicable to all systems in a security zone or to all interfaces between two security zones.

Implementation of Industry-Suggested Control Sets: An industry-suggested control set is a subset of the NISTIR-7628 Volume-1 security requirements that are applicable to a SmartGrid system based upon its interfaces.

Detailed descriptions of both security control implementations are covered in the following subsections.

8.1 CREATION OF SECURITY ZONES AND IMPLEMENTATION OF TAILORED CONTROL SETS

This type of security control implementation includes a collection of security controls specifically tailored for the SmartGrid project based upon security zones and interfaces between security zones. As mentioned above, each security zone includes SmartGrid systems that have the same criticality level and perform similar business functions. The goal of this implementation is to recommend controls that will bring high risk systems down to medium risk and adequately protect the systems based on their impact levels. As

[9] KCP&L Green Impact Zone SmartGrid Demonstration, *SmartGrid Cyber Security Plan*, Version v1.0 - November 18, 2010

such, the selection of controls in this type of implementation is also based on the risk and impact ratings calculated for each system as part of the end-to-end risk assessment.

8.1.1 Security Zones

First, the SmartGrid systems are placed into cyber security zones. This placement should be based upon the criticality of the system and the business function it performs. The eight security zones that are recommended are as follows:

8.1.1.1 Energy Operations - High

The primary purpose of this group of systems is energy management. All systems belonging to this zone are highly critical. These systems also belong to the *Secured* KCP&L Trust Model domain. In addition, all interfaces receiving or sending data to or from this security zone belong to the *Trusted* transport class within KCP&L's Trust Model.

8.1.1.2 Distribution Operations - High

All highly critical systems that contribute towards the function of distribution management reside in this security zone. The *Secured* KCP&L Trust Model domain will be applicable to this zone, while the interfaces will be in the *Trusted* transport class.

8.1.1.3 Customer Operations - High

Systems included in this zone are also highly critical, but their primary function is customer management. These systems fall under the *Secured* domain in the KCP&L Trust Model, while its interfaces belong to the *Trusted* transport class.

8.1.1.4 Distribution Operations - Medium

Systems in this security zone have the primary function of distribution management; however, their criticality level is medium. The KCP&L Trust Model domain applicable to this zone is the *Restricted* domain. The zone interfaces belong to either the *Trusted* or *Managed* transport classes.

8.1.1.5 Delivery Operations – Medium

This group of systems performs the function of energy delivery, yet all its systems are all moderately critical to overall operations. These systems are within the *Restricted* KCP&L Trust Model domain, while their data interfaces fall under the *Trusted* or the *Managed* transport classes.

8.1.1.6 Customer Operations – Medium

All systems whose criticality to the organization is moderate and whose primary functionality is customer-facing business operations fall within this security zone. The applicable KCP&L Trust Model domain for this security zone is the *Restricted* domain. As with the other moderately critical security zones, the interfaces in this zone belong to either the *Trusted* or *Managed* transport classes.

8.1.1.7 Distribution Operations – Low

This security zone should house systems that are part of the distribution network but only the ones whose criticality is determined to be low. These systems belong to the *Controlled* domain in the KCP&L Trust Model. The interfaces for the systems in this security zone belong to the *Managed* transport class.

8.1.1.8 Deliver Operations – Low

Systems in this security zone have low criticality and solve the business function of servicing or supporting field issues. Systems from this security zone reside in the *Controlled* domain, while their interfaces belong to the *Managed* transport class within the KCP&L Trust Model.

8.1.1.9 Customer Operations – Low

All systems that are owned and managed by KCP&L customers belong to this security zone. Since KCP&L has little to no control over these systems, the Trust Model domain assigned to this zone is *Uncontrolled*. The interfaces for these systems are mainly located at customer premises, and as such, the transport class most suitable is the *Public* class.

Table 8-1 lists the recommended security zone for each SmartGrid system.

System	Security Zone
AHE	Delivery Operations – Medium
ALNE	Customer Operations – Medium
BMS	Customer Operations – Low
CIS	Customer Operations – High
DCADA	Distribution Operations – Medium
DER - C&I	Customer Operations – Low
DER – Grid-Connected	Distribution Operations – Low
DERM	Distribution Operations – Medium
DER - Residential	Customer Operations – Low
DMAT	Delivery Operations – Low
DMS	Distribution Operations – High
EMS	Energy Operations – High
Field DADs	Distribution Operations – Low
GIS	Delivery Operations – Low
HAND	Customer Operations – Low
HANG	Customer Operations – Low
HEMP	Customer Operations – Medium
MDM	Delivery Operations – Medium
MTR	Delivery Operations – Medium
MWFM	Delivery Operations – Low
Substation DADs	Distribution Operations – Low

Table 8-1 Security Zone Recommendations for SmartGrid Systems

Figure 8-1 provides a graphical view of the recommended security zones.

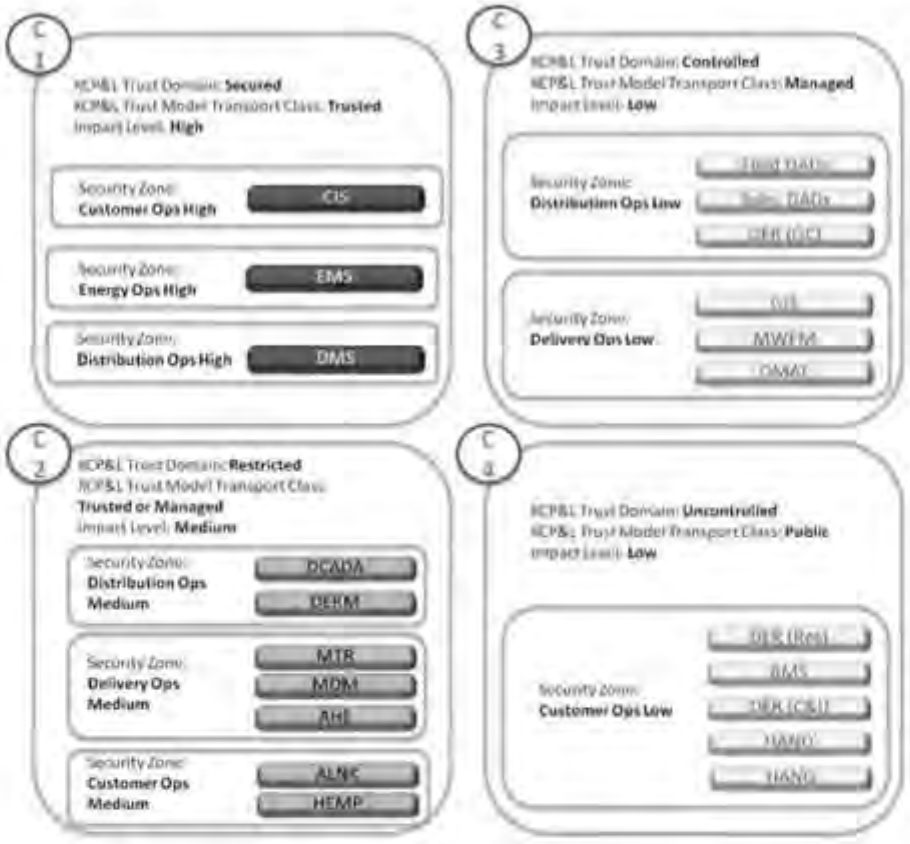


Figure 8-1 Representation of SmartGrid Systems in Respective Security Zones

8.1.2 Tailored Control Sets

Second, security control sets are created that tailor to the security zones and interfaces between them. Each control set is a collection of security requirements from the NISTIR-7628 Volume-I as well as many of the ones included in the UCA International Users Group (UCAIug)[16] AMI and DM Security Profiles. The security requirements in each set are also determined based upon the risk and impact ratings calculated for the SmartGrid systems as part of the risk assessment. Following is the definition of each control set and its applicability in the SmartGrid project.

[16] UCA International Users Group http://www.ucaiug.org/default.aspx

8.1.2.1 Control Set – C0

The control set C0 represents security requirements that are common to all security zones (except *Customer Operations – Low*) and the interfaces between any two security zones.

8.1.2.2 Control Set – C1

This set represents common requirements for systems that belong to one of the high impact security zones. This control set is also applicable to all data transfers within the high impact security zones. That is, any system that is part of *Customer Operations – High*, *Distribution Operations – High*, or *Energy Operations – High* should be implemented with C0 and C1.

8.1.2.3 Control Set – C2

This control set is specifically chosen for systems that belong to one of the medium impact security zones. As such, any system that has been placed in *Delivery Operations – Medium*, *Customer Operations – Medium*, or *Distribution Operations – Medium* should be implemented with control sets C0 and C2. This control set is also applicable to all data transfers within the medium impact security zones.

8.1.2.4 Control Set – C3

This set represents security requirements for low impact systems that are managed by the KCP&L staff. This set, therefore, is only applicable to the systems that are either in the *Distribution Operations – Low* or *Delivery Operations – Low* security zones. This control set is also applicable to all data transfers within the low impact security zones managed by KCP&L. The control sets C0 and C3 should be implemented in conjunction for these zones.

8.1.2.5 Control Set – C4

This set of security requirements is created for KCP&L end customers. The set represents control mechanisms to be suggested to the customers as they manage the *Customer Operations – Low* security zones. This set may not be mandated by KCP&L; however, it is recommended that KCP&L suggest this set to all customers participating in the SmartGrid program. To restate, all systems within the *Customer Operations – Low* security zone need only implement the controls within set C4.

8.1.2.6 Control Set - C5

This set represents the security requirements that are recommended for all interfaces between high impact security zone(s) and medium impact security zone(s). This set should be implemented along with the control set C0.

8.1.2.7 Control Set – C6

All interfaces between high impact security zone(s) and low impact security zone(s) should be implemented with these requirements. The control sets C0 and C6 should be implemented together for all such interfaces.

8.1.2.8 Control Set – C7

This set represents the security requirements that are recommended for all interfaces between medium impact security zone(s) and low impact security zone(s). This set should be implemented along with the control set C0.

8.1.2.9 Control Set – C8

All interfaces between medium impact security zone(s) and the *Customer Operations - Low* security zone should be implemented with these requirements. Note that some of these requirements may need to be fulfilled by the consumers. For the interfaces that involve data being sent to KCP&L from the *Customer Operations - Low* security zone, both control sets C0 and C8 should be implemented.

Figure 8-2 provides a visual representation of the control sets applicable to each security zone and their interfaces. For a list of the NISTIR-7628 security controls that are contained in each control set, see Appendix F.

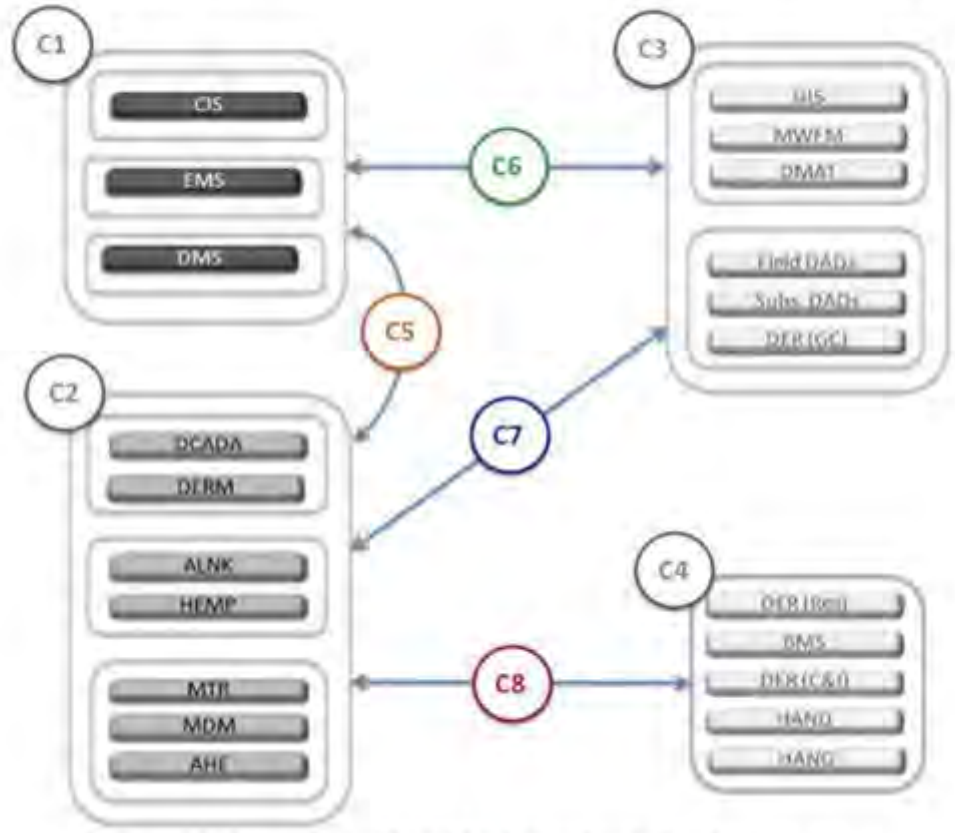


Figure 8-2 Representation of Control Sets for Inter-Security Zone Communication

8.2 INDUSTRY-SUGGESTED CONTROLS

The second type of security control implementation is a collection of controls based on industry best practices and guidelines. This type lists all the controls suggested in the NISTIR-7628 Volume-1[37] based strictly on the applicable Logical Interface Categories and their recommended controls. These security requirements, if implemented to their fullest, should adequately secure the SmartGrid systems. It is worth noting that the controls recommended in the implementation type discussed in section 8.1.2 are a subset of the controls recommended in this type.

[37] NIST Interagency Report 7628 Volume 1. http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf

Table 8-2 provides a summarized listing of the KCP&L SmartGrid systems along with their applicable NISTIR-7628 Logical Interface Categories. A brief definition of each NISTIR Logical Interface Category is available in Appendix A. The table indicates that a majority of the NISTIR-7628 security requirements were found to be applicable to all the SmartGrid systems. To improve readability and act as a quick reference, the table lists requirements in the format "**All** Except... the requirements found not to be applicable."

SmartGrid System	Applicable NISTIR-7628 Logical Interface Categories	Applicable NISTIR-7628 Security Controls*
AHF	5, 13, 14	**All** Except: SG.AC-12, SG.IA-5, SG.SC-4, SG.SC-17
BMS	15	**All** Except: SG.AC-11, SG.AC-12, SG.AU-16, SG.IA-5, SG.SC-4, SG.SC-6, SG.SC-9, SG.SC-17, SG.SC-26, SG.SC-29
CIS	7, 8, 10	All Except: SG.SC-6, SG.SC-9, SG.SC-17
DCADA	1, 2, 3, 5	**All** Except: SG.AC-12, SG.AU-16, SG.SC-4, SG.SC-9, SG.SC-17, SG.SC-26
DER - C&I, DER - Grid-Connected, DER - Residential	18	**All** Except: SG.AC-11, SG.AC-12, SG.AC-14, SG.AU-16, SG.IA-4, SG.IA-5, SG.IA-6, SG.SC-3, SG.SC-4, SG.SC-5, SG.SC-6, SG.SC-7, SG.SC-9, SG.SC-17, SG.SC-26, SG.SC-29, SG.SI-7
DERM	8, 9, 16	**All** Except: SG.SC-6, SG.SC-17, SG.SC-29
DMS	5, 10	**All** Except: SG.AC-12, SG.AU-16, SG.IA-5, SG.SC-3, SG.SC-9, SG.SC-26
EMS	1	**All** Except: SG.AC-12, SG.AU-16, SG.SC-4, SG.SC-6, SG.SC-9, SG.SC-26
Field DADs, Substation DADs	18	**All** Except: SG.AC-11, SG.AC-12, SG.AC-14, SG.AU-16, SG.IA-4, SG.IA-5, SG.IA-6, SG.SC-3, SG.SC-4, SG.SC-5, SG.SC-6, SG.SC-7, SG.SC-9, SG.SC-26, SG.SC-29, SG.SI-7
GIS	10	**All** Except: SG.AC-12, SG.AU-16, SG.IA-5, SG.SC-3, SG.SC-6, SG.SC-9, SG.SC-26
HAND, HANG	15	**All** Except: SG.AC-11, SG.AC-12, SG.AU-16, SG.IA-5, SG.SC-6, SG.SC-4, SG.SC-9, SG.SC-26, SG.SC-29
HEMP	8, 16	**All** Except: SG.SC-5, SG.SC-6, SG.SC-29
MDM	7, 8, 10	**All** Except: SG.SC-6, SG.SC-9
MTP	15	**All** Except: SG.AC-11, SG.AC-12, SG.AU-16, SG.IA-5, SG.SC-4, SG.SC-6, SG.SC-9, SG.SC-26, SG.SC-29

Table 8-2 NISTIR-7628 Security Requirements Applicability by System

*. AHF, DMS, and MVPM are not specifically listed in the table because their interfaces are covered under the interfaces of HEMP, MDM and CIS, respectively

The detailed results of determining which security controls are currently mandated by KCP&L are included in Appendix E. For each of recommended security control from the NISTIR-7628, this appendix lists the following information:

- The applicable Logical Interface Category from Table 1-2
- The corresponding recommended security control from the UCAIug Security Profile for AMI
- The corresponding recommended security control from the UCAIug Security Profile for DM
- Indication of requirement being mandated by KCP&L policies, standards, and/or processes
- Reference to KCP&L policy, standard, and/or process, if applicable

For a few requirements, the readers will find that the fulfillment of a control is stated as *No*. This is to indicate that the requirement is believed to not be currently fulfilled based upon analysis of KCP&L's policies, standards, and processes and discussion with the KCP&L Security Team.

See Appendix H for a list of the security requirements from the UCAIug Security Profiles for AMI and DM that were not confirmed to be covered in the NISTIR-7628. A further discussion will be needed with the KCP&L security team to confirm whether these security requirements are already fulfilled and if not, whether they should be implemented as part of the project.

9.0 PROJECT RECOMMENDATIONS

The success of the SmartGrid program is heavily dependent on the commitment from Senior Management and the implementers to deploy secure systems. This risk assessment for the KCP&L SmartGrid program was an important step towards ensuring cyber security. The United States Department of Energy (DOE) has also made cyber security a key focus area in all government-funded SmartGrid programs. On several occasions, the DOE has indicated that the success of individual programs will be dependent on the strength of deployed cyber security. The recommendations provided in this section are aimed towards maintaining KCP&L's focus on and commitment to implementing a secured SmartGrid program.

9.1 SELECT AND IMPLEMENT CONTROLS

Section 8.0 provided a recommended a list of procedural, operational, and technical controls to be implemented for securing the SmartGrid systems. The KCP&L cyber security team should assess each of these controls and select the ones that will be implemented. For the systems that are hosted externally by a third-party, the selected list of security controls should be made mandatory implementations enforced through contracts. For the systems that are hosted internally, the selection process should start with verification of all controls that are unconfirmed (Appendix E) to be currently met by KCP&L policies, procedures, and standards.

A three-phase implementation strategy should be considered. Phase I should include controls that need be implemented immediately to increase the security of systems already in place and the systems whose implementation is planned to be in next 1-3 months time. Phase II should include all controls not included in Phase I but are suggested in the tailored control sets (Section 8.0). The implementation of Phase II controls should be coordinated with the master system implementation schedule. Phase III implementation should include all controls that are covered in Section 8.0 but not included in Phases I and II.

9.2 CREATE SECURITY ZONES

Network segregation based on systems' business functions, criticality level, and physical location is one of the key factors for a successful cyber security implementation. It is recommended that the eight security zones suggested in Section 8.0 are implemented using a combination of firewalls, switch and router access control lists, authentication boundaries, and physical security measures. This action should be performed in collaborative design sessions between network designers, system integrators, subject matter experts and the security team. The creation of security zones is an important step towards a secured architecture.

9.3 CREATE A SECURITY IMPLEMENTATION PLAN

A plan should be created to depict the commissioning of controls and the security zones. The plan should identify the controls, implementation schedule, roles, responsibilities and the budget. This plan should be approved, signed, and periodically reviewed by KCP&L Senior Management. A Key Performance Indicators (KPI) matrix should be created to keep track of the implementation and provide KCP&L management a quick view of the progress. Close attention by Senior Management on the cyber security implementation is verified to be one of the key periodic evaluation criteria for the DOE.

A very tight working relationship between the integration and security team is strongly encouraged for the success of the security program for the SmartGrid systems. The security implementation schedule should mirror the master implementation schedule with key milestones tied between the two plans. The security team should also be required to provide their official "sign-offs" to all system documentation.

9.4 UPDATE THE CYBER SECURITY PLAN FOR THE DOE

The findings of the risk assessment and the resultant controls selection should be conveyed to the DOE by updating the previously submitted cyber security plan. A periodic review and update to the cyber security plan is not only one of the requirements of DOE grant projects, but is also another criterion used by the DOE during their evaluation visits. It is recommended that the signed security implementation plan be submitted as a supplement to the cyber security plan as an evidence of Senior Management's commitment to the cyber security of the SmartGrid systems.

9.5 CREATE SECURITY REQUIREMENTS FOR ALL SYSTEMS IN THE PROJECT

The control sets provided in Section 8.0 are conceptual controls which need to be converted to actual controls. The actual controls should identify firewalls, port numbers, monitoring software, encryption techniques, authentication, authorization, and other specific parameters. The actual security requirements should be created for each system and data interface. Each vendor should be provided with their system's security requirements and, where applicable, the contracts should be modified to make implementation of security requirements as payment milestones.

9.6 RECOMMENDATIONS FOR EXTERNALLY HOSTED SYSTEMS

Several systems within the SmartGrid environment are hosted by contracted vendors outside the physical control of KCP&L support and management personnel. This produces some unique challenges for

ensuring the Confidentiality, Integrity, and Availability of the data produced, processed, stored, or transmitted to or from those systems.

Although each vendor is bound by service contracts with KCP&L, the nature of the information being exchanged dictates the need to actively monitor and assess the measures being taken to provide safeguards for both data at rest, and data in motion. During the course of this risk assessment, it became apparent that each vendor had implemented or planned specific controls to protect the data that will be transmitted to and stored on their systems. It was also apparent that each vendor implemented controls according to their own internal policies and processes.

Providing guidance to vendors and ensuring uniform and adequate security controls for KCP&L's data is just one aspect of a robust vendor risk management program that KCP&L should implement. In 2009, Gartner Research released a series of papers in a special report dedicated to assessing, managing, and reducing all aspects of vendor risks.[38] This Special Report also outlines many aspects of managing vendor risks outside of information and IT security.

Many other organizations and security professionals have also provided guidance for managing vendor risk. For example, Evantix lists the steps for establishing a vendor risk management program as: Corporate Governance, Vendor Contracts, Risk Assessments, Onsite Audit, Reporting, and Risk Monitoring.[39] Another risk management vendor, PivotPoint Security, points out that companies may outsource many things, including call centers, application development, or IT operations, but they cannot outsource responsibility or liability.[40]

At the current stage of implementation and integration, KCP&L should begin by focusing on performing a thorough risk assessment of their chosen SmartGrid service providers, potentially including an onsite audit of information, transmission, and physical security. If the current service contracts do not have a provision for performing such an audit, KCP&L should ask each vendor to document their operational and security controls as thoroughly as possible. Appendix G provides a sample questionnaire that can be customized for each vendor to simplify the information gathering process.

---

[38] Gartner, Inc., *Special Report: Vendor Risk Management*, 2009, http://www.gartner.com/technology/research/reports/vendor-risk-management.jsp
[39] Evantix, LLC, Rene Barraza, *6 Steps to Establishing A Vendor Risk Management Program*, 26 July, 2010, http://www.evantix.com/blog/bid/39941/6-Steps-For-Building-a-Vendor-Risk-Management-Program
[40] Pivot Point Security, Inc., *Vendor (& Partner) Information Security Risk Management*, 28 March, 2011

Security control recommendations are detailed earlier in this report, but for externally hosted systems, the following should be the minimum recommended high-level requirements for maintaining the Confidentiality, Integrity, and Availability of KCP&L's data. Note that these recommendations do not supersede those made in Section 8.0. This list is merely a benchmark to ensure that external vendors meet a set of minimum security requirements. Vendors should provide written documentation verifying compliance with these baseline security control requirements.

9.6.1 Authentication

All access to externally hosted systems, whether interactive human access, or automated system or application access, should provide some type of authentication. This authentication may take the form of interactive passwords, public key certificates, secret key cryptography, or similar mechanisms.

9.6.2 Authorization

Every account on externally hosted systems should limit the user or remote system to specific functions required to perform specific tasks.

9.6.3 Transmission Security (Public)

Data in motion across public transmission media such as the Internet, cellular networks, or wireless networks, should be encrypted with a strong, proven algorithm such as AES and RSA, or certificate encryption such as SSL. This recommendation applies to KCP&L data classified as "Restricted" or "Internal Use Only."

9.6.4 Transmission Security (Private)

Data in motion across private transmission media such as dedicated hardwired circuits should be accessed only by those individuals with a justified need (i.e. data owner or administrator).

9.6.5 Data Storage Security

Data at rest on backup or storage media should be afforded the same level of security controls as the externally hosted system from which the data originated. Backup media stored in a public facility should be afforded the same level of control listed above under "Transmission Security (Public)".

9.6.6 Physical Security

Physical access to externally hosted systems should be restricted to those individuals requiring access for specific functions, such as system administrators, data center staff, or select maintenance personnel.

9.6.7 Auditing and Accountability

All externally hosted systems should be configured to provide detailed audit logs of all unauthorized activity and all system-level or privilege use activity on the system. These audit logs should be kept for a period of time prescribed by KCP&L and should be made available to authorized KCP&L personnel upon request.

9.6.8 Incident Response and Disaster Recovery

Externally hosted systems should be covered by a robust incident response plan, produce verified backups on a regular basis, and be subject to periodic recovery tests to ensure system recoverability in the event of an incident. In addition, highly critical systems should be designed with network and system redundancy with rapid failover in the event of a major service disruption.

9.6.9 Risk Assessment

All externally hosted systems should be subject to scheduled security audits and risk assessments performed by KCP&L or a designated third-party vendor.

Ensuring these baseline security controls are implemented for all externally hosted systems will establish a minimum level of assured security for KCP&L data residing outside the control of KCP&L personnel.

9.7 POLICY UPDATES ON RECOMMENDED PROCEDURAL CONTROLS

Several procedural and operational controls were recommended in Section 8.0. It is recommended that existing KCP&L Policies, Standards and Processes documentation be modified with these controls. This could be accomplished by either creating addendums to the existing policies or creating supplements. It is also recommended that existing policy enforcement mechanisms be extended to the SmartGrid systems, serving as further evidence of commitment from Senior Management to a secured implementation of SmartGrid program at KCP&L.

9.8 CREATE & EXECUTE TEST CASES

It is very important that the security controls and architecture are tested to verify deployment as intended. A series of test cases should be created and executed to ensure systems are secured. The test cases should also cover any externally hosted system and field equipment. Considerations should be given to create a test environment to perform rigorous testing. Two types of tests should be conducted: Verification against the Design Specifications and Penetration Tests. The results should be reviewed with the Senior Management, system integrators, network designers, and security team. Changes to the system should be

made and tests re-executed when needed. The processes should be repeated until the results are accepted by the SmartGrid system stakeholders.

9.9 PERFORM PERIODIC SECURITY ASSESSMENT

A security assessment in each SDLC phase shall be conducted to assess cyber vulnerabilities and threats to the SmartGrid systems. The assessments should be conducted in accordance with principles and standards set forth by organizations like NIST and NERC. This step will ensure that the systems are protected up to the date and cyber security focus is maintained throughout the project duration. A strategy should be crafted to incorporate SmartGrid systems (once the project is over) into the existing production systems security assessments.

9.10 PARTICIPATE IN WORKING GROUPS

There are several ways to keep pace with ever-changing cyber security requirements. It is recommended that the security and operational teams at KCP&L participate and collaborate in cyber security working groups created specifically for the utility industry, several of which are mentioned in this report. Table 9-1 provides a good coverage of working groups dealing with various aspects of security and functionality of smart grid applications.

Area of Responsibility	Industry Interest Group	Website
Distribution	SGIP	http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/SGIP
	Zigbee Alliance	http://www.zigbee.org/
	UCAIug	http://www.ucaiug.org/default.aspx
	SGMM	http://www.sei.cmu.edu/smartgrid/tools/
Transmission	Transmission Forum	http://www.transmissionforum.net/forum/
	ICSJWG	http://www.us-cert.gov/control_systems/icsjwg/index.html
	IEC 61850 User Group	http://iec61850.ucaiug.org/default.aspx
	NERC 706 SDT	http://www.nerc.com/files/standards/Cyber-Security-Initiatives.html
	EEI Cyber Security	http://www.eei.org/ourissues/ElectricityTransmission/Pages/CyberSecurity.aspx
Cyber Security	NERC 706 SDT	http://www.nerc.com/files/standards/Cyber-Security-Initiatives.html
	ISA	http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821
	NESCO	http://www.energyser.org/nesco
	UTC	http://www.utc.org/
Physical Security	ASIS International	http://www.asisonline.org/
	NERC 706 SDT	http://www.nerc.com/files/standards/Cyber-Security-Initiatives.html
	SIA	http://www.siaonline.org/

Table 9-1 Industry Working Groups

9.11 CONCLUSION

Performing a risk assessment on the majority of systems in the KCP&L SmartGrid Demonstration Project produced a large amount of documentation and data. The analysis for some systems confirmed the risk level previously assumed prior to the risk assessment, while for others indicated the need for either additional security, or the need to reduce some of the focus. It soon became apparent that the protection of systems like the DMS, HEMP, AHE, and others was critical to the success of the project. In other cases, systems like the Field and Substations DADs, were found to be at lower risk than originally expected.

Another discovery was that the most critical and highest impact systems were not necessarily those with the highest level of assessed risk, due to existing security controls in place for those systems. Processing each cyber asset through the risk rating model provided an accurate and objective evaluation of each system's current risk, and allowed the assessment team to provide focused recommendations for system security zones, network segmentation, and mitigating controls.

To date, KCP&L SmartGrid program personnel have provided proper attention to the cyber security needs of the project in accordance with the DOE's expectations. This risk assessment and its reliance on industry standards and best practices was an important step towards a secure KCP&L SmartGrid infrastructure. Continued support from KCP&L management and focus from the project and security teams to implement these recommendations is needed to ensure the success of the project.

APPENDIX A THE NISTIR-7628 LOGICAL INTERFACE CATEGORIES

NISTIR-7628 Logical Interface Category	NISTIR-7628 Logical Interface Category Description
1	Interface between control systems and equipment with high availability, and with compute and/or bandwidth constraints
2	Interface between control systems and equipment without high availability, but with compute and/or bandwidth constraints
3	Interface between control systems and equipment with high availability, without compute nor bandwidth constraints
4	Interface between control systems and equipment without high availability, without compute nor bandwidth constraints
5	Interface between control systems within the same organization
6	Interface between control systems in different organizations
7	Interface between back office systems under common management authority
8	Interface between back office systems not under common management authority
9	Interface with B2B connections between systems usually involving financial or market transactions
10	Interface between control systems and non-control/corporate systems
11	Interface between sensors and sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analog measurements
12	Interface between sensor networks and control systems
13	Interface between systems that use the AMI network
14	Interface between systems that use the AMI network with high availability
15	Interface between systems that use customer (residential, commercial, and industrial) site networks
16	Interface between external systems and the customer site
17	Interface between systems and mobile field crew laptops/equipment
18	Interface between metering equipment
19	Interface between operations decision support systems
20	Interface between engineering/maintenance systems and control equipment
21	Interface between control systems and their vendors for standard maintenance and service
22	Interface between security/network/system management consoles and all networks and systems

APPENDIX B KCP&L TO NISTIR-7628 LOGICAL INTERFACE MAPPING

NISTIR-7628 Logical Interface Category Description	NISTIR-7628 Logical Interface Category	From	To	KCP&L Logical Interface	NISTIR-7628 Logical Interface
Interface between control systems and equipment with high availability, and with compute and/or bandwidth constraints	1	EMS	Substation DADs	3	U67
		DDC	DER	26	U65
Interface between control systems and equipment without high availability, but with compute and/or bandwidth constraints	2	DDC	Field DAD	11	U117
Interface between control systems and equipment with high availability, without compute nor bandwidth constraints	3	DDC	Substation DAD	21	U117
Interface between control systems within the same organization	5	AHE	Legacy OMS	2	U26
		D-SCADA	DNA	7	U9
		D-SCADA	DAC	12a	New
		D-SCADA	DDC	22	New
		DAC	DDC	24	New
Interface between back office systems under common management authority	7	MDM	DERM	4	New
		CIS	MDM	8	New
		CIS	Legacy MWFM	27	U131
		CIS	GIS	30	U110
		MDM	DMAT	33	New
Interface between back office systems not under common management authority	8	MDM	HEMP	9	New
		DERM	HEMP	15	U106
		DERM	VEMS	18	U106
		DERM	AHE	23	U22
		HEMP	AHE	25	U2
		HEMP	ALNK	29	New
		CIS	HEMP	31	U119
		CIS	DERM	32	U33
Interface with B2B connections between systems usually involving financial or market transactions	9	DERM	RTO	20	U93
Interface between control systems and non-control/corporate systems	10	CIS	AHE	1	U21
		MDM	AHE	6	U2
		DMS	MDM	10	U8
		GIS	MWFM	13	U102
		DNA	DERM	14a	U11
Interface between sensors and sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analog measurements	11	DADC	DAD-A/DAD-M	54	U112
		DERC	DER-A/DER-M	55	U112

Interface between systems that use customer (residential, commercial, and industrial) site networks	15	VEMS	EVSE	19	U62
		HANG	Residential DER	28	U130
		EVSE	PEV	34	New
		BMS	Commercial & Industrial DER	35	U45
		ESI	HAND	52a	U120
		HAND	ESI	52b	U120
		HAND	HAND	52c	N/A
		CHR	HAND	53a	N/A
		HAND	CHR	53b	N/A
		HAND	HAND	53c	N/A
Interface between external systems and the customer site	16	HEMP	IPI	16	U42
		DERM	BMS	17	U106
Interface between systems that use the AMI network (with high availability)	13 (14)	AHE	MFR	5	U24

APPENDIX C KCP&L SMARTGRID SYSTEM DESCRIPTIONS

System	Name	Description
AHE	AMI Head-End	The Advanced Metering Infrastructure Head-End (AHE) is a system that serves as the operational control application for the Advanced Metering Infrastructure (AMI) solution. Optionally, it manages required meter reading collection and enacts other meter- and communication-related commands. The AHE also manages the transfer of meter information to the Meter Data Management System (MDM).
ALNK	AccountLink	AccountLink (ALNK) is an interactive Web-site that is accessible via the Internet that enables the exchange and display of account information for the Customer.
BMS	Building Management System	A Building Management System (BMS) is a system/service that monitors and controls building energy and responds to signals while minimizing impact on building occupants.
CIS	Customer Information System	The Customer Information System (CIS) is an enterprise-wide software application that allows the Utility to manage aspects of their relationship with Customers. In addition to Customer revenue management and service order management, the CIS supports the Utility function that manages Customer relationships by providing a point-of-contact and resolution for Customer issues and problems.
DAC	Distribution Automation Controller	The Distribution Automation Controller is the processing portion of the Distributed Control and Data Acquisition System (DCADA) that implements the following functionalities: Supervisory Control and Data Acquisition (SCADA), Switching Procedure Management (SPM), Distribution Network Analysis (DNA), Distribution System State Estimator (DSSE), Short-Term Load Scheduler (STLS), Fault Detection and Immediate Restoration (FDIR), Volt/var Control (VVC), and Feeder Load Transfer (FLT).
DDC	Distribution Data Concentrator	The Distribution Data Concentrator (DDC) acts as a multi-protocol pipeline for data flow between the Substation, Field Automation, and Distribution Operations security zones. It is the other main portion of the Distributed Control and Data Acquisition System (DCADA).
DER - C&I	Commercial & Industrial Distributed Energy Resource	Commercial & Industrial Distributed Energy Resources (C&I DER) include small-scale generation or storage of any form that is located on a commercial or industrial customer's premises. These energy resources include, but are not limited to, energy storage devices, photovoltaic panels, backup generators, and plug-in electric vehicles.
DER - Grid-Connected	Grid-Connected Distributed Energy Resource	Grid-Connected Distributed Energy Resources (DER) include small-scale generation or storage of any form that is attached to the distribution grid. These energy resources include, but are not limited to, energy storage devices, photovoltaic panels, backup generators, biomass, and plug-in electric vehicles. In this project, this energy resource is a grid-connected battery located in the Midtown Substation.
DER - Residential	Residential Distributed Energy Resource	Residential Distributed Energy Resources (DER) include small-scale generation or storage of any form that is located on a residential customer's premises. These generation facilities include, but are not limited to, energy storage devices, photovoltaic panels, wind generators, biomass, and plug-in electric vehicles.

System	Name	Description
DERM	Distributed Energy Resource Management System	The Distributed Energy Resource Management System (DERM) is a system used to manage demand response events. The DERM schedules events based on requests from Regional Transmission Organization Wholesale Markets (RTOs) and the Distribution Management System (DMS) and issues the appropriate event signals with the Home Energy Management Portal (HEMP), aggregators, commercial customers, and distribution Grid-Connected Distributed Energy Resources (DER).
DMAT	Data Mining & Analysis Tool	The Data Mining & Analysis Tool (DMAT) is a system that receives data from the Meter Data Management System (MDM), mines the data upon request, and passes it along to requestors.
DMS	Distribution Management System	The Distribution Management System (DMS) is a suite of application software that monitors and controls the distribution system equipment based on computer-aided applications, market information, and operator control decisions. The DMS integrates the Distribution Operator GUI (DOG), Distribution Supervisory Control and Data Acquisition (D-SCADA), Distribution Network Analysis (DNA), Outage Management System (OMS), and Mobile Workforce Management System (MWFM).
EMS	Energy Management Systems	Energy Management Systems (EMS) are a collection of systems used to manage the bulk power delivery system. These systems include Transmission Supervisory Control and Data Acquisition (T-SCADA), Transmission Management Systems (TMS), and Generation Management Systems (GMS).
EVSE	Electric Vehicle Supply Equipment	Electric Vehicle Supply Equipment (EVSE) are the physical electrical cord and connectors that are specified by applicable Society of Automotive Engineers (SAE) standards to provide the transfer of electric energy from the charging point to the Plug-in Electric Vehicle (PEV).
Field DADs	Field Distribution Automation Devices	Field Distribution Automation Devices (DADs) are a variety of devices (switches, automatic reclosers, capacitors, regulators, etc.) located throughout SmartGrid Demonstration Zone that support distribution automation functionality.
GIS	Geographic Information System	Geographic Information System (GIS) is a spatial asset management system that provides the Utility with asset information and network connectivity for advanced applications.
HAND	Home Area Network Device	A Home Area Network Device (HAND) is a device owned by a Customer or a third party that is registered on the Home Area Network (HAN). A HAND communicates in a secure way with other HANDs (e.g., Programmable Communicating Thermostat (PCT), Load Control Switch (LCS), and Customer Household Appliance (CHA)).
HANG	Home Area Network Gateway	A Home Area Network Gateway (HANG) is a device that registers with the SmartMeter (MTR) to receive usage data and creates a secondary HAN to which HAN Devices (HANDs) are registered. The HANG also connects the HAN to the Home Energy Management Portal (HEMP) via a customer broadband connection. The HANG provides cyber security and coordinates functions that enable secure interactions between relevant HANDs, MTRs, and the Utility.
HEMP	Home Energy Management Portal	The Home Energy Management Portal (HEMP) is an Internet-based system that provides access to various data, including billing plans and electricity usage, to the customer. The customer uses the Home Energy Management Portal (HEMP) to manage their in-premise Home Area Network Devices (HANDs) and, in turn, control their energy consumption.

System	Name	Description
MDM	Meter Data Management System	The Meter Data Management System (MDM) is a system that stores SmartMeter (MTR) data (e.g., energy usage, energy generation, meter logs, meter test results) and makes data available to authorized systems. The MDM performs VEE (validation, estimation, and editing) and creates bill determinants for the Customer Information System (CIS) billing engine.
MTR	SmartMeter	A SmartMeter (MTR) is a device that measures the amount of electricity used at a particular site. MTRs are typically located at the Customer facility and owned by the distributor (e.g., Utility) or retail provider.
MWFM	Mobile Workforce Management System	The Mobile Workforce Management System (MWFM) is an enterprise-wide system that is used to manage trouble order and customer order dispatch to field crews.
OMS	Outage Management System	The Outage Management System (OMS) is an enterprise-wide system that is used by operators of electric distribution systems to assist in outage identification and power restoration.
PEV	Plug-in Electric Vehicle	A Plug-In Electric Vehicle (PEV) is a motorized car or truck which runs exclusively or partially on stored battery power, as opposed to being powered directly by carbon-based fuel. Additionally, a PEV plugs into premise Electric Vehicle Supply Equipment (EVSE) to charge the vehicle.
RTO	Regional Transmission Organization Wholesale Market	A Regional Transmission Organization Wholesale Market (RTO) is a organization in charge of bulk electricity markets, such as Southwest Power Pool (SPP).
Substation DADs	Substation Distribution Automation Devices	Substation Distribution Automation Devices (DADs) are a variety of devices (switches, automatic reclosers, capacitors, regulators, etc.) located in Midtown Substation that support distribution automation functionality.
VEMS	Vehicle Energy Management System	A Vehicle Energy Management System (VEMS) is a system that encourages/discourages charging Plug-in Electric Vehicles (PEVs) through relevant pricing or other (dis)incentives, processes and stores data about PEV programs, contracts, and relevant historic information, creates behavioral models, and collects, processes, and stores customer-specific data.

APPENDIX D DEFINITION LOCATION OF NISTIR-7628 RECOMMENDED SECURITY REQUIREMENTS

NISTIR-7628 Smart Grid Requirement Number	NISTIR-7268 Smart Grid Requirement Name	NISTIR-7628 Volume 1 Page Number(s)
SG.AC-1	Access Control Policy and Procedures	91-92
SG.AC-2	Remote Access Policy and Procedures	92
SG.AC-3	Account Management	92-93
SG.AC-4	Access Enforcement	93
SG.AC-6	Separation of Duties	94-95
SG.AC-7	Least Privilege	95
SG.AC-8	Unsuccessful Login Attempts	95-96
SG.AC-9	Smart Grid Information System Use Notification	96-97
SG.AC-11	Concurrent Session Control	97
SG.AC-12	Session Lock	98
SG.AC-14	Permitted Actions without Identification or Authentication	98-99
SG.AC-16	Wireless Access Restrictions	100
SG.AC-17	Access Control for Portable and Mobile Devices	100-101
SG.AC-18	Use of External Information Control Systems	101-102
SG.AC-19	Control System Access Restrictions	102
SG.AC-20	Publicly Accessible Content	103
SG.AC-21	Passwords	103-104
SG.AT-1	Awareness and Training Policy and Procedures	104-105
SG.AT-2	Security Awareness	105
SG.AT-3	Security Training	105-106
SG.AT-4	Security Awareness and Training Records	106
SG.AT-6	Security Responsibility Testing	107
SG.AT-7	Planning Process Training	107-108
SG.AU-1	Audit and Accountability Policy and Procedures	108-109
SG.AU-2	Auditable Events	109
SG.AU-3	Content of Audit Records	109-110
SG.AU-4	Audit Storage Capacity	110
SG.AU-5	Response to Audit Processing Failures	110-111
SG.AU-6	Audit Monitoring, Analysis, and Reporting	111-112
SG.AU-7	Audit Reduction and Report Generation	112
SG.AU-8	Time Stamps	112
SG.AU-9	Protection of Audit Information	113
SG.AU-10	Audit Record Retention	113
SG.AU-11	Conduct and Frequency of Audits	113-114
SG.AU-12	Auditor Qualification	114
SG.AU-13	Audit Tools	114-115

NISTIR-7628 Smart Grid Requirement Number	NISTIR-7268 Smart Grid Requirement Name	NISTIR-7628 Volume 1 Page Number(s)
SG.AU-14	Security Policy Compliance	115
SG.AU-15	Audit Generation	116
SG.AU-16	Non-Repudiation	116-117
SG.CA-1	Security Assessment and Authorization Policy and Procedures	117-118
SG.CA-2	Security Assessments	118
SG.CA-4	Smart Grid Information System Connections	119
SG.CA-5	Security Authorization to Operate	120
SG.CA-6	Continuous Monitoring	120-121
SG.CM-1	Configuration Management Policy and Procedures	121-122
SG.CM-2	Baseline Configuration	122
SG.CM-3	Configuration Change Control	122-123
SG.CM-4	Monitoring Configuration Changes	123-124
SG.CM-5	Access Restrictions for Configuration Change	124
SG.CM-6	Configuration Settings	124-125
SG.CM-7	Configuration for Least Functionality	125-126
SG.CM-8	Component Inventory	126
SG.CM-9	Addition, Removal, and Disposal of Equipment	127
SG.CM-10	Factory Default Settings Management	127-128
SG.CM-11	Configuration Management Plan	128
SG.CP-1	Continuity of Operations Policy and Procedure	128-129
SG.CP-2	Continuity of Operations Plan	129-130
SG.CP-3	Continuity of Operations Roles and Responsibilities	130
SG.CP-4	Continuity of Operations Training	130-131
SG.CP-5	Continuity of Operations Plan Testing	131
SG.CP-6	Continuity of Operations Plan Update	131-132
SG.CP-7	Alternate Storage Sites	132
SG.CP-8	Alternate Telecommunication Services	133
SG.CP-9	Alternate Control Center	133-134
SG.CP-10	Smart Grid Information System Recovery and Reconstitution	134-135
SG.CP-11	Fail-Safe Response	135
SG.IA-1	Identification and Authentication Policy and Procedures	136
SG.IA-2	Identifier Management	136-137
SG.IA-3	Authenticator Management	137

NISTIR-7628 Smart Grid Requirement Number	NISTIR-7268 Smart Grid Requirement Name	NISTIR-7628 Volume 1 Page Number(s)
SG.IA-4	User Identification and Authentication	138
SG.IA-5	Device Identification and Authentication	138-139
SG.IA-6	Authenticator Feedback	139
SG.ID-1	Information and Document Management Policy and Procedures	139-140
SG.ID-2	Information and Document Retention	140-141
SG.ID-3	Information Handling	141
SG.ID-4	Information Exchange	141-142
SG.IR-1	Incident Response Policy and Procedures	143-144
SG.IR-2	Incident Response Roles and Responsibilities	144
SG.IR-3	Incident Response Training	144-145
SG.IR-4	Incident Response Testing and Exercises	145
SG.IR-5	Incident Handling	145-146
SG.IR-6	Incident Monitoring	146
SG.IR-7	Incident Reporting	146-147
SG.IR-8	Incident Response Investigation and Analysis	147
SG.IR-9	Corrective Action	147-148
SG.IR-10	Smart Grid Information System Backup	148
SG.IR-11	Coordination of Emergency Response	149
SG.MA-1	Smart Grid Information System Maintenance Policy and Procedures	149-150
SG.MA-2	Legacy Smart Grid Information System Upgrades	150
SG.MA-3	Smart Grid Information System Maintenance	150-151
SG.MA-4	Maintenance Tools	152
SG.MA-5	Maintenance Personnel	152-153
SG.MA-6	Remote Maintenance	153
SG.MA-7	Timely Maintenance	154
SG.MP-1	Media Protection Policy and Procedures	154-155
SG.MP-2	Media Sensitivity Level	155
SG.MP-3	Media Marking	155-156
SG.MP-4	Media Storage	156
SG.MP-5	Media Transport	156-157
SG.MP-6	Media Sanitization and Disposal	157
SG.PE-1	Physical and Environmental Security Policy and Procedures	157-158
SG.PE-2	Physical Access Authorizations	158-159
SG.PE-3	Physical Access	159-160

NISTIR-7628 Smart Grid Requirement Number	NISTIR-7268 Smart Grid Requirement Name	NISTIR-7628 Volume 1 Page Number(s)
SG.PE-4	Monitoring Physical Access	160
SG.PE-5	Visitor Control	160-161
SG.PE-6	Vistor Records	161
SG.PE-7	Physical Access Log Retention	161-162
SG.PE-8	Emergency Shutoff Protection	162
SG.PE-9	Emergency Power	162-163
SG.PE-10	Delivery and Removal	163
SG.PE-11	Alternate Work Site	163-164
SG.PE-12	Location of Smart Grid Information System Assets	164
SG.PL-1	Strategic Planning Policy and Procedures	164-165
SG.PL-2	Smart Grid Information System Security Plan	165-166
SG.PL-3	Rules of Behavior	166
SG.PL-4	Privacy Impact Assessment	167
SG.PL-5	Security-Related Activity Planning	167
SG.PM-1	Security Policy and Procedures	168
SG.PM-2	Security Program Plan	168-169
SG.PM-3	Senior Management Authority	169-170
SG.PM-4	Security Architecture	170
SG.PM-5	Risk Management Strategy	170-171
SG.PM-6	Security Authorization to Operate Process	171
SG.PM-7	Mission/Business Process Definition	171
SG.PM-8	Management Accountability	171-172
SG.PS-1	Personnel Security Policy and Procedures	172-173
SG.PS-2	Position Categorization	173
SG.PS-3	Personnel Screening	173-174
SG.PS-4	Personnel Termination	174-175
SG.PS-5	Personnel Transfer	175
SG.PS-6	Access Agreements	175-176
SG.PS-7	Contractor and Third-Party Personnel Security	176
SG.PS-8	Personnel Accountability	176-177
SG.PS-9	Personnel Roles	177
SG.RA-1	Risk Assessment Policy and Procedures	177-178
SG.RA-2	Risk Management Plan	178-179
SG.RA-3	Security Impact Level	179
SG.RA-4	Risk Assessment	179-180
SG.RA-5	Risk Assessment Update	180
SG.RA-6	Vulnerability Assessment and Awareness	180-181

NISTIR-7628 Smart Grid Requirement Number	NISTIR-7268 Smart Grid Requirement Name	NISTIR-7628 Volume 1 Page Number(s)
SG.SA-1	Smart Grid Information System and Services Acquisition Policy and Procedures	181-182
SG.SA-2	Security Policies for Contractors and Third Parties	182-183
SG.SA-3	Life-Cycle Support	183
SG.SA-4	Acquisitions	183-184
SG.SA-5	Smart Grid Information System Documentation	184
SG.SA-6	Software License Usage Restrictions	184-185
SG.SA-7	User-Installed Software	185
SG.SA-8	Security Engineering Principles	185-186
SG.SA-9	Developer Configuration Management	186-187
SG.SA-10	Developer Security Testing	187
SG.SA-11	Supply Chain Protection	187-188
SG.SC-1	Smart Grid Information System and Communication Protection Policy and Procedures	188-189
SG.SC-3	Security Function Isolation	190
SG.SC-4	Information Remnants	190
SG.SC-5	Denial-of-Service Protection	190-191
SG.SC-6	Resource Priority	191
SG.SC-7	Boundary Protection	191-193
SG.SC-8	Communication Integrity	193
SG.SC-9	Communication Confidentiality	193
SG.SC-11	Cryptographic Key Establishment and Management	194
SG.SC-12	Use of Validated Cryptography	194-195
SG.SC-13	Collaborative Computing	195
SG.SC-15	Public Key Infrastructure Certificates	196
SG.SC-16	Mobile Code	196-197
SG.SC-18	System Connections	197-198
SG.SC-19	Security Roles	198
SG.SC-20	Message Authenticity	198-199
SG.SC-21	Secure Name/Address Resolution Service	199
SG.SC-22	Fail in Known State	199-200
SG.SC-26	Confidentiality of Information at Rest	201
SG.SC-29	Application Partitioning	203
SG.SC-30	Smart Grid Information System Partitioning	203-204
SG.SI-1	Smart Grid Information System and Information Integrity Policy and Procedures	204-205

NISTIR-7628 Smart Grid Requirement Number	NISTIR-7268 Smart Grid Requirement Name	NISTIR-7628 Volume 1 Page Number(s)
SG.SI-2	Flaw Remediation	205
SG.SI-3	Malicious Code and Spam Protection	206
SG.SI-4	Smart Grid Information System Monitoring Tools and Techniques	206-207
SG.SI-5	Security Alerts and Advisories	207-208
SG.SI-6	Security Functionality Verification	208
SG.SI-7	Software and Information Integrity	208-209
SG.SI-8	Information Input Validation	209
SG.SI-9	Error Handling	209-210

APPENDIX E CONTROL ANALYSIS RESULTS

NISTIR 7628 Smart Grid Requirement Number	NISTIR 7628 Smart Grid Requirement Name	Applicable Interface Categories	UCAIug Security Profile for AMI	UCAIug Security Profile for DM	Requirement Fulfilled by KCP&L Policies, Standards, & Processes	KCP&L Policy Number(s)	KCP&L Standard(s)	KCP&L Process(es)
SG.AC-1	Access Control Policy and Procedures	All	1869-2.15.1	Policy 4	Yes	KCP&L-[illegible], KCP&L-[illegible]	Access Control Standard	Access Management Process
SG.AC-2	Remote Access Policy and Procedures	All	1869-2.15.34	Policy 4	Yes	KCP&L-[illegible]	Remote Access Standard	Remote Access Procedure
SG.AC-3	Account Management	All	1869-2.15.3	Protection 26, Protection 27, Detection 23, Prevention 31	Yes	None	Access Control Standard	Access Management Process
SG.AC-4	Access Enforcement	All	1869-2.15.7	Protection 29	Yes	None	Access Control Standard	None
SG.AC-5	Information Flow Enforcement	None	1869-2.15.33	Protection 35	Yes	None	Confidentiality Protection Standard	None
SG.AC-6	Separation of Duties	All	1869-2.15.8	Policy 2	Yes	None	Change Control Standard	Change Management Process
SG.AC-7	Least Privilege	All	1869-2.15.9	Protection 30	Yes	KCP&L-[illegible]	None	None
SG.AC-8	Unsuccessful Login Attempts	All	1869-2.15.20	Reaction 4	Yes	None	Access Control Standard, Remote Access Standard	None
SG.AC-9	Smart Grid Information System Use Notification	All	1869-2.15.27	Policy 4	Yes	None	Access Control Standard, Remote Access Standard	None
SG.AC-10	Previous Logon Notification	None	1869-2.15.19	Detection 28	No	None	None	None
SG.AC-11	Concurrent Session Control	1,2,3,5,7,8,9,10,13,14,16	1869-2.15.18	Protection 37	No	None	None	None
SG.AC-12	Session Lock	7,8	1869-2.15.21	Protection 38	No	None	None	None
SG.AC-13	Remote Session Termination	None	1869-2.15.22	Protection 39	No	None	None	None
SG.AC-14	Permitted Actions without Identification or Authentication	1,2,3,5,7,8,9,10,13,14,15,16	1869-2.15.11	Reaction 5	Yes	None	Access Control Standard	None
SG.AC-15	Remote Access	None	1869-2.15.24	Detection 14	Yes	KCP&L-[illegible]	Remote Access Standard	Remote Access Procedure
SG.AC-16	Wireless Access Restrictions	All	1869-2.15.26	Policy 9	Yes	KCP&L-[illegible]	Wireless Networking Standard	None
SG.AC-17	Access Control for Portable and Mobile Devices	All	1869-2.15.29	Protection 40	Yes	KCP&L-[illegible]	Access Control Standard, Account Management	None
SG.AC-18	Use of External Information Control Systems	All	1869-2.15.29	Policy 4	Yes	None	Remote Access Standard	Remote Access Procedure, Access Management Process
SG.AC-19	Control System Access Restrictions	All	N/A	Network 3, 4	Yes	None	Access Control Standard	None
SG.AC-20	Publicly Accessible Content	All	N/A	N/A	No	None	None	None
SG.AC-21	Passwords	All	1869-2.15.16	Protection 36	Yes	None	Access Control Standard, Remote Access Standard	Access Management Process, Remote Access Process
SG.AT-1	Awareness and Training Policy and Procedures	All	N/A	Policy 2	Yes	KCP&L-[illegible], KCP&L-[illegible], KCP&L-[illegible]	Information Security Awareness Standard	PCI Life Cycle Process
SG.AT-2	Security Awareness	All	N/A	Policy 2	Yes	KCP&L-[illegible], KCP&L-[illegible], KCP&L-[illegible]	Information Security Awareness Standard	PCI Life Cycle Process
SG.AT-3	Security Training	All	N/A	Policy 2	Yes	KCP&L-[illegible]	None	None
SG.AT-4	Security Awareness and Training Records	All	N/A	N/A	Yes	None	Information Security Awareness Standard	None
SG.AT-5	Contact with Security Groups and Associations	None	N/A	N/A	No	None	None	None
SG.AT-6	Security Responsibility Testing	All	N/A	N/A	No	None	None	None
SG.AT-7	Planning Process Training	All	N/A	N/A	Yes	None	None	None

NISTIR 7628 Smart Grid Requirement Number	NISTIR 7628 Smart Grid Requirement Name	Applicable Interface Categories	UCAIug Security Profile for AMI	UCAIug Security Profile for DM	Requirement Fulfilled by KCP&L Policies, Standards, & Processes	KCP&L Policy Number(s)	KCP&L Standard(s)	KCP&L Process(es)
SG.AU-1	Audit and Accountability Policy and Procedures	All	N/A	Policy 9	No	None	None	None
SG.AU-2	Auditable Events	All	1869-2.16.2	Policy 9	No	None	None	None
SG.AU-3	Content of Audit Records	All	1869-2.16.3	N/A	No	None	None	None
SG.AU-4	Audit Storage Capacity	All	1869-2.16.4	N/A	No	None	None	None
SG.AU-5	Response to Audit Processing Failures	All	1869-2.16.5	N/A	No	None	None	None
SG.AU-6	Audit Monitoring, Analysis, and Reporting	All	N/A	Policy 9	No	None	None	None
SG.AU-7	Audit Reduction and Report Generation	All	1869-2.16.7	N/A	No	None	None	None
SG.AU-8	Time Stamps	All	1869-2.16.8	N/A	No	None	None	None
SG.AU-9	Protection of Audit Information	All	1869-2.16.9	N/A	No	None	None	None
SG.AU-10	Audit Record Retention	All	N/A	Policy 9	No	None	None	None
SG.AU-11	Conduct and Frequency of Audits	All	N/A	N/A	Yes	None	None	None
SG.AU-12	Auditor Qualification	All	1869-2.16.12	N/A	Yes	None	None	None
SG.AU-13	Audit Tools	All	AMISP-2.16.1	Policy 9	Yes	None	None	None
SG.AU-14	Security Policy Compliance	All	N/A	Policy 2	Yes	None	None	None
SG.AU-15	Audit Generation	All	N/A	N/A	No	None	None	None
SG.AU-16	Non-Repudiation	7,8,9,15,16,18	N/A	N/A	No	None	None	None
SG.CA-1	Security Assessment and Authorization Policy and Procedures	All	N/A	Policy 3	No	None	None	None
SG.CA-2	Security Assessments	All	N/A	Policy 5, Detection 12	No	None	None	None
SG.CA-3	Continuous Improvement	None	N/A	Policy 10	No	None	None	None
SG.CA-4	Smart Grid Information System Connections	All	N/A	Policy 3	Yes	None	Remote Access Standard	Remote Access Procedure
SG.CA-5	Security Authorization to Operate	All	N/A	N/A	Yes	None	None	Change Control Procedure
SG.CA-6	Continuous Monitoring	All	N/A	Policy 3	No	None	None	None
SG.CM-1	Configuration Management Policy and Procedures	All	N/A	Policy 7	Yes	KCP&L-[illegible]	Configuration Management Standard	Configuration Management Process
SG.CM-2	Baseline Configuration	All	N/A	Detection 8	Yes	KCP&L-[illegible]	None	None
SG.CM-3	Configuration Change Control	All	N/A	Policy 7	Yes	None	None	Configuration Management Process
SG.CM-4	Monitoring Configuration Changes	All	N/A	Policy 7	Yes	None	Configuration Management Standard	Configuration Management Process
SG.CM-5	Access Restrictions for Configuration Change	All	N/A	N/A	Yes	None	None	Configuration Management Process
SG.CM-6	Configuration Settings	All	N/A	Detection 10	Yes	None	Configuration Management Standard	Configuration Management Process
SG.CM-7	Configuration for Least Functionality	All	N/A	Policy 7	Yes	None	Access Control Standard	None
SG.CM-8	Component Inventory	All	N/A	Detection 7	Yes	None	Configuration Management Standard	Access Management Hardware Process, Computer System Requests Process, Information Technology Planning Process

NISTIR 7628 Smart Grid Requirement Number	NISTIR 7268 Smart Grid Requirement Name	Applicable Interface Categories	UCAIug Security Profile for AMI	UCAIug Security Profile for DM	Requirement Fulfilled by KCP&L Policies, Standards, & Processes	KCP&L Policy Number(s)	KCP&L Standard(s)	KCP&L Process(s)
SG.CM-6	Addition, Removal, and Disposal of Equipment	All	N/A	Policy 3	Yes	None	Configuration Management Standard	Access Management Hardware Process, Configuration Management Process
SG.CM-10	Factory Default Settings Management	All	N/A	Protection 9	No	None	None	None
SG.CM-11	Configuration Management Plan	All	N/A	Policy 7	Yes	None	Configuration Management Standard	Configuration Management Process
SG.CP-1	Continuity of Operations Policy and Procedure	All	N/A	N/A	No	None	None	None
SG.CP-2	Continuity of Operations Plan	All	DHS-2.12.2	Recovery 8	Yes	None	Availability Protection Standard	None
SG.CP-3	Continuity of Operations Roles and Responsibilities	All	DHS-2.12.3	N/A	Yes	None	Incident Response Standard	None
SG.CP-4	Continuity of Operations Training	All	AMERP-2.12.1	Policy 2	Yes	None	None	None
SG.CP-5	Continuity of Operations Plan Testing	All	DHS-2.12.5	N/A	Yes	None	Availability Protection Standard	None
SG.CP-6	Continuity of Operations Plan Update	All	AMERP-2.12.2	N/A	Yes	None	Availability Protection Standard	None
SG.CP-7	Alternate Storage Sites	All	N/A	Policy 6	Yes	None	None	Backup and Recovery Process
SG.CP-8	Alternate Telecommunication Services	All	N/A	Policy 6	No	None	None	None
SG.CP-9	Alternate Control Center	All	N/A	Policy 6	Yes	KCPL-ISMS	None	None
SG.CP-10	Smart Grid Information System Recovery and Reconstitution	All	N/A	Policy 6	Yes	KCPL-ISMS	None	None
SG.CP-11	Fail-Safe Response	All	N/A	Protection 10, 20	Yes	KCPL-ISMS	None	None
SG.IA-1	Identification and Authentication Policy and Procedure	All	DHS-2.15.2	Protection 1, 10, 11, 27, 28, 29, 32, 33	Yes	None	Access Control Standard	None
SG.IA-2	Identifier Management	All	DHS-2.15.4	Detection 26	Yes	None	Access Control Standard	None
SG.IA-3	Authenticator Management	All	DHS-2.15.5	Protection 27	Yes	None	Access Control Standard	None
SG.IA-4	User Identification and Authentication	1,2,3,5,7,8,9,10,13,14,15,16	DHS-2.15.10	Protection 31	Yes	None	Access Control Standard	None
SG.IA-5	Device Identification and Authentication	1,2,3,7,8	DHS-2.15.11	Protection 30	Yes	KCPL-ISMS	None	None
SG.IA-6	Authenticator Feedback	1,2,3,5,7,8,9,10,13,14,15,16	DHS-2.15.14	Protection 30	No	None	None	None
SG.SD-1	Information and Document Management Policy and Procedures	All	DHS-2.9.1	Policy 6	Yes	None	None	Information Management Process
SG.SD-2	Information and Document Retention	All	DHS-2.9.2	Policy 6	Yes	None	None	Change Management Process, Framework Process
SG.SD-3	Information Handling	All	DHS-2.9.3	Policy 6	Yes	None	Confidentiality Protection Standard	None
SG.SD-4	Information Exchange	All	DHS-2.9.5	Policy 6	Yes	None	Remote Access Standard	Information Management Process
SG.SD-5	Automated Labeling	None	AMERP-2.9.1	Protection 35	No	None	None	None
SG.SI-1	Incident Response Policy and Procedures	All	DHS-2.11.1	Policy 6	Yes	KCPL-ISMS	Incident Response Standard	None
SG.SI-2	Incident Response Roles and Responsibilities	All	N/A	Policy 6	Yes	None	Incident Response Standard	None
SG.SI-3	Incident Response Training	All	AMERP-2.12.1	Policy 2	No	None	None	None
SG.SI-4	Incident Response Testing and Exercises	All	N/A	N/A	Yes	None	Incident Response Standard	None
SG.SI-5	Incident Handling	All	N/A	Policy 6	Yes	None	None	Remote Access Procedure

NISTIR 7628 Smart Grid Requirement Number	NISTIR 7268 Smart Grid Requirement Name	Applicable Interface Categories	UCAIug Security Profile for AMI	UCAIug Security Profile for DM	Requirement Fulfilled by KCP&L Policies, Standards, & Processes	KCP&L Policy Number(s)	KCP&L Standard(s)	KCP&L Process(s)
SG.SI-6	Incident Monitoring	All	N/A	Policy 6	Yes	None	Incident Response Standard	None
SG.SI-7	Incident Reporting	All	N/A	Policy 6	Yes	None	Incident Response Standard	None
SG.SI-8	Incident Response Investigation and Analysis	All	N/A	Policy 6	Yes	None	Incident Response Standard	None
SG.SI-9	Corrective Action	All	N/A	Policy 6	Yes	None	Incident Response Standard	None
SG.SI-10	Smart Grid Information System Backup	All	DHS-2.10.4	Policy 6	Yes	None	None	Backup and Recovery Process
SG.SI-11	Coordination of Emergency Response	All	N/A	N/A	Yes	None	Incident Response Standard	None
SG.MA-1	Smart Grid Information System Maintenance Policy and Procedures	All	DHS-2.10.1	Policy 6	Yes	None	Configuration Management Standard	Infrastructure Process
SG.MA-2	Legacy Smart Grid Information System Upgrades	All	DHS-2.10.3	Policy 6	Yes	None	None	Infrastructure Process
SG.MA-3	Smart Grid Information System Maintenance	All	DHS-2.10.6	Policy 7	Yes	None	Configuration Management Standard	Infrastructure Process
SG.MA-4	Maintenance Tools	All	AMERP-2.10.1	Policy 3	No	None	None	None
SG.MA-5	Maintenance Personnel	All	DHS-2.10.8	Policy 7	Yes	None	Remote Access Standard	None
SG.MA-6	Remote Maintenance	All	DHS-2.10.9	Policy 3	Yes	None	Remote Access Standard	None
SG.MA-7	Timely Maintenance	All	N/A	N/A	No	None	None	None
SG.MP-1	Media Protection Policy and Procedures	All	N/A	Policy 2	Yes	None	Confidentiality Protection Standard	None
SG.MP-2	Media Sensitivity Level	All	N/A	N/A	Yes	None	Confidentiality Protection Standard	None
SG.MP-3	Media Marking	All	N/A	Policy 6	Yes	None	Confidentiality Protection Standard	None
SG.MP-4	Media Storage	All	N/A	Policy 6	Yes	None	Confidentiality Protection Standard	None
SG.MP-5	Media Transport	All	N/A	Policy 6	Yes	None	Confidentiality Protection Standard	None
SG.MP-6	Media Sanitization and Disposal	All	N/A	Policy 6	Yes	None	Confidentiality Protection Standard	Asset Management Hardware Process
SG.PE-1	Physical and Environmental Security Policy and Procedures	All	N/A	Policy 2, Protection 2,3	No*	None	None	None
SG.PE-2	Physical Access Authorizations	All	N/A	Policy 6, Protection 2,3 Detection 1,2	No*	None	None	None
SG.PE-3	Physical Access	All	N/A	Policy 6, Protection 2,3 Detection 1,2 Response 1,2	No*	None	None	None
SG.PE-4	Monitoring Physical Access	All	N/A	Detection 1, Protection 2,3	No*	None	None	None
SG.PE-5	Visitor Control	All	N/A	Policy 6	No*	None	None	None
SG.PE-6	Visitor Records	All	N/A	Policy 6	No*	None	None	None
SG.PE-7	Physical Access Log Retention	All	N/A	Policy 6	No*	None	None	None
SG.PE-8	Emergency Shutoff Protection	All	N/A	Protection 8	No*	None	None	None
SG.PE-9	Emergency Power	All	N/A	Recovery 1, 2	No*	None	None	None
SG.PE-10	Delivery and Removal	All	N/A	N/A	No*	None	None	None
SG.PE-11	Alternate Work Site	All	N/A	Policy 6	No*	None	None	None

NISTIR 7628 Smart Grid Requirement Number	NISTIR 7268 Smart Grid Requirement Name	Applicable Interface Categories	UCAIug Security Profile for AMI	UCAIug Security Profile for DM	Requirement Fulfilled by KCP&L Policies, Standards, & Processes	KCP&L Policy Number(s)	KCP&L Standard(s)	KCP&L Process(s)
SG.PM-13	Incidents of Smart Grid Information System Assets	All	N/A	N/A	No*	None	None	None
SG.PL-1	Strategic Planning Policy and Procedures	All	N/A	Policy 1	Yes	None	None	Information Technology Planning Process
SG.PL-2	Smart Grid Information System Security Plan	All	N/A	Policy 2, Protection 42, 46	No	None	None	None
SG.PL-3	Rules of Behavior	All	N/A	Policy 2, Protection 2	Yes	KCP&L-ESM	None	None
SG.PL-4	Privacy Impact Assessment	All	N/A	N/A	No	None	None	None
SG.PL-5	Security-Related Activity Planning	All	N/A	Policy 4	Yes	None	None	Information Technology Planning Process
SG.PM-1	Security Policy and Procedures	All	N/A	Policy 1	Yes	KCP&L-ESM, KCP&L-SSM	System Lifecycle Management Security Standard	None
SG.PM-2	Security Program Plan	All	N/A	Policy 1	Yes	KCP&L-ESM, KCP&L-SSM	None	None
SG.PM-3	Senior Management Authority	All	N/A	N/A	Yes	KCP&L-ESM	None	None
SG.PM-4	Security Architecture	All	N/A	N/A	No	None	None	None
SG.PM-5	Risk Management Strategy	All	N/A	Policy 1	Yes	KCP&L-ESM	Cyber Risk Management Standard	None
SG.PM-6	Security Authorization to Operate Process	All	N/A	N/A	No	None	None	None
SG.PM-7	Mission/Business Process Definition	All	N/A	Policy 4	No	None	None	None
SG.PM-8	Management Accountability	All	N/A	Policy 2	Yes	None	System Lifecycle Management Security Standard	None
SG.PM-9	Personnel Security Policy and Procedures	All	N/A	Policy 3	Yes	KCP&L-ESM, KCP&L-SSM	System Lifecycle Management Security Standard	Access Management Process
SG.PS-1	Position Categorization	All	N/A	N/A	No	None	None	None
SG.PS-2	Personnel Screening	All	N/A	Policy 3	No	None	None	None
SG.PS-3	Personnel Termination	All	N/A	Policy 3	Yes	None	None	Access Management Process
SG.PS-4	Personnel Transfer	All	N/A	Policy 3	Yes	None	None	Access Management Process
SG.PS-5	Access Agreements	All	N/A	N/A	No	None	None	None
SG.PS-7	Contractor and Third-Party Personnel Security	All	N/A	N/A	Yes	None	Remote Access Standard	Access Management Process, Information Management Process
SG.PS-8	Personnel Accountability	All	N/A	Policy 2	Yes	Policy and Procedure Overview, KCP&L-ESM	None	None
SG.PS-9	Personnel Roles	All	N/A	N/A	Yes	Policy and Procedure Overview	None	None
SG.RA-1	Risk Assessment Policy and Procedures	All	N/A	Policy 5	Yes	KCP&L-ESM	Cyber Risk Management Standard, Vulnerability Assessment Standard	None
SG.RA-2	Risk Management Plan	All	N/A	Policy 5	Yes	KCP&L-ESM	Cyber Risk Management Standard, Vulnerability Assessment Standard	None
SG.RA-3	Security Impact Level	All	N/A	N/A	No	None	None	None
SG.RA-4	Risk Assessment	All	N/A	Policy 5	Yes	KCP&L-ESM	Cyber Risk Management Standard	None
SG.RA-5	Risk Assessment Update	All	N/A	Policy 5	Yes	None	Cyber Risk Management Standard	None

NISTIR 7628 Smart Grid Requirement Number	NISTIR 7268 Smart Grid Requirement Name	Applicable Interface Categories	UCAIug Security Profile for AMI	UCAIug Security Profile for DM	Requirement Fulfilled by KCP&L Policies, Standards, & Processes	KCP&L Policy Number(s)	KCP&L Standard(s)	KCP&L Process(s)
SG.RA-6	Vulnerability Assessment and Awareness	All	N/A	Policy 5, Protection 14	Yes	KCP&L-ESM	Vulnerability Assessment Standard, Vulnerability Management Standard	None
SG.SA-1	Smart Grid Information System and Services Acquisition Policy and Procedures	All	N/A	N/A	Yes	KCP&L-ESM	None	None
SG.SA-2	Security Policies for Contractors and Third Parties	All	N/A	Policy 2	Yes	None	Remote Access Standard	Access Management Process, Information Management Process
SG.SA-3	Life-Cycle Support	All	N/A	Policy 9	Yes	KCP&L-ESM	System Lifecycle Management Security Standard	PC Life Cycle Process, System Development Life Cycle Process
SG.SA-4	Acquisitions	All	N/A	Policy 9	Yes	KCP&L-ESM	None	None
SG.SA-5	Smart Grid Information System Documentation	All	N/A	Policy 9	Yes	None	System Lifecycle Management Security Standard	System Development Life Cycle Process
SG.SA-6	Software License Usage Restrictions	All	N/A	N/A	Yes	None	Configuration Management Standard	Software Management Process, PC Life Cycle Process
SG.SA-7	User-Installed Software	All	N/A	Policy 9	Yes	None	None	Software Management Process
SG.SA-8	Security Engineering Principles	All	N/A	Protection 40	Yes	None	System Lifecycle Management Security Standard	System Development Life Cycle Process
SG.SA-9	Developer Configuration Management	All	N/A	Policy 9, Protection 40	Yes	KCP&L-ESM	Change Control Standard	Change Management Process, System Development Life Cycle Process
SG.SA-10	Developer Security Testing	All	N/A	Policy 9	Yes	None	System Lifecycle Management Security Standard	System Development Life Cycle Process
SG.SA-11	Supply Chain Protection	All	N/A	N/A	No	None	None	None
SG.SC-1	Smart Grid Information System and Communication Protection Policy and Procedures	All	N/A	Policy 2	No	None	None	None
SG.SC-2	Communication Partitioning	None	DHS-2.8.2	Protection 10	No	None	None	None
SG.SC-3	Security Function Isolation	2,3,5,7,8,10,11,13,14	DHS-2.8.3	Protection 11	No	None	None	None
SG.SC-4	Information Remnants	7,8,10	DHS-2.8.4	Protection 10	No	None	None	None
SG.SC-5	Denial-of-Service Protection	2,3,5,7,8,10,11,13	DHS-2.8.5	Protection 10	No	None	None	None
SG.SC-6	Resource Priority	5,14	DHS-2.8.6	Protection 12	No	None	None	None
SG.SC-7	Boundary Protection	2,3,5,6,9,10,13,14,15,16	DHS-2.8.7	Policy 6	Yes	None	Confidentiality Protection Standard, Remote Access Standard	LAN Systems Process, Remote Access Process
SG.SC-8	Communication Integrity	All	DHS-2.8.8	Protection 11	Yes	None	Configuration Management Standard	Information Management Process, Remote Access Process
SG.SC-9	Communication Confidentiality	10,14,16	DHS-2.8.9	Protection 35	Yes	None	Confidentiality Protection Standard, Remote Access Standard	Remote Access Process
SG.SC-10	Trusted Path	None	DHS-2.8.10	N/A	No	None	None	None
SG.SC-11	Cryptographic Key Establishment and Management	All	DHS-2.8.11	Protection 15, 16	No	None	None	None
SG.SC-12	Use of Validated Cryptography	All	DHS-2.8.12	Policy 5, Protection 14	No	None	None	None
SG.SC-13	Collaborative Computing	All	DHS-2.8.13	N/A	No	None	None	None
SG.SC-14	Transmission of Security Parameters	None	DHS-2.8.14	N/A	No	None	None	None

NISTIR 7628 Smart Grid Requirement Number	NISTIR 7628 Smart Grid Requirement Name	Applicable Interface Categories	UCAIug Security Profile for AMI	UCAIug Security Profile for DM	Requirement Fulfilled by KCP&L Policies, Standards, & Processes	KCP&L Policy Number(s)	KCP&L Standard(s)	KCP&L Process(es)
SG.SC-15	Public Key Infrastructure Certificates	All	DMS-2.8.15	Policy 4	No	None	None	None
SG.SC-16	Mobile Code	All	DMS-2.8.16	Protection 22	No	None	None	None
SG.SC-17	Voice-Over Internet Protocol	None	DMS-2.8.17	Policy 9	No	None	None	None
SG.SC-18	System Connections	All	DMS-2.8.18	Policy 7	Yes	None	Remote Access Standard	Remote Access Process
SG.SC-19	Security Roles	All	DMS-2.8.19	Policy 3	No	None	None	None
SG.SC-20	Message Authenticity	All	DMS-2.8.20	Protection 17	No	None	None	None
SG.SC-21	Secure Name/Address Resolution Service	All	DMS-2.8.22	Policy 8	No	None	None	None
SG.SC-22	Fail in Known State	All	N/A	Protection 19	No	None	None	None
SG.SC-23	Thin Nodes	None	N/A	N/A	No	None	None	None
SG.SC-24	Honeypots	None	N/A	Detection 19	No	None	None	None
SG.SC-25	Operating System-Independent Applications	None	N/A	N/A	No	None	None	None
SG.SC-26	Confidentiality of Information at Rest	7,8,11,14,16	N/A	Policy 3	Yes	None	Access Control Standard	None
SG.SC-27	Heterogeneity	None	N/A	N/A	No	None	None	None
SG.SC-28	Virtualization Techniques	None	N/A	N/A	No	None	None	None
SG.SC-29	Application Partitioning	1,2,3,5,11,13,15	N/A	N/A	Yes	None	Access Management Standard	Infrastructure Process, LAN Systems Process
SG.SC-30	Smart Grid Information System Partitioning	All	N/A	N/A	Yes	None	Availability Protection Standard	None
SG.SI-1	Smart Grid Information System and Information Integrity Policy and Procedures	All	DMS-2.14.1	Policy 5	Yes	KCP&L 4508	None	Information Management Process
SG.SI-2	Flaw Remediation	All	DMS-2.14.2	Detection 15	No	None	None	None
SG.SI-3	Malicious Code and Spam Protection	All	DMS-2.14.3	Detection 16	Yes	KCP&L 4508	Anti-Virus Standard	Malicious Software Prevention Process
SG.SI-4	Smart Grid Information System Monitoring Tools and Techniques	All	DMS-2.14.4	Detection 19	Yes	KCP&L 4508	Anti-Virus Standard, Threat Monitoring Standard	Malicious Software Prevention Process, LAN Systems Process
SG.SI-5	Security Alerts and Advisories	All	DMS-2.14.5	Policy 6	Yes	KCP&L 4508	None	Malicious Software Prevention Process, LAN Systems Process
SG.SI-6	Security Functionality Verification	All	AMISP-2.14.1	N/A	No	None	None	None
SG.SI-7	Software and Information Integrity	1,2,3,5,7,8,9,10,11,13,14,15,16	DMS-2.14.7	Detection 16, 20, 21	Yes	None	Configuration Management Standard	Change Management Process, Configuration Management Process
SG.SI-8	Information Input Validation	All	AMISP-2.14.2	Detection 21	No	None	None	None
SG.SI-9	Error Handling	All	DMS-2.14.11	Detection 21, Protection 23	No	None	None	None

* - The physical security requirements in the NISTIR-7628 (PE Control Family) are not currently mandated in KCP&L policies, standards, and processes for any of the systems except for the EMS. In the case of EMS, it is believed that all 17 physical security requirements are currently mandated by KCP&L.

APPENDIX F SECURITY REQUIREMENTS FOR CONTROL SETS

NISTIR 7628 Smart Grid Requirement Number	NISTIR 7268 Smart Grid Requirement Name	Control Sets								
		C0	C1	C2	C3	C4	C5	C6	C7	C8
SG.AC-1	Access Control Policy and Procedures		X	X	X					
SG.AC-2	Remote Access Policy and Procedures		X	X	X					
SG.AC-3	Account Management		X	X	X					
SG.AC-4	Access Enforcement		X	X	X					
SG.AC-5	Information Flow Enforcement		X	X	X		X	X	X	X
SG.AC-6	Separation of Duties		X	X						
SG.AC-7	Least Privilege		X	X						
SG.AC-8	Unsuccessful Login Attempts		X	X	X	X				
SG.AC-9	Smart Grid Information System Use Notification		X	X	X					
SG.AC-10	Previous Logon Notification									
SG.AC-11	Concurrent Session Control		X	X						
SG.AC-12	Session Lock		X	X	X					
SG.AC-13	Remote Session Termination		X	X	X					
SG.AC-14	Permitted Actions without Identification or Authentication		X	X						
SG.AC-15	Remote Access		X	X	X					
SG.AC-16	Wireless Access Restrictions		X	X	X	X				
SG.AC-17	Access Control for Portable and Mobile Devices		X	X	X	X				
SG.AC-18	Use of External Information Control Systems	X								
SG.AC-19	Control System Access Restrictions		X							
SG.AC-20	Publicly Accessible Content	X								
SG.AC-21	Passwords	X								
SG.AT-1	Awareness and Training Policy and Procedures		X	X						
SG.AT-2	Security Awareness		X	X	X					
SG.AT-3	Security Training		X	X						
SG.AT-4	Security Awareness and Training Records		X							
SG.AT-5	Contact with Security Groups and Associations									
SG.AT-6	Security Responsibility Testing		X	X						
SG.AT-7	Planning Process Training									
SG.AU-1	Audit and Accountability Policy and Procedures		X	X						
SG.AU-2	Auditable Events		X	X						
SG.AU-3	Content of Audit Records		X	X						
SG.AU-4	Audit Storage Capacity		X	X						

NISTIR 7628 Smart Grid Requirement Number	NISTIR 7268 Smart Grid Requirement Name	Control Sets								
		C0	C1	C2	C3	C4	C5	C6	C7	C8
SG.AU-5	Response to Audit Processing Failures		X	X						
SG.AU-6	Audit Monitoring, Analysis, and Reporting		X	X						
SG.AU-7	Audit Reduction and Report Generation		X	X						
SG.AU-8	Time Stamps		X	X						
SG.AU-9	Protection of Audit Information		X	X						
SG.AU-10	Audit Record Retention		X	X						
SG.AU-11	Conduct and Frequency of Audits		X	X						
SG.AU-12	Auditor Qualification		X	X						
SG.AU-13	Audit Tools		X	X						
SG.AU-14	Security Policy Compliance	X								
SG.AU-15	Audit Generation									
SG.AU-16	Non-Repudiation									
SG.CA-1	Security Assessment and Authorization Policy and Procedures	X								
SG.CA-2	Security Assessments	X								
SG.CA-3	Continuous Improvement	X								
SG.CA-4	Smart Grid Information System Connections		X	X	X	X	X	X	X	X
SG.CA-5	Security Authorization to Operate	X				X				
SG.CA-6	Continuous Monitoring	X								
SG.CM-1	Configuration Management Policy and Procedures	X								
SG.CM-2	Baseline Configuration	X				X				
SG.CM-3	Configuration Change Control	X								
SG.CM-4	Monitoring Configuration Changes	X								
SG.CM-5	Access Restrictions for Configuration Change	X								
SG.CM-6	Configuration Settings	X				X				
SG.CM-7	Configuration for Least Functionality	X				X				
SG.CM-8	Component Inventory	X				X				
SG.CM-9	Addition, Removal, and Disposal of Equipment	X				X				
SG.CM-10	Factory Default Settings Management	X				X				
SG.CM-11	Configuration Management Plan	X								
SG.CP-1	Continuity of Operations Policy and Procedure	X				X				
SG.CP-2	Continuity of Operations Plan	X				X				
SG.CP-3	Continuity of Operations Roles and Responsibilities	X				X				
SG.CP-4	Continuity of Operations Training	X								

NISTIR 7628 Smart Grid Requirement Number	NISTIR 7268 Smart Grid Requirement Name	Control Sets								
		C0	C1	C2	C3	C4	C5	C6	C7	C8
SG.CP-5	Continuity of Operations Plan Testing	X				X				
SG.CP-6	Continuity of Operations Plan Update	X				X				
SG.CP-7	Alternate Storage Sites		X	X						
SG.CP-8	Alternate Telecommunication Services						X	X	X	
SG.CP-9	Alternate Control Center		X	X						
SG.CP-10	Smart Grid Information System Recovery and Reconstitution		X	X	X					
SG.CP-11	Fail-Safe Response		X	X						
SG.IA-1	Identification and Authentication Policy and Procedures	X								
SG.IA-2	Identifier Management	X								
SG.IA-3	Authenticator Management	X								
SG.IA-4	User Identification and Authentication		X	X	X					
SG.IA-5	Device Identification and Authentication		X	X	X	X	X	X	X	X
SG.IA-6	Authenticator Feedback	X								
SG.ID-1	Information and Document Management Policy and Procedures	X								
SG.ID-2	Information and Document Retention	X								
SG.ID-3	Information Handling	X								
SG.ID-4	Information Exchange	X								
SG.ID-5	Automated Labeling									
SG.IR-1	Incident Response Policy and Procedures	X								
SG.IR-2	Incident Response Roles and Responsibilities	X								
SG.IR-3	Incident Response Training	X								
SG.IR-4	Incident Response Testing and Exercises	X								
SG.IR-5	Incident Handling	X								
SG.IR-6	Incident Monitoring		X	X	X		X	X	X	
SG.IR-7	Incident Reporting	X								
SG.IR-8	Incident Response Investigation and Analysis	X								
SG.IR-9	Corrective Action	X								
SG.IR-10	Smart Grid Information System Backup		X	X	X					
SG.IR-11	Coordination of Emergency Response	X				X				
SG.MA-1	Smart Grid Information System Maintenance Policy and Procedures	X								
SG.MA-2	Legacy Smart Grid Information System Upgrades	X								
SG.MA-3	Smart Grid Information System Maintenance	X								

NISTIR 7628 Smart Grid Requirement Number	NISTIR 7268 Smart Grid Requirement Name	Control Sets								
		C0	C1	C2	C3	C4	C5	C6	C7	C8
SG.MA-4	Maintenance Tools	X								
SG.MA-5	Maintenance Personnel		X	X						
SG.MA-6	Remote Maintenance		X	X	X					
SG.MA-7	Timely Maintenance		X	X	X					
SG.MP-1	Media Protection Policy and Procedures	X								
SG.MP-2	Media Sensitivity Level	X								
SG.MP-3	Media Marking	X								
SG.MP-4	Media Storage	X								
SG.MP-5	Media Transport	X								
SG.MP-6	Media Sanitization and Disposal	X								
SG.PE-1	Physical and Environmental Security Policy and Procedures	X								
SG.PE-2	Physical Access Authorizations		X	X	X		X	X	X	
SG.PE-3	Physical Access		X	X	X		X	X	X	
SG.PE-4	Monitoring Physical Access		X	X	X		X	X	X	
SG.PE-5	Visitor Control		X	X	X		X	X	X	
SG.PE-6	Visitor Records		X	X	X		X	X	X	
SG.PE-7	Physical Access Log Retention		X	X	X		X	X	X	
SG.PE-8	Emergency Shutoff Protection	X								
SG.PE-9	Emergency Power				X				X	
SG.PE-10	Delivery and Removal		X	X	X					
SG.PE-11	Alternate Work Site		X	X						
SG.PE-12	Location of Smart Grid Information System Assets		X	X						
SG.PL-1	Strategic Planning Policy and Procedures	X				X				
SG.PL-2	Smart Grid Information System Security Plan	X				X				
SG.PL-3	Rules of Behavior	X								
SG.PL-4	Privacy Impact Assessment	X				X				
SG.PL-5	Security-Related Activity Planning	X				X				
SG.PM-1	Security Policy and Procedures	X				X				
SG.PM-2	Security Program Plan	X				X				
SG.PM-3	Senior Management Authority	X								

NISTIR 7628 Smart Grid Requirement Number	NISTIR 7268 Smart Grid Requirement Name	Control Sets								
		C0	C1	C2	C3	C4	C5	C6	C7	C8
SG.PM-4	Security Architecture	X								
SG.PM-5	Risk Management Strategy	X				X				
SG.PM-6	Security Authorization to Operate Process									
SG.PM-7	Mission/Business Process Definition	X				X				
SG.PM-8	Management Accountability	X								
SG.PS-1	Personnel Security Policy and Procedures	X								
SG.PS-2	Position Categorization		X	X	X					
SG.PS-3	Personnel Screening		X	X	X					
SG.PS-4	Personnel Termination	X								
SG.PS-5	Personnel Transfer	X								
SG.PS-6	Access Agreements	X								
SG.PS-7	Contractor and Third Party Personnel Security	X								
SG.PS-8	Personnel Accountability	X								
SG.PS-9	Personnel Roles	X								
SG.RA-1	Risk Assessment Policy and Procedures	X				X				
SG.RA-2	Risk Management Plan	X				X				
SG.RA-3	Security Impact Level	X				X				
SG.RA-4	Risk Assessment	X				X				
SG.RA-5	Risk Assessment Update	X				X				
SG.RA-6	Vulnerability Assessment and Awareness	X								
SG.SA-1	Smart Grid Information System and Services Acquisition Policy and Procedures		X	X	X					
SG.SA-2	Security Policies for Contractors and Third Parties	X								
SG.SA-3	Life-Cycle Support	X				X				
SG.SA-4	Acquisitions	X								
SG.SA-5	Smart Grid Information System Documentation	X								
SG.SA-6	Software License Usage Restrictions	X								
SG.SA-7	User-Installed Software	X								
SG.SA-8	Security Engineering Principles	X								
SG.SA-9	Developer Configuration Management	X								
SG.SA-10	Developer Security Testing	X								
SG.SA-11	Supply Chain Protection		X	X	X		X	X	X	X
SG.SC-1	Smart Grid Information System and Communication Protection Policy and Procedures	X								
SG.SC-2	Communications Partitioning	X								

NISTIR 7628 Smart Grid Requirement Number	NISTIR 7268 Smart Grid Requirement Name	Control Sets								
		C0	C1	C2	C3	C4	C5	C6	C7	C8
SG.SC-3	Security Function Isolation	X				X				
SG.SC-4	Information Remnants	X								
SG.SC-5	Denial-of-Service Protection		X	X	X	X				
SG.SC-6	Resource Priority									
SG.SC-7	Boundary Protection		X	X	X		X	X	X	X
SG.SC-8	Communication Integrity	X								
SG.SC-9	Communication Confidentiality		X	X	X		X	X	X	X
SG.SC-10	Trusted Path		X	X	X		X	X	X	X
SG.SC-11	Cryptographic Key Establishment and Management	X								
SG.SC-12	Use of Validated Cryptography	X								
SG.SC-13	Collaborative Computing									
SG.SC-14	Transmission of Security Parameters	X								
SG.SC-15	Public Key Infrastructure Certificates	X								
SG.SC-16	Mobile Code									
SG.SC-17	Voice-Over Internet Protocol									
SG.SC-18	System Connections	X								
SG.SC-19	Security Roles	X								
SG.SC-20	Message Authenticity	X								
SG.SC-21	Secure Name/Address Resolution Service									
SG.SC-22	Fail in Known State		X	X	X					
SG.SC-23	Thin Nodes									
SG.SC-24	Honeypots									
SG.SC-25	Operating System-Independent Applications									
SG.SC-26	Confidentiality of Information at Rest		X	X						
SG.SC-27	Heterogeneity	X								
SG.SC-28	Virtualization Techniques									
SG.SC-29	Application Partitioning		X	X	X					
SG.SC-30	Smart Grid Information System Partitioning	X								
SG.SI-1	Smart Grid Information System and Information Integrity Policy and Procedures	X								
SG.SI-2	Flaw Remediation									
SG.SI-3	Malicious Code and Spam Protection		X	X	X					
SG.SI-4	Smart Grid Information System Monitoring Tools and Techniques		X	X			X	X	X	X
SG.SI-5	Security Alerts and Advisories		X	X			X	X	X	X
SG.SI-6	Security Functionality Verification	X								

NISTIR 7628 Smart Grid Requirement Number	NISTIR 7268 Smart Grid Requirement Name	Control Sets								
		C0	C1	C2	C3	C4	C5	C6	C7	C8
SG.SI-7	Software and Information Integrity		X	X	X					
SG.SI-8	Information Input Validation	X								
SG.SI-9	Error Handling	X								

APPENDIX G SAMPLE QUESTIONNAIRE FOR HOSTING VENDORS

Service/Software/System Description	
Name of Service/System	
Short Description of Service/System	

Sponsoring Department	Name	
Lead Project Administrator		
Lead Technical Contact		
Additional KCP&L Contacts *list any additional administrative contacts or those providing technical support from other departments*	Name	Department

Hosting Service Provider			
Company Name			
Contacts	Name	Phone	Email Address
Administrative Representative			
Technical Contact			
Reference URL			
Additional Information Needed			

Data Classification Definitions

Restricted: Information for which inadvertent access or disclosure would have legal, regulatory, reputation, or financial repercussions. Access is limited to specific individuals.

Internal Use Only: Information that is generally available to employees and approved non-employees

Public: Information officially released for widespread public disclosure or considered to have value but no risk of unauthorized disclosure

Security Controls

1.0 HIGH LEVEL DESCRIPTION	
1.1	Please provide a brief description of the purpose of the system, including how the information will be used. If possible, include a simple diagram of the dataflow and where Restricted or Internal Use Only Data will be stored.

2.0 AUTHENTICATION			YES	NO
2.1	Will users of the hosted service be authenticated by KCP&L systems?			
2.2	Will users be authenticated by the hosting service provider?			
	2.2.1	Will userids assigned by the service provider match KCP&L userids?		
	2.2.2	Will each user have a unique userid?		
	2.2.3	Can the service provider's system be configured to require strong passwords?		
	2.2.4	Can KCP&L dictate password criteria as needed to ensure compliance with KCP&L security standards?		
	2.2.5	Can the service provider's system be configured to expire user passwords periodically in accordance with KCP&L security standards?		
	2.2.6	Does the service provider provide a function to enable users to change their own password securely?		
	2.2.7	Can accounts be locked after a KCP&L defined number of unsuccessful login attempts?		
	2.2.8	Can the service provider's system de-authenticate users after a KCP&L defined period of inactivity?		
	2.2.9	Does the hosted service provide a logout on-demand option?		
	2.2.10	Are passwords entered in a non-display field?		
	2.2.11	Are passwords encrypted during network transit?		
	2.2.12	Are passwords encrypted in storage?		
	2.2.13	Are all attempted and successful logins logged, include date/time, userid, source network address. and are maintained for at least one year?		

3.0 AUTHORIZATION – Logical Access Control			YES	NO
3.1	Will users be authorized by a KCP&L based system?			
3.2	Will users be authorized by the hosting service provider's system?			
	3.2.1	Does the service provider's system offer the ability to restrict access within the application based on roles assigned to authorized users?		
	3.2.2	Will the service provider's system provide easy to read security reports that identify users and their access levels for periodic review?		
	3.2.3	Can the authorization process be configured to automatically disable user accounts or access privileges after a KCP&L defined period of non-use?		
3.3	Can the service provider's security controls detect and report unauthorized access attempts?			

4.0 DATA SECURITY			YES	NO
4.1	Is all network transfer of KCP&L Restricted or Internal Use Only Data encrypted when traversing the service provider's network and the KCP&L network or non-KCP&L networks?			
4.2	Is all network transfer of KCP&L Restricted or Internal Use Only Data encrypted between multiple service providers' systems (e.g. web and database servers)?			
4.3	Is all physical transfer of KCP&L Restricted Data encrypted (e.g. backups to tape, disk, DVD)?			
4.4	Will any KCP&L Restricted or Internal Use Only Data be stored, temporarily or otherwise, on end-user workstations, portable devices, or removable media?			
	4.4.1	If so, will the data be stored encrypted using a strong encryption methodology?		
4.5	If encryption is used, are there procedures for key generation, distribution, storage, use, destruction, and archiving?			
4.6	Does the service provider's software provide appropriate controls to ensure data integrity (e.g. input validation, checksums of stored data, transaction redo logs)?			
4.7	Will the service provider's developers and systems administration staff who have access to KCP&L Restricted or Internal Use Only Data, have unique account IDs assigned to them?			

4.8	Are the duties of the service provider's technical staff separated to ensure least privilege and individual accountability?			
	4.8.1	Are there documented job descriptions that accurately reflect assigned duties and responsibilities and that segregate duties?		
4.9	Is the activity of service provider's technical staff logged when performing system maintenance?			
	4.9.1	If so, are activity logs maintained for at least one year?		
4.10	Is user-level access to KCP&L Restricted or Internal Use Only Data logged, monitored, and possible security violations investigated?			
	4.10.1	Can this log data be made available to KCP&L?		
	4.10.2	Does this log data specify the data element or data record accessed and the action taken upon the data (e.g. View, Modify, Delete)?		
	4.10.3	Can the log data support after-the-fact investigations detailing who, when, and how data or systems were accessed?		
	4.10.4	Will the service provider's system provide easy to read access audit reports for periodic review?		
	4.10.5	Will access to the audit reports be logged and strictly controlled?		

5.0 RECOVERABILITY		**YES**	**NO**
5.1	Is the service provider fully aware of KCP&L's recoverability objectives?		
5.2	Does the service provider have and follow a data and system backup plan commensurate with KCP&L's recoverability objective?		
5.3	Does the service provider have an adequate hardware maintenance contract or hot spare inventory to meet KCP&L's recoverability objective after a hardware failure?		
5.4	Does the service provider have the capability to execute a recovery from a security incident, complete system failure or destruction within the time-frame of KCP&L's recoverability objective?		
5.5	To what extent does the hosting service provider ensure system availability consistent with KCP&L's recoverability objectives? (e.g. backup power systems, redundant network paths, use of virtual machines, etc)		

6.0 OPERATIONAL CONTROLS			YES	NO
6.1	Does the service provider outsource hosting of their application and data storage servers to a third-party?			
6.2	Has the service provider taken measures to ensure the physical security of the data center(s) in which the application and data storage servers are housed, specifically addressing access controlled and audited entry ways, temperature monitoring and control, fire prevention and suppression, and use of a backup power source?			
6.3	If the service provider is currently providing hosting services for other clients, is multi-client access effectively controlled to ensure users are restricted to only the data they are authorized to access?			
6.4	Does the service provider maintain and apply host security standards on their servers and verify them whenever changes in configuration are introduced into the system?			
6.5	Does the service provider have and exercise a process to maintain current patch levels of software running on their systems?			
6.6	Does the service provider implement anti-malware controls on servers?			
6.7	Does the service provider practice effective electronic data destruction procedures when hardware is recycled for repair or removed for disposal?			
	8.6.1	If the service provider outsources information destruction services, is the outsourced destruction service a NAID Certified Operation? see: http://www.naidonline.org/certified_members.html		
	8.6.2	If the service provider outsources information destruction services, please specify the name and address of the outsourced vendor:		
6.8	What process will be provided to purge old records from service provider systems?			
6.9	Does the service provider have an information security audit or evaluation program for their operation?			
6.10	What methods are used to ensure the expertise of service provider employees who have access to KCP&L Restricted or Internal Use Only Data?			
6.11	What methods are used to ensure that service provider employees, who have access to KCP&L Restricted or Internal Use Only Data, have been properly vetted? (e.g. law enforcement background checks)			
6.12	Does the service provider have an effective procedure for timely termination of access of their staff and KCP&L users (upon notification) who no longer need access to the service provider's system?			

6.13	What methods are used by service provider staff for remote access to systems that store KCP&L Restricted or Internal Use Only Data?		
6.14	What administrative access will KCP&L IT workers have to hosted service on vendor systems?		
6.15	To what extent does the service provider test its software for security vulnerabilities, including conducting software penetration tests?		
6.16	Are tests and examinations of key controls routinely made, i.e., network scans, analyses of router and switch settings, penetration testing?		

7.0 INCIDENT RESPONSE		**YES**	**NO**
7.1	Does the service provider have a documented process for reporting security incidents involving systems used to store/access/modify hosted KCP&L data to the KCP&L Department contact or, if appropriate, law enforcement?		
7.2	Are security incidents monitored and tracked until resolved?		
7.3	Is incident information and common vulnerabilities or threats shared with owners of interconnected systems or data hosting customers?		
7.4	Will a third party ever have access to the service provider's hardware or systems that store KCP&L Restricted or Internal Use Only Data?		
7.5	Are the service provider's database and web server access and error logs regularly reviewed for anomalies that could indicate a compromise?		
7.6	What process does the service provider have in place to identify security breaches on vendor managed systems (e.g. file integrity checks)?		
7.7	In the case of a security breach or unexpected exposure of KCP&L Restricted or Internal Use Only Data, what are the hosting service provider's incident response procedures?		
7.8	What is the service provider's process for disclosing to KCP&L any data requests, such as subpoenas or warrants, from a third party?		

8.0 APPLICATION SECURITY			YES	NO
8.1	Does the software development life-cycle model used by the hosting service provider in the development of their software, incorporate features from any standards based framework models (e.g. TSP-Secure, SAMM, Microsoft SDL, OWASP, NIST SP800-64 rev 2,)? If so, please specify.			
	8.1.1	Are security components identified and represented during each phase of the software development life -cycle?		
8.2	Does the service provider have change management policies in place?			
	8.2.1	Is a pre-determined maintenance window used to apply changes?		
	8.2.2	How much lead-time will the service provider give KCP&L of upcoming changes?		
	8.2.3	How are customers notified of changes?		
	8.2.4	Does the service provider have a process to test their software for anomalies when new operating system patches are applied?		
	8.2.5	Has a technical and/or security evaluation been completed or conducted when a significant change occurred?		
8.3	Are source code audits performed regularly?			
	8.3.1	Are source code audits performed by someone other than the person or team that wrote the code?		
8.4	Is access to the service provider's application restricted to encrypted channels (e.g. https)?			
8.5	Describe the session management processes used by the hosted service's applications.			

9.0 TESTING AND VALIDATION			YES	NO
9.1	Are risk assessments performed and documented on a regular basis or whenever the system, facilities, or other conditions change?			
9.2	Can the hosting service provider make available a test evaluation instance of their service or application that can be used by KCP&L IT security staff to validate the information security assertions made by the vendor?			
	9.2.1	Can the test evaluation instance include access at both the user-level interface and management-level interface?		

APPENDIX H UNCONFIRMED SECURITY REQUIREMENTS FROM UCAIUG AMI AND DM SECURITY PROFILES

UCAIug AMI Security Profile Requirement	Requirement Title
DHS-2.8.21	Architecture and Provisioning for Name/Address Resolution Service
DHS-2.8.23	Secure Name/Address Resolution Service (Recursive or Caching Resolver)
AMISP-2.8.1	Secure Name/Address Resolution Service (Address Resolution Tampering)
DHS-2.9.4	Information Classification
DHS-2.9.6	Information and Document Classification
DHS-2.9.7	Information and Document Retrieval
DHS-2.9.8	Information and Document Destruction
DHS-2.9.9	Information and Document Management Review
DHS-2.10.3	System Monitoring and Evaluation
DHS-2.10.5	Unplanned System Maintenance
DHS-2.14.8	Unauthorized Communications Protection
DHS-2.14.9	Information Input Restrictions
DHS-2.14.12	Information Output Handling and Retention
AMISP-2.15.1	Supervision and Review
DHS-2.15.14	Cryptographic Module Authentication
DHS-2.15.27	Untrusted IT Equipment
DHS-2.15.28	External Access Protections
AMISP-2.15.2	Unauthorized Access Reporting
AMISP-2.17.1	Delay of Remote Connect/Disconnect

Source: The Advanced Security Acceleration Project for the Smart Grid (ASAP-SG) - Security Profile for Advanced Metering Infrastructure V2.0

UCAIug DM Security Profile Requirement	Requirement Title
Network.1	DM Networks are Private
Network.5	Redundancy
Network.6	Emergency Network Segmentation
Detection.3	Electronic Log Format
Detection.4	Power Source Monitoring/Logging
Detection.5	Location of Mobile Components
Detection.6	Fire Detection
Detection.9	Self Identification
Detection.17	Firmware/Configuration Authenticity
Detection.22	Message Delay Detection
Detection.23	Device Self Test
Detection.24	Heartbeat
Detection.27	Inappropriate User Activity
Detection.29	IDS Architecture
Detection.30	Physical Access Indications
Detection.32	Message Validation
Protection.5	Power Sources and Cables
Protection.6	Component Location
Protection.7	Control Center Location
Protection.8	EMI/Surge Protection
Protection.14	Remote Interactive Sessions
Protection.18	Addressing
Protection.23	Disabling Unnecessary Communication Services
Protection.24	No Internet Access
Protection.34	Cryptographic Module Authentication
Protection.41	Wireless Encryption
Protection.43	WAN Communication Outage
Protection.45	Non-adjacent Network Restrictions
Protection.47	Centralized Authentication
Protection.49	Message Identities
Protection.50	Data Point State Indicators
Protection.52	Application Layer Security
Protection.53	Separate Keys for Separate Functions
Reaction.3	Physical Access Correlation
Reaction.4	Unscheduled or Unapproved Activity

UCAIug DM Security Profile Requirement	Requirement Title
Reaction.7	End Point Isolation
Recovery 4	Rebuild System

Source: The Advanced Security Acceleration Project for the Smart Grid (ASAP-SG) - Security Profile for Distribution Management V0.9

APPENDIX I ADDITIONAL REFERENCES

- Standards for Security Categorization of Federal Information and Information Systems. FIPS PUB 199. http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
- Creating a Patch and Vulnerability Management Program. National Institute of Standards and Technology (NIST) Special Publication 800-40 Version 2.0. http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf
- Study of Security Attributes of Smart Grid Systems Current Cyber Security Issues April 2009. Idaho National Lab (INL) Critical Infrastructure Protection/Resilience Center. U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability. http://www.inl.gov/scada/publications/d/securing_the_smart_grid_current_issues.pdf
- Recommended Security Controls for Federal Information Systems and Organizations. National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 3. http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf
- Guide to Industrial Control Systems (ICS) Security. Recommendations of the National Institute of Standards and Technology (NIST) Special Publication 800-82. http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

This page intentionally blank

Appendix N Cyber Security Controls Matrix

Legend (Non-Network Requirements)
For each control that was found to be applicable to a system ("Yes"), the cell is shaded a specific color to indicate the following:
Green indicates that the requirement is the responsibility of the vendor(s) to implement.
Yellow indicates that the requirement is the responsibility of both KCP&L and the vendor(s) to implement.
Blue indicates that the requirement is the responsibility of KCP&L to implement.

Cyber Security Controls Matrix										
Requirement Number	Requirement Name	Req. Type	NTWK	MDM	AMI	DERM	HEMP	DMS	DCADA DDC	BESS
SG.AC-1	Access Control Policy and Procedures	Admin	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.AC-2	Remote Access Policy and Procedures	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.AC-3	Account Management	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.AC-4	Access Enforcement	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.AC-5	Information Flow Enforcement	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.AC-6	Separation of Duties	Tech	No	Yes	Yes	Yes	Yes	Yes	Yes	No
SG.AC-7	Least Privilege	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
SG.AC-8	Unsuccessful Login Attempts	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.AC-9	Smart Grid Information System Use Notification	Tech	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.AC-10	Previous Logon Notification	Tech	No	No	No	No	No	No	No	No
SG.AC-11	Concurrent Session Control	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.AC-12	Session Lock	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.AC-13	Remote Session Termination	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.AC-14	Permitted Actions without Identification or Authentication	Tech	No	Yes	Yes	Yes	Yes	Yes	Yes	No
SG.AC-15	Remote Access	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.AC-16	Wireless Access Restrictions	Tech	No	No	Yes	No	Yes	No	Yes	Yes
SG.AC-17	Access Control for Portable and Mobile Devices	Tech	No	No	No	No	Yes	No	No	No
SG.AC-18	Use of External Information Control Systems	Admin	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Cyber Security Controls Matrix										
Requirement Number	Requirement Name	Req. Type	NTWK	MDM	AMI	DERM	HEMP	DMS	DCADA DDC	BESS
SG.AC-19	Control System Access Restrictions	Admin	Yes	No	No	No	No	Yes	No	No
SG.AC-20	Publicly Accessible Content	Admin	No	No	No	No	No	No	No	No
SG.AC-21	Passwords	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.AT-1	Awareness and Training Policy and Procedures	Admin	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.AT-2	Security Awareness	Admin	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.AT-3	Security Training	Admin	No	Yes	Yes	Yes	Yes	Yes	Yes	No
SG.AT-4	Security Awareness and Training Records	Admin	No	No	No	No	No	No	No	No
SG.AT-5	Contact with Security Groups and Associations	Admin	No	No	No	No	No	No	No	No
SG.AT-6	Security Responsibility Testing	Admin	No	Yes	Yes	Yes	Yes	Yes	Yes	No
SG.AT-7	Planning Process Training	Admin	No	No	No	No	No	No	No	No
SG.AU-1	Audit and Accountability Policy and Procedures	Admin	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.AU-2	Auditable Events	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.AU-3	Content of Audit Records	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.AU-4	Audit Storage Capacity	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.AU-5	Response to Audit Processing Failures	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.AU-6	Audit Monitoring, Analysis, and Reporting	Admin	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.AU-7	Audit Reduction and Report Generation	Admin	No	No	No	No	No	No	No	No
SG.AU-8	Time Stamps	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.AU-9	Protection of Audit Information	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.AU-10	Audit Record Retention	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.AU-11	Conduct and Frequency of Audits	Admin	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.AU-12	Auditor Qualification	Admin	No	No	No	No	No	Yes	Yes	Yes
SG.AU-13	Audit Tools	Admin	No	No	No	No	No	No	No	No
SG.AU-14	Security Policy Compliance	Admin	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.AU-15	Audit Generation	Tech	No	No	No	No	No	No	No	No
SG.AU-16	Non-Repudiation	Tech	No	No	No	No	No	No	No	No
SG.CA-1	Security Assessment and Authorization Policy and Procedures	Admin	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Cyber Security Controls Matrix										
Requirement Number	Requirement Name	Req. Type	NTWK	MDM	AMI	DERM	HEMP	DMS	DCADA DDC	BESS
SG.CA-2	Security Assessments	Admin	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.CA-3	Continuous Improvement	Admin	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.CA-4	Smart Grid Information System Connections	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.CA-5	Security Authorization to Operate	Admin	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.CA-6	Continuous Monitoring	Admin	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.CM-1	Configuration Management Policy and Procedures	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.CM-2	Baseline Configuration	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.CM-3	Configuration Change Control	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.CM-4	Monitoring Configuration Changes	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.CM-5	Access Restrictions for Configuration Change	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.CM-6	Configuration Settings	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.CM-7	Configuration for Least Functionality	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.CM-8	Component Inventory	Tech	Yes	No	No	No	No	Yes	Yes	Yes
SG.CM-9	Addition, Removal, and Disposal of Equipment	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.CM-10	Factory Default Settings Management	Admin	Yes	No	No	No	No	Yes	Yes	Yes
SG.CM-11	Configuration Management Plan	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.CP-1	Continuity of Operations Policy and Procedure	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.CP-2	Continuity of Operations Plan	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.CP-3	Continuity of Operations Roles and Responsibilities	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.CP-4	Continuity of Operations Training	Admin	Yes	No	No	No	No	Yes	Yes	Yes
SG.CP-5	Continuity of Operations Plan Testing	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.CP-6	Continuity of Operations Plan Update	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.CP-7	Alternate Storage Sites	Admin	No	No	No	No	No	Yes	Yes	No
SG.CP-8	Alternate Telecommunication Services	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.CP-9	Alternate Control Center	Admin	Yes	No	No	No	No	No	No	No

Cyber Security Controls Matrix										
Requirement Number	Requirement Name	Req. Type	NTWK	MDM	AMI	DERM	HEMP	DMS	DCADA DDC	BESS
SG.CP-10	Smart Grid Information System Recovery and Reconstitution	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.CP-11	Fail-Safe Response	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.IA-1	Identification and Authentication Policy and Procedures	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.IA-2	Identifier Management	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.IA-3	Authenticator Management	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.IA-4	User Identification and Authentication	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.IA-5	Device Identification and Authentication	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.IA-6	Authenticator Feedback	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.ID-1	Information and Document Management Policy and Procedures	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.ID-2	Information and Document Retention	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.ID-3	Information Handling	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.ID-4	Information Exchange	Admin	No	Yes	Yes	Yes	Yes	No	No	No
SG.ID-5	Automated Labeling	Admin	No	No	No	No	No	No	No	No
SG.IR-1	Incident Response Policy and Procedures	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.IR-2	Incident Response Roles and Responsibilities	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.IR-3	Incident Response Training	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.IR-4	Incident Response Testing and Exercises	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.IR-5	Incident Handling	Admin	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.IR-6	Incident Monitoring	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.IR-7	Incident Reporting	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.IR-8	Incident Response Investigation and Analysis	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.IR-9	Corrective Action	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.IR-10	Smart Grid Information System Backup	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Cyber Security Controls Matrix										
Requirement Number	Requirement Name	Req. Type	NTWK	MDM	AMI	DERM	HEMP	DMS	DCADA DDC	BESS
SG.IR-11	Coordination of Emergency Response	Admin	No	No	No	No	No	Yes	Yes	Yes
SG.MA-1	Smart Grid Information System Maintenance Policy and Procedures	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.MA-2	Legacy Smart Grid Information System Upgrades	Admin	No	No	No	No	No	No	No	No
SG.MA-3	Smart Grid Information System Maintenance	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.MA-4	Maintenance Tools	Admin	Yes	No	No	No	No	No	No	No
SG.MA-5	Maintenance Personnel	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.MA-6	Remote Maintenance	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.MA-7	Timely Maintenance	Admin	Yes	No	No	No	No	No	No	No
SG.MP-1	Media Protection Policy and Procedures	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.MP-2	Media Sensitivity Level	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.MP-3	Media Marking	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.MP-4	Media Storage	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.MP-5	Media Transport	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.MP-6	Media Sanitization and Disposal	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.PE-1	Physical and Environmental Security Policy and Procedures	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.PE-2	Physical Access Authorizations	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.PE-3	Physical Access	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.PE-4	Monitoring Physical Access	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.PE-5	Visitor Control	Admin	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.PE-6	Vistor Records	Admin	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.PE-7	Physical Access Log Retention	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.PE-8	Emergency Shutoff Protection	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.PE-9	Emergency Power	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.PE-10	Delivery and Removal	Admin	Yes	No	No	No	No	Yes	Yes	Yes
SG.PE-11	Alternate Work Site	Admin	No	No	No	No	No	No	No	No
SG.PE-12	Location of Smart Grid Information System Assets	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.PL-1	Strategic Planning Policy and Procedures	Admin	Yes	No	No	No	No	Yes	Yes	Yes

Cyber Security Controls Matrix										
Requirement Number	Requirement Name	Req. Type	NTWK	MDM	AMI	DERM	HEMP	DMS	DCADA DDC	BESS
SG.PL-2	Smart Grid Information System Security Plan	Admin	Yes	No	No	No	No	Yes	Yes	Yes
SG.PL-3	Rules of Behavior	Admin	Yes	No	No	No	No	Yes	Yes	Yes
SG.PL-4	Privacy Impact Assessment	Admin	No	No	No	No	Yes	No	No	No
SG.PL-5	Security-Related Activity Planning	Admin	Yes	No	No	No	No	Yes	Yes	Yes
SG.PM-1	Security Policy and Procedures	Admin	Yes	No	No	No	No	Yes	Yes	Yes
SG.PM-2	Security Program Plan	Admin	Yes	No	No	No	No	Yes	Yes	Yes
SG.PM-3	Senior Management Authority	Admin	Yes	No	No	No	No	Yes	Yes	Yes
SG.PM-4	Security Architecture	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.PM-5	Risk Management Strategy	Admin	Yes	No	No	No	No	Yes	Yes	Yes
SG.PM-6	Security Authorization to Operate Process	Admin	No	No	No	No	No	No	No	No
SG.PM-7	Mission/Business Process Definition	Admin	Yes	No	No	No	No	No	No	No
SG.PM-8	Management Accountability	Admin	Yes	Yes	Yes	Yes	Yes	No	No	No
SG.PS-1	Personnel Security Policy and Procedures	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.PS-2	Position Categorization	Admin	Yes	No	No	No	No	No	No	No
SG.PS-3	Personnel Screening	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.PS-4	Personnel Termination	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.PS-5	Personnel Transfer	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.PS-6	Access Agreements	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.PS-7	Contractor and Third-Party Personnel Security	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.PS-8	Personnel Accountability	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.PS-9	Personnel Roles	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.RA-1	Risk Assessment Policy and Procedures	Admin	Yes	No	No	No	No	Yes	Yes	Yes
SG.RA-2	Risk Management Plan	Admin	Yes	No	No	No	No	Yes	Yes	Yes
SG.RA-3	Security Impact Level	Admin	Yes	No	No	No	No	Yes	Yes	Yes
SG.RA-4	Risk Assessment	Admin	Yes	No	No	No	No	Yes	Yes	Yes
SG.RA-5	Risk Assessment Update	Admin	Yes	No	No	No	No	Yes	Yes	Yes
SG.RA-6	Vulnerability Assessment and Awareness	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Cyber Security Controls Matrix										
Requirement Number	Requirement Name	Req. Type	NTWK	MDM	AMI	DERM	HEMP	DMS	DCADA DDC	BESS
SG.SA-1	Smart Grid Information System and Services Acquisition Policy and Procedures	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SA-2	Security Policies for Contractors and Third Parties	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SA-3	Life-Cycle Support	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SA-4	Acquisitions	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SA-5	Smart Grid Information System Documentation	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SA-6	Software License Usage Restrictions	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SA-7	User-Installed Software	Admin	Yes	No	No	No	No	Yes	Yes	Yes
SG.SA-8	Security Engineering Principles	Admin	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SA-9	Developer Configuration Management	Admin	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SA-10	Developer Security Testing	Tech	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SA-11	Supply Chain Protection	Tech	Yes	No	No	No	No	No	No	No
SG.SC-1	Smart Grid Information System and Communication Protection Policy and Procedures	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SC-2	Communications Partitioning	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SC-3	Security Function Isolation	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SC-4	Information Remnants	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SC-5	Denial-of-Service Protection	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SC-6	Resource Priority	Tech	No	No	No	No	No	No	No	No
SG.SC-7	Boundary Protection	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SC-8	Communication Integrity	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SC-9	Communication Confidentiality	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SC-10	Trusted Path	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SC-11	Cryptographic Key Establishment and Management	Tech	No	No	No	No	No	Yes	Yes	Yes
SG.SC-12	Use of Validated Cryptography	Tech	No	No	No	No	No	Yes	Yes	Yes
SG.SC-13	Collaborative Computing	Admin	No	No	No	No	No	No	No	No
SG.SC-14	Transmission of Security Parameters	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Cyber Security Controls Matrix										
Requirement Number	Requirement Name	Req. Type	NTWK	MDM	AMI	DERM	HEMP	DMS	DCADA DDC	BESS
SG.SC-15	Public Key Infrastructure Certificates	Tech	No	No	No	No	No	Yes	Yes	Yes
SG.SC-16	Mobile Code	Tech	No	No	No	No	No	No	No	No
SG.SC-17	Voice-Over Internet Protocol	Tech	No	No	No	No	No	No	No	No
SG.SC-18	System Connections	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SC-19	Security Roles	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SC-20	Message Authenticity	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SC-21	Secure Name/Address Resolution Service	Tech	No	No	No	No	No	No	No	No
SG.SC-22	Fail in Known State	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SC-23	Thin Nodes	Tech	No	No	No	No	No	No	No	No
SG.SC-24	Honeypots	Tech	No	No	No	No	No	No	No	No
SG.SC-25	Operating System-Independent Applications	Tech	No	No	No	No	No	No	No	No
SG.SC-26	Confidentiality of Information at Rest	Tech	No	Yes	Yes	Yes	Yes	Yes	Yes	No
SG.SC-27	Heterogeneity	Tech	No	No	No	No	No	No	No	No
SG.SC-28	Virtualization Techniques	Tech	Yes	No	No	No	No	No	No	No
SG.SC-29	Application Partitioning	Tech	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SC-30	Smart Grid Information System Partitioning	Tech	Yes	Yes	Yes	Yes	Yes	No	No	No
SG.SI-1	Smart Grid Information System and Information Integrity Policy and Procedures	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SI-2	Flaw Remediation	Tech	Yes	No	No	No	No	Yes	Yes	Yes
SG.SI-3	Malicious Code and Spam Protection	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SI-4	Smart Grid Information System Monitoring Tools and Techniques	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SI-5	Security Alerts and Advisories	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SI-6	Security Functionality Verification	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SI-7	Software and Information Integrity	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SI-8	Information Input Validation	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SI-9	Error Handling	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Appendix O AMI Audit Results

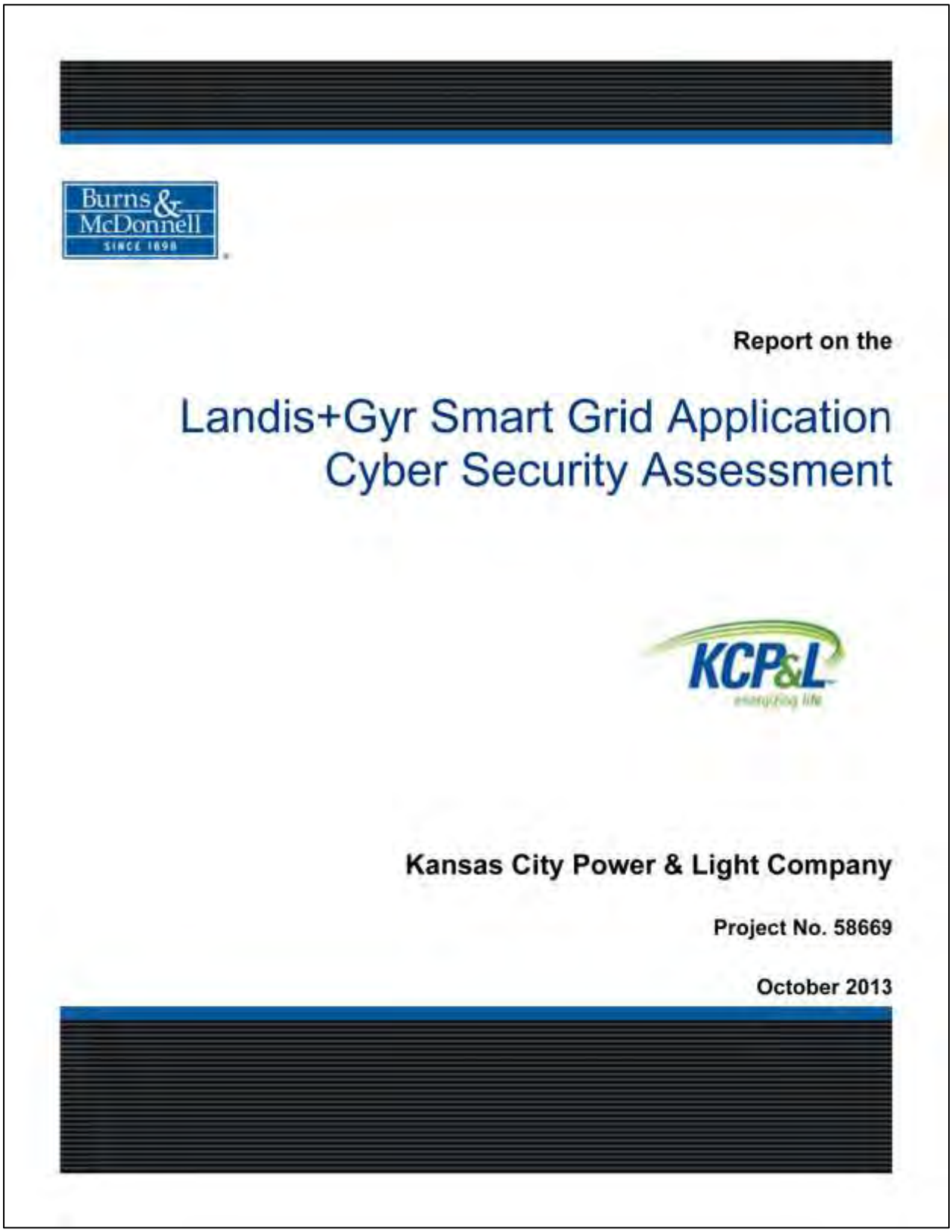


TABLE OF CONTENTS

Issue Date	Description
August 9, 2013	Original version issued to KCP&L
October 22, 2013	Various modifications based upon review with KCP&L

1.0 EXECUTIVE SUMMARY

Kansas City Power & Light Company (KCP&L) retained Burns & McDonnell to conduct an assessment of Smart Grid application vendor Landis+Gyr and their Command Center application used by KCP&L as their Advanced Metering Infrastructure Head-End (AIIE). The purpose of this assessment is to determine Landis+Gyr's capabilities to host KCP&L Smart Grid application(s) and adherence to application controls, policies, processes and procedures in accordance with the NISTIR 7628 guidelines. The security controls for the wireless field area network that Landis+Gyr hosts and the backhaul of data from the wireless field area network to Landis+Gyr's datacenters is outside the scope of this report. This report focuses on the security controls for the application hosted within Landis+Gyr's datacenters. The assessment approach includes four phases: Pre-Verification Data Collection and Review, On-Site Verification, Analysis, and Report Generation and Delivery.

The assessment results contained in this report are designed to meet the following objectives:

- Evaluate Smart Grid Project application(s) hosting services
- Demonstrate to the Department of Energy that KCP&L is on target in meeting its expectations with assessing security for the Smart Grid Project application(s)
- Gap Analysis of Smart Grid Project application(s) maturity towards meeting adherence to the NISTIR 7628 guidelines

Based on the results of Pre-Assessment Data Collection, On-Site Verification and Analysis, the assessment team has concluded that the Landis+Gyr Command Center (AIIE) application and Landis+Gyr practices are ***satisfactory*** in the assessed areas of Cyber Security and Information Technology controls. Landis+Gyr demonstrated a vigorous cyber security program that utilizes industry best practices. Landis+Gyr currently complies with 115 of the 116 applicable NISTIR 7628 security control requirements and satisfies the standards/guidelines for twenty-two (22) areas of Cyber Security and Information Technology controls. The only applicable NISTIR 7628 security control requirement that Landis+Gyr does not currently comply with is AC-11 (Concurrent Session Control). Landis+Gyr has acknowledged that they currently do not meet this requirement and has identified a path to resolution for this requirement in their future feature enhancement roadmap.

Descriptions of the assessment and the assessment results are provided in Sections 2.0 through 5.0 of this report.

2.0 INTRODUCTION

2.1 Scope and Objective

Kansas City Power & Light Company (KCP&L), as part of the KCP&L Smart Grid Project, is conducting assessments of Smart Grid application vendors to determine their capabilities to host KCP&L Smart Grid application(s) and adherence to application controls, policies, processes and procedures in accordance with the NISTIR 7628 guidelines. The assessment approach includes four phases for each vendor: Pre-Verification Data Collection and Review, On-Site Verification, Analysis, and Report Generation and Delivery.

KCP&L retained Burns & McDonnell to conduct an assessment of Smart Grid application vendor Landis+Gyr and their Command Center application used by KCP&L as their Advanced Metering Infrastructure Head-End (AHE). The security controls for the wireless field area network that Landis+Gyr hosts and the backhaul of data from the wireless field area network to Landis+Gyr's datacenters is outside the scope of this report. This report focuses on the security controls for the application hosted within Landis+Gyr's datacenters. This report includes the assessment results of Phase I - III (Data Collection, On-Site Verification, and Analysis) and serves as completion of Phase IV (Report Generation and Delivery) for the Landis+Gyr Smart Grid application assessment. A summary of the results for Phase I through Phase III of the assessment can be found in Section 4.0 of this report.

The assessment results contained in this report are designed to meet the following objectives:

- Evaluate Smart Grid Project application(s) hosting services
- Demonstrate to the Department of Energy that KCP&L is on target in meeting its expectations with assessing security for the Smart Grid Project application(s)
- Gap Analysis of Smart Grid Project application(s) maturity towards meeting adherence to the NISTIR 7628 guidelines

2.2 Assessment Participants

Table 2-1: Landis+Gyr Smart Grid Assessment Participants

Name	Company	Responsibility	Contact Information
Jim Blake	Landis+Gyr	Director, Customer Operations	Jim.Blake@landisgyr.com
Connie Cockriel-Collison	Landis+Gyr	Manager, Technical Services	Connie.Cockriel-Collison@landisgyr.com
Jon Anthony	Landis+Gyr	Manager, Network Services	Jonathan.Anthony@landisgyr.com
Tracy Jefferson	Landis+Gyr	Project Manager	Tracy.Jefferson@landisgyr.com

Name	Company	Responsibility	Contact Information
Brad Caraway	Landis+Gyr	Security Engineer	Brad.Caraway@landisgyr.com
George Throener	Landis+Gyr	Supervisor, Systems Admin	George.Throener@landisgyr.com
Al Pruitt	Landis+Gyr	Supervisor, Network Admin	Al.Pruitt@landisgyr.com
Hugh Head	Landis+Gyr	Sr. Product Manager	Hugh.Head@landisgyr.com
Mike DelCampo	Landis+Gyr	Technical Implementation Manager	Michael.DelCampo@landisgyr.com
Jeff Ethier	Landis+Gyr	Sr. Technical Business Analyst	Jeff.Ethier@landisgyr.com
Kevin Lane	Landis+Gyr	Technical Business Analyst	Kevin.Lane@landisgyr.com
Justin Higdon	KCP&L	Senior Information Security Analyst	Justin.Higdon@kcpl.com
Ed Hedges	KCP&L	Manager of Smart Grid Technical Planning	Ed.Hedges@kcpl.com
Matthew Milligan	Burns & McDonnell/ KCP&L	Network/Security Analyst	Matt.Milligan@kcpl.com MMilligan@burnsmcd.com
Peter Gonzalez	Burns & McDonnell	Senior System Security Engineer	PMGonzalez@burnsmcd.com

3.0 AMI & LANDIS+GYR COMMAND CENTER APPLICATION

This section contains an overview of Advanced Metering Infrastructure (AMI) and the Landis+Gyr Command Center (AHE) Application.

3.1 AMI Overview

The Landis+Gyr Gridstream Smart Grid communication system and Smart Meters provide the building blocks for Advanced Metering Infrastructure (AMI) and Home Area Networks (HAN) via a common two-way communication infrastructure. The Gridstream system supports the acquisition of load profile, time-of-use and demand meter data, and meter and site diagnostic information from the electric meters that perform these measurements. Using meters equipped with these capabilities, the system also supports "under-glass" remote physical disconnect and HAN communication via the ZigBee- standard Smart Energy Profile. Smart Meters also support outage and restoration reporting and real-time on-demand reads.

The Landis+Gyr AMI is composed of two main components: Command Center – the AMI Head-End System (AHE) and the Gridstream Wireless Field Area Network (FAN). The AHE is the software and hardware that allows the utility to interact with the AMI and integrate the AMI with other systems within the utility. The FAN is the hardware (collectors, routers, and meters) that enables the utility to receive meter data and send commands to meters.

3.2 Command Center – The AMI Head-End (AHE) System

The Gridstream AHE is the advanced metering software and hardware platform that enables data reporting and system control between it and the FAN. The scalable system enables KCP&L to remotely program meters, manage remote connects/disconnects, analyze critical peak usage, view load control indices, and perform other critical, day-to-day functional operations. The AHE simultaneously manages the meter data collected from all Smart Meters within the Smart Grid Project area, validating each data element, and integrates the data with the Meter Data Management system (MDM). The Gridstream AHE is compliant with the Multispeak, CIM, and IEC CIM 61968 standards. It also utilizes Web Service Application Programming Interfaces (APIs) to interface with other systems and can deliver specific scheduled data extracts to these systems.

4.0 SECURITY ASSESSMENT RESULTS

This section contains a detailed summary of the cyber security assessment conducted on the Landis+Gyr Command Center (AHE) application. The assessment was conducted in four phases: Pre-Verification Data Collection and Review, On-Site Verification, Analysis and Report Generation and Delivery.

4.1 Phase I: Pre-Verification Data Collection

In the first phase of the assessment, the assessment team submitted a data request to Landis+Gyr to gather data about their Smart Grid application product offerings and how well they adhere to the NISTIR 7628 guidelines. The data request included:

1. Completion of a security questionnaire that included all applicable NISTIR 7628 requirements (118 in total)
2. A detailed list of servers and work stations that would be used for hosting the KCP&L application(s)
3. A diagram detailing the network topology of the hosted applications
4. Copy of internal or third party audit reports (general IT or cyber security specific) performed for hosted site
5. The reports, findings, and action plans of any vulnerability assessment performed within the last twelve calendar months
6. A detailed description of implemented physical security controls to secure the hosted site

The detailed responses to the Data Collection Questionnaire can be found in Appendix A. Based on the information provided by Landis+Gyr, out of the 118 applicable NISTIR security controls:

- 112 controls are supported
- 1 control is not supported
  - AC-11 (Concurrent Session Control): Future feature enhancement (roadmap) - Earliest it would be available would be 2014, no definite date at this time.
- 1 control is partially supported
  - AC-13 (Remote Session Termination): Command Center will log out the user after a certain period of time but it only does a lockout if the password is entered incorrectly too many times.

- 4 controls are not applicable
  - AC-18 (Use of External Information Control Systems): Per contract, all information is confidential and not shared with outside sources.
  - AU-14 (Security Policy Compliance): Audits to validate security policy compliance outside scope of Command Center Head-End System.
  - IA-1 (Identification and Authentication Policy and Procedures): Definition of Identification and Authentication Procedure outside scope of Command Center Head-End System.
  - SC-30 (Smart Grid Information System Partitioning): Partitioning in different environments outside scope of Command Center Head-End System. Customer is able to define different Command Center environments (production, development, testing).

4.2 Phase II: On-Site Verification

Following the Data Collection and Review phase, the assessment team engaged in an on-site visit with Landis+Gyr to discuss the questionnaire results and confirm the accuracy of Landis+Gyr provided information. The assessment team prioritized focus areas for the on-site visit based on:

- NISTIR 7628 Assessment Guidelines
- KCP&L Smart Grid Deployment Project Design
- Risk Assessment Results from Fall-2011
- Areas applicable to Landis+Gyr's hosting of KCP&L Applications
- Lessons learned from NERC CIP audits and violations
- Observations and outcomes of vulnerability assessments

The selected focus areas consisted of seventy-two (72) of the NISTIR 7628 requirements answered by Landis+Gyr in the Phase I Pre-Verification Security Questionnaire. These requirements are listed in Table 4-1 below. The assessment team utilized various audit approaches (interviews, observations, discussions, documentation review, and evidence reviews) to evaluate the seventy-two (72) NISTIR security controls. The methodology applied to each of the seventy-two (72) requirements during the On-Site Verification Phase can be found in Appendix B.

Table 4-1: On-Site Verification Focus Areas

Requirement Number	Title	Results of Questionnaire	On-Site Objective
SG.AC-1	Access Control Policy & Procedures	Supported	Confirm Requirement is supported through Examination and Interviews
SG.AC-2	Remote Access Policy & Procedures	Supported	Confirm Requirement is supported through Examination, Interviews & Testing

Requirement Number	Title	Results of Questionnaire	On-Site Objective
SG.AC-3	Account Management	Supported	Confirm Requirement is supported through Examination and Interviews
SG.AC-4	Access Enforcement	Supported	Confirm Requirement is supported through Examination
SG.AC-5	Information Flow Enforcement	Supported	Confirm Requirement is supported through Examination and Testing
SG.AC-6	Separation of Duties	Supported	Confirm Requirement is supported through Examination, Interviews & Testing
SG.AC-7	Least Privilege	Supported	Confirm Requirement is supported through Examination and Interviews
SG.AC-8	Unsuccessful LoginAttempts	Supported	Confirm Requirement is supported through Examination and Testing
SG.AC-11	Concurrent Session Control	***Not Supported***	Confirm Requirement is **not** supported through Examination and Testing
SG.AC-13	Remote Session Termination	***Partially Supported***	Confirm Requirement is **partially** supported through Examination & Testing
SG.AC-15	Remote Access	Supported	Confirm Requirement is supported through Examination, Interviews & Testing
SG.AC-18	Use of External Information Control Systems	***Not Applicable***	Confirm Requirement is **not applicable** through Examination and Interviews
SG.AC-21	Passwords	Supported	Confirm Requirement is supported through Examination and Testing
SG.AT-1	Awareness and Training Policy and Procedures	Supported	Confirm Requirement is supported through Examination and Interviews
SG.AU-14	Security Policy Compliance	***Not Applicable***	Confirm Requirement is **not applicable** through Examination and Interviews
SG.CA-4	Information System Connections	Supported	Confirm Requirement is supported through Examination and Interviews
SG.CA-6	Continuous Monitoring	Supported	Confirm Requirement is supported through Examination and Interviews
SG.CM-1	Configuration Management Policy and Procedures	Supported	Confirm Requirement is supported through Examination and Interviews
SG.CM-2	Baseline Configuration	Supported	Confirm Requirement is supported through Examination and Interviews
SG.CM-3	Configuration Change Control	Supported	Confirm Requirement is supported through Examination and Interviews
SG.CM-4	Monitoring Configuration Changes	Supported	Confirm Requirement is supported through Examination and Interviews
SG.CM-5	Access Restrictions for Configuration Change	Supported	Confirm Requirement is supported through Examination, Interviews & Testing
SG.CM-6	Configuration Settings	Supported	Confirm Requirement is supported through Examination and Interviews
SG.CM-7	Configuration for Least Functionality	Supported	Confirm Requirement is supported through Examination, Interviews & Testing
SG.CM-9	Addition, Removal, and Disposal of Equipment	Supported	Confirm Requirement is supported through Examination and Interviews
SG.CM-11	Configuration Management Plan	Supported	Confirm Requirement is supported through Examination and Interviews

Requirement Number	Title	Results of Questionnaire	On-Site Objective
SG.CP-2	Continuity of Operations Plan	Supported	Confirm Requirement is supported through Examination and Interviews
SG.CP-3	Continuity of Operations Roles and Responsibilities	Supported	Confirm Requirement is supported through Examination and Interviews
SG.CP-5	Continuity of Operations Plan Testing	Supported	Confirm Requirement is supported through Examination and Interviews
SG.CP-6	Continuity of Operations Plan Update	Supported	Confirm Requirement is supported through Examination and Interviews
SG.CP-8	Alternate Telecommunication Services	Supported	Confirm Requirement is supported through Examination and Interviews
SG.CP-10	Smart Grid Information System Recovery and Reconstitution	Supported	Confirm Requirement is supported through Examination, Interviews & Testing
SG.CP-11	Fail-Safe Response	Supported	Confirm Requirement is supported through Examination, Interviews & Testing
SG.IA-1	Identification and Authentication Policy and Procedures	*Not Applicable*	Confirm Requirement is **not applicable** through Examination and Interviews
SG.ID-3	Information Handling	Supported	Confirm Requirement is supported through Examination and Interviews
SG.IR-2	Incident Response Roles and Responsibilities	Supported	Confirm Requirement is supported through Examination and Interviews
SG.IR-3	Incident Response Training	Supported	Confirm Requirement is supported through Examination and Interviews
SG.IR-4	Incident Response Testing and Exercises	Supported	Confirm Requirement is supported through Examination and Interviews
SG.IR-5	Incident Handling	Supported	Confirm Requirement is supported through Examination, Interviews & Testing
SG.IR-6	Incident Monitoring	Supported	Confirm Requirement is supported through Examination, Interviews & Testing
SG.IR-7	Incident Reporting	Supported	Confirm Requirement is supported through Examination and Interviews
SG.IR-8	Incident Response Investigation & Analysis	Supported	Confirm Requirement is supported through Examination and Interviews
SG.IR-9	Corrective Action	Supported	Confirm Requirement is supported through Examination and Interviews
SG.IR-10	Smart Grid Information System Backup	Supported	Confirm Requirement is supported through Examination and Interviews
SG.MA-1	Smart Grid Information System Maintenance Policy and Procedures	Supported	Confirm Requirement is supported through Examination and Interviews
SG.MA-3	Smart Grid Information System Maintenance	Supported	Confirm Requirement is supported through Examination and Interviews
SG.MA-5	Maintenance Personnel	Supported	Confirm Requirement is supported through Examination and Interviews
SG.MP-1	Media Protection Policy and Procedures	Supported	Confirm Requirement is supported through Examination and Interviews

Requirement Number	Title	Results of Questionnaire	On-Site Objective
SG.MP-3	Media Marking	Supported	Confirm Requirement is supported through Examination and Interviews
SG.MP-4	Media Storage	Supported	Confirm Requirement is supported through Examination and Interviews
SG.MP-5	Media Transport	Supported	Confirm Requirement is supported through Examination and Interviews
SG.MP-6	Media Sanitization and Disposal	Supported	Confirm Requirement is supported through Examination and Interviews
SG.PE-2	Physical Access Authorizations	Supported	Confirm Requirement is supported through Examination and Interviews
SG.PE-3	Physical Access	Supported	Confirm Requirement is supported through Examination, Interviews & Testing
SG.PE-4	Monitoring Physical Access	Supported	Confirm Requirement is supported through Examination, Interviews & Testing
SG.PE-5	Visitor Control	Supported	Confirm Requirement is supported through Examination, Interviews & Testing
SG.PE-6	Visitor Records	Supported	Confirm Requirement is supported through Examination and Interviews
SG.PE-7	Physical Access Log Retention	Supported	Confirm Requirement is supported through Examination and Interviews
SG.PE-8	Emergency Shutoff Protection	Supported	Confirm Requirement is supported through Examination and Interviews
SG.PE-9	Emergency Power	Supported	Confirm Requirement is supported through Examination and Testing
SG.PS-3	Personnel Screening	Supported	Confirm Requirement is supported through Examination and Interviews
SG.PS-4	Personnel Termination	Supported	Confirm Requirement is supported through Examination and Interviews
SG.PS-5	Personnel Transfer	Supported	Confirm Requirement is supported through Examination and Interviews
SG.PS-6	Access Agreements	Supported	Confirm Requirement is supported through Examination and Interviews
SG.PS-7	Contractor and Third-Party Personnel Security	Supported	Confirm Requirement is supported through Examination and Interviews
SG.PS-8	Personnel Accountability	Supported	Confirm Requirement is supported through Examination and Interviews
SG.PS-9	Personnel Roles	Supported	Confirm Requirement is supported through Examination and Interviews
SG.SC-7	Boundary Protection	Supported	Confirm Requirement is supported through Examination, Interviews & Testing
SG.SC-30	Information System Partitioning	*Not Applicable*	Confirm Requirement is **not applicable** through Examination and Interviews
SG.SI-3	Malicious Code and Spam Protection	Supported	Confirm Requirement is supported through Examination, Interviews & Testing
SG.SI-4	Smart Grid Information System Monitoring Tools and Techniques	Supported	Confirm Requirement is supported through Examination and Interviews

Requirement Number	Title	Results of Questionnaire	On-Site Objective
SG.SI-5	Security Alerts and Advisories	Supported	Confirm Requirement is supported through Examination and Interviews

In addition to the seventy-two (72) NISTIR requirements, the On-Site Verification also evaluated Landis+Gyr against twenty-two (22) areas of Cyber Security and Information Technology included in the NISTIR 7628 guidelines:

1. Hosting Services applicable to KCP&L
2. Secure Software Development Life Cycle (SDLC)
3. Security Configurations Management
   a. Ports and Services
   b. Patch Management
   c. Malicious Software Prevention
   d. Logging, Auditing and Monitoring
4. Access/Account Management
5. Change Management
6. Network Security Architecture
7. Code Management
8. Vulnerability and Security Assessments
9. Electronic Access Controls and Monitoring
10. Physical Access Controls and Monitoring
11. Cyber Security Incident Response Process and Procedures
12. Data Backup & Restoration
13. Disaster Recovery/Continuity of Operations
14. Data Center Operations
15. Information Protection
16. Test Environment
17. Testing Methodology
18. Personnel Security and Training
19. Cyber Security Team
20. Leadership Commitment/Support
21. Internal/Third Party Audits
22. Industry Participation

During the On-Site Verification, Landis+Gyr provided the assessment team with the following documentation for review:

- Landis+Gyr Technology Hosted SOC1 Report FINAL.pdf
- 2012-08-15_Response to L+G Questionnaire111412.xlsx
- Badge Access Work Instruction. SCS-W-014
- User Request Form Work Instruction - SCS-W-002
- Production Firewall Authentication Work Instruction - SCS-W-047
- IT Baseline Security policy (no document number)
- Change Management Procedure SCS-P-010
- Business Continuity Plan Procedure SCS-P-041
- Business Continuity Plan - Master Plan
- Business Continuity Plan - Site Plan - Lenexa
- Landis+Gyr Disaster Recovery – Lenexa Data Center Plan;
- Landis+Gyr Business Continuity Crisis Communication Plan
- Landis+Gyr Pandemic Preparedness Plan; SCS-P-039
- Disaster Recovery Universal Plan
- Corrective Action Preventative Action Procedure CQ-P-002
- Business Ethics Policy HR-F-007
- Employee Access Termination Procedure SCS-P-040 HR Infrastructure Form
- HR-F-005; Personnel Change Notice - HR-F-014
- Associated Training and documentation Procedures

4.3 Phase III: Analysis

In this phase, the assessment team analyzed the information collected in the first two phases of the assessment. The analysis focused on verification of the seventy-two (72) NISTIR security control requirements and adherence to the twenty-two (22) areas of Cyber Security and Information Technology controls identified in Phase II for the Landis+Gyr AHE application and practices.

Utilizing the methodology provided in Appendix B, the assessment team evaluated the AHE application against the criteria described above and provided an appropriate conclusion for each criterion:

- *"Satisfactory"* - Satisfies the standards/guidelines
- *"Other than Satisfactory"* - Falls short of satisfying the standards/guidelines

A summary of the On-Site Verification results are described below (details of the results can be found in Appendices C and D). The On-Site Verification concluded that out of the twenty-two (22) areas of Cyber Security and Information Technology controls, the Landis+Gyr AHE application and practices satisfied the standards/guidelines for all twenty-two (22) areas. In addition, out of the seventy-two (72) NISTIR 7628 security control requirements, the On-Site Verification concluded that:

- 66 controls are fully supported
- 1 control is not supported
  - AC-11 (Concurrent Session Control): Future feature enhancement (roadmap) - Earliest it would be available would be 2014, no definite date at this time.
- 1 control previously determined (in the Pre-Verification Phase) as "partially supported" was assessed to be fully supported
  - AC-13 (Remote Session Termination): Thirty minutes of inactivity will automatically log out the user. Three unsuccessful login attempts causes lockout.
- 2 controls previously determined (in the Pre-Verification Phase) as "not applicable" was assessed to be fully supported
  - AU-14 (Security Policy Compliance): Document SSAE-16 covers security controls validation performed annually IMS (Integrated Management System): audited by external vendor, multi ISO standard compliance system, recertification or checkup annually (recertification every 3 years). Internal audits are performed at least yearly (continuous).
  - SC-30 (Smart Grid Information System Partitioning): Customer is able to define different Command Center environments (production, development, testing).
- 2 controls were confirmed as not applicable
  - AC-18 (Use of External Information Control Systems): Per contract, all information is confidential and not shared with outside sources.
  - IA-1 (Identification and Authentication Policy and Procedures): Definition of Identification and Authentication Procedure outside scope of Command Center Head-End System.

Out of the sixty-nine (69) NISTIR controls that were confirmed to be supported and applicable, the most significant controls dealt with access control, configuration management, continuity of operations, and communication protection. Detailed results for a sampling of these key controls are provided below. Detailed results of all seventy-two (72) NISTIR controls assessed during the On-Site Verification can be

found in Appendix C. Furthermore, detailed results of all twenty-two (22) areas of Cyber Security and Information Technology assessed on-site are provided in Appendix D.

- **AC-7 (Least Privilege)**
  - Individual privileges are documented through a User Request Form.
  - There are some shared administrative accounts.
  - From an application perspective, Command Center utilizes RBAC and Security Admin Roles. RBAC is applied based upon job function.
  - Landis+Gyr goes through a detailed, formal approval process that involves the user's direct manager and the supervisor of the team responsible for granting access to the user.
  - The User Request Forms are renewed on an annual basis.

- **AC-8 (Unsuccessful Login Attempts)**
  - Users are locked out of Command Center after 3 unsuccessful login attempts by default.
  - The quantity of attempts to cause lock-out is configurable.

- **AC-15 (Remote Access)**
  - Remote access to Command Center for Landis+Gyr personnel requires 2-factor authentication (via VPN client and RSA token) to connect to Landis+Gyr corporate network followed by authentication with the production firewall.
  - Firewall authentication is based upon LDAP account.
  - Command Center access for KCP&L personnel is available from any KCPL corporate IP address. Communication traveling between KCP&L and Landis+Gyr traverses private T1 lines.

- **CM-3 (Configuration Change Control)**
  - Landis+Gyr has a change management procedure that is reviewed internally at least annually.
  - Tickets created for change control request include a description of functionality being added/removed/modified, answers for a set of 11 default questions, the customers affected, and the level of risk.
  - Change control process breaks down tasks that need to be handled by different Landis+Gyr groups. Process includes automated procedure that notifies personnel responsible for next phase of change. Process also auto populates who needs to approve change.
  - Change control process includes audit trail to track what Landis+Gyr personnel performed which task at which time.

- **CP-2 (Continuity of Operations Plan)**
  - Landis+Gyr continuity of operations plans are reviewed at least once per year internally.
  - Landis+Gyr performs internal disaster recovery testing for each customer on an annual basis. Disaster recovery testing involving the customer is offered on contractual basis.
  - Disaster recovery plan includes high level timelines.
  - Landis+Gyr has a disaster recovery site in Alpharetta, GA.
  - Landis+Gyr has both external and internal policies for disaster recovery. Internal policies include employee-specific information (such as contact information) that is excluded from the external policies.

- **SC-7 (Boundary Protection)**
  - Firewall rules are configured as implicit-deny.
  - Anti-spoofing is on by default on Landis+Gyr's ASA firewalls.
  - Landis+Gyr has 3 separate Intrusion Protection System (IPS) modules in datacenter: one protecting WAN interface, one protecting Internet connection, one protecting Landis+Gyr user access to Internet. A third party Security Operations Center monitors the IPS modules.
  - Landis+Gyr is moving toward implementing an IPS combined with an Intrusion Detection System at the external boundary of their datacenter.
  - Landis+Gyr logically separates their internal business Internet connection from the Internet connection utilized for customer access.

- **SC-30 (Information System Partitioning)**
  - Landis+Gyr segregates KCP&L data from other customer's data using VLANs and DMZs.
  - KCP&L's Command Center instance is running on a dedicated virtual server.
  - KCP&L's database is logically separated from other customer's databases.
  - VMWare template images are used to build virtual machines for Command Center application server and web server.

5.0 CONCLUSION

Landis+Gyr demonstrated a vigorous cyber security program that utilizes industry best practices. Landis+Gyr complies with 115 of the 116 applicable NISTIR 7628 security control requirements including excellent implementation of security controls to support the major families of the NISTIR 7628 security requirements: access control, configuration management, continuity of operations, and communication protection. Examples of specific NISTIR 7628 requirements which Landis+Gyr has fully supported include: Least Privilege (AC-7), Unsuccessful Login Attempts (AC-8), Remote Access (AC-15), Configuration Change Control (CM-3), Continuity of Operations Plau (CP-2), Boundary Protection (SC-7), and Information System Partitioning (SC-30) (among many others). Landis+Gyr also satisfies the standards/guidelines for all twenty-two (22) areas of Cyber Security and Informatiou Technology controls.

One area with room for improvement was identified during the Pre-Assessment Data Collection and confirmed during the On-Site Verification and Analysis phases. The assessment determined that Landis+Gyr does not comply with one of the applicable NISTIR 7628 requirements (AC-11: Concurrent Session Control). Landis+Gyr has acknowledged that they currently do not meet this requirement and has identified a path to resolution for this requirement in their future feature enhancement roadmap.

Based on the results of Pre-Assessment Data Collection, On-Site Verification and Analysis, the assessment team has concluded that the Landis+Gyr Command Center (AIIE) application and Landis+Gyr practices are ***satisfactory*** in the assessed areas of Cyber Security and Information Technology controls.

APPENDIX A - DATA COLLECTION QUESTIONNAIRE RESPONSE

The Appendix to this document was not published as it includes Confidential and Proprietary Information

APPENDIX B - ON-SITE VERIFICATION METHODOLOGY

The Appendix to this document was not published as it includes Confidential and Proprietary Information

APPENDIX C - NISTIR 7628 ON-SITE VERIFICATION RESULTS

The Appendix to this document was not published as it includes Confidential and Proprietary Information

APPENDIX D - CYBER SECURITY AND INFORMATION TECHNOLOGY CONTROLS ON-SITE VERIFICATION RESULTS

The Appendix to this document was not published as it includes Confidential and Proprietary Information

Burns & McDonnell World Headquarters
9400 Ward Parkway
Kansas City, MO 64114
Phone: 816-333-9400
Fax: 816-333-3690
www.burnsmcd.com

Burns & McDonnell: Making our clients successful for more than 100 years

Appendix P Education & Outreach Collateral

P.1 All KCP&L Customers

P.1.1 Project Literature

P.1.1.1 SmartGrid – An initiative to benefit our customers and the communities we serve (with map)

KCP&L

SmartGrid

the future of energy

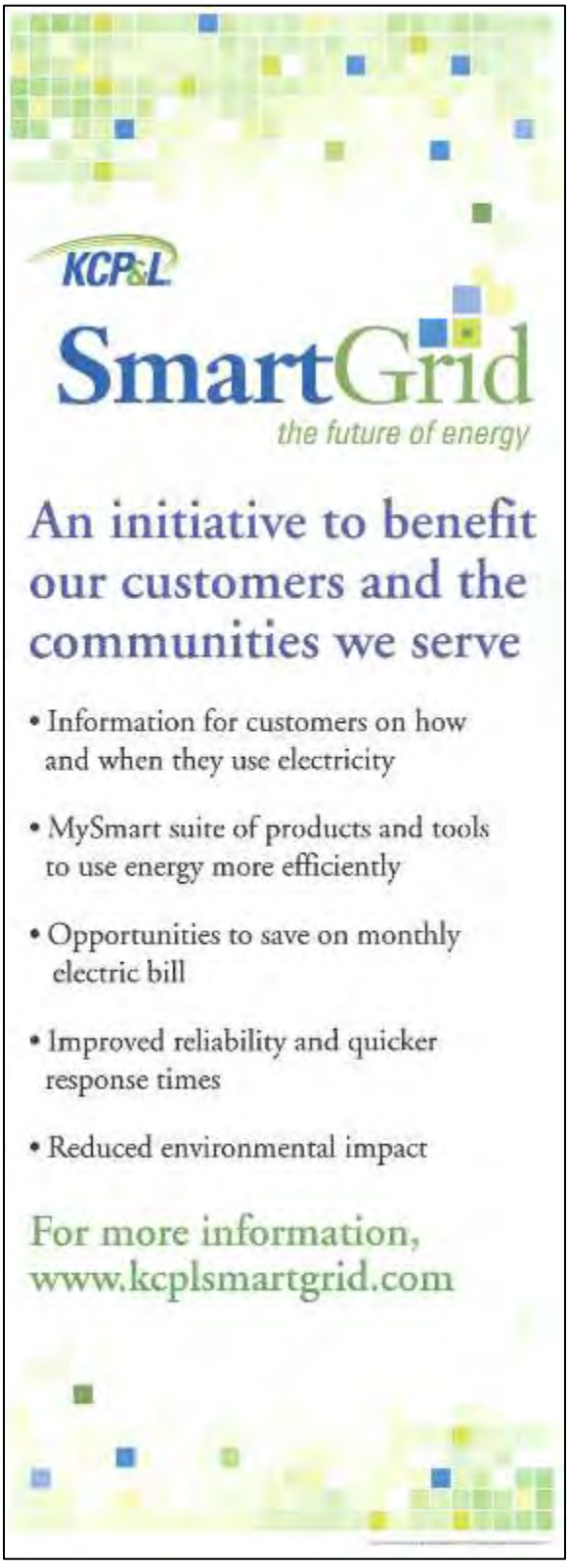
An initiative to benefit our customers and the communities we serve

- Information for customers on how and when they use electricity
- MySmart suite of products and tools to use energy more efficiently
- Opportunities to save on monthly electric bill
- Improved reliability and quicker response times
- Reduced environmental impact

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

KCP&L energizing life

P.1.1.2 SmartGrid – An initiative to benefit our customers and the communities we serve



P.1.1.3 SmartGrid demonstration fact sheet

SmartGrid demonstration fact sheet

KCP&L's SmartGrid demonstration will introduce advanced technologies in Kansas City's urban core.

Within the Green Impact Zone and surrounding areas, KCP&L will deploy a fully integrated SmartGrid demonstration of the latest technologies to show how the advanced utility of the future will work. KCP&L's project will invest approximately $48.1 million and deliver meaningful benefits to the 14,000 customers in this area.

Through this demonstration, KCP&L will gain knowledge about customer needs, energy-efficiency measures, storage capabilities, supply and delivery and the applications customers find most useful. This information will reduce outages and shorten service interruptions, reduce energy delivery costs and enhance information flow for all of KCP&L's service territory. In addition to significant infrastructure and technology upgrades, KCP&L will provide all homes and businesses an advanced two-way interactive meter and offer many homes in the community an energy management system, the Energy Optimizer programmable thermostat, energy audits, weatherization and other energy-efficiency upgrades.

The SmartGrid demonstration improvements will enhance service for the entire Midtown area through improved service reliability, reduced energy delivery costs, more efficient energy consumption, an improved carbon footprint and better information flow.

KCP&L SmartGrid focus

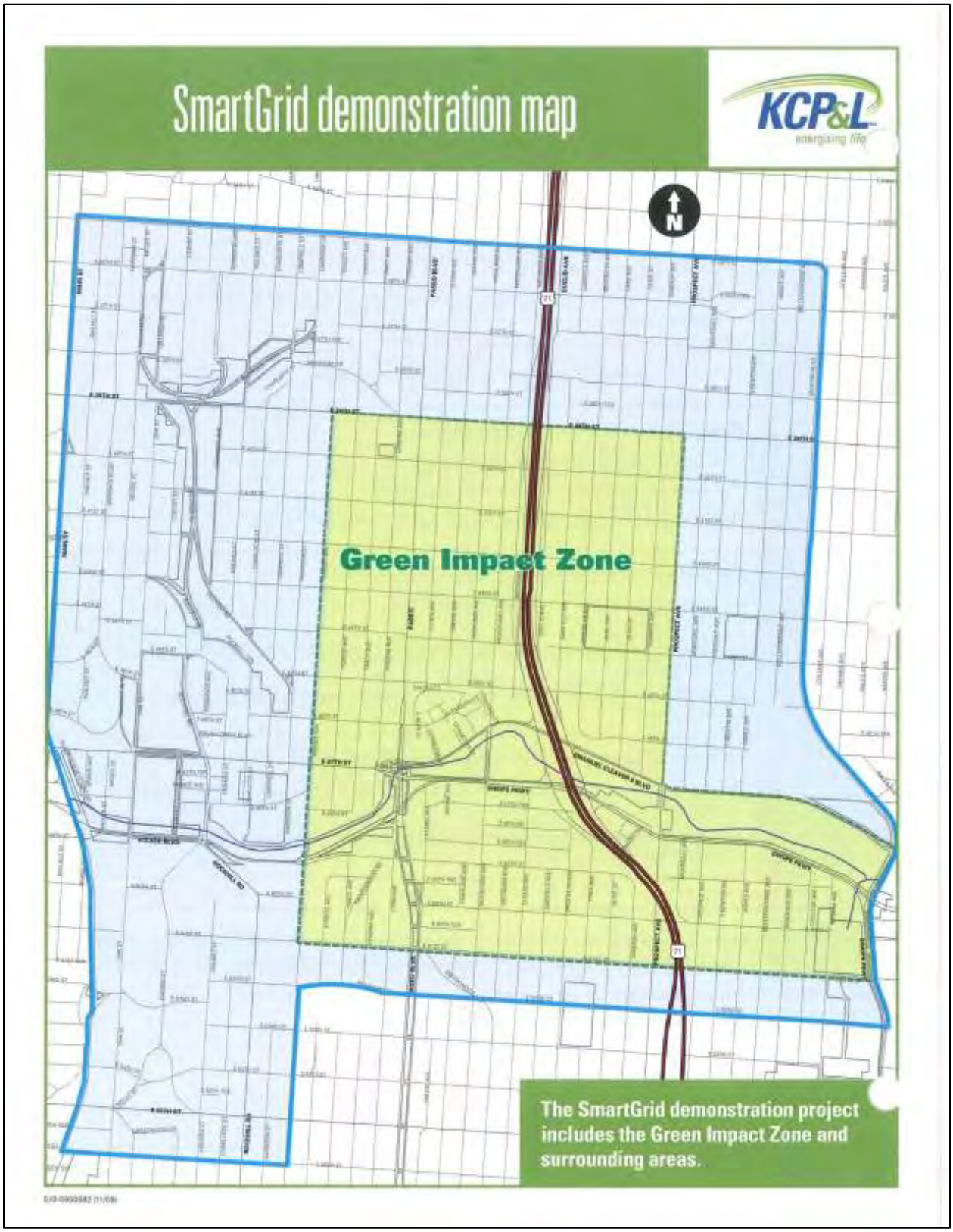
- **Smart Generation** Cost-effective solutions, such as rooftop solar systems and battery storage. These resources will be used to add renewable energy while reducing and shortening system outages.
- **Smart Distribution** KCP&L has already implemented smart applications like automated meter reading, smart switches and smart capacitors. Improved customer delivery and service quality will result from future advanced technologies. This also allows for the ability to communicate with customers on prices and conditions of the system.
- **Smart Consumption** Educating customers and giving them the tools to manage their electricity usage and costs are essential components to the success of the project. KCP&L will focus on updating the area's metering system to accommodate smart appliances, time-of-use pricing options and advanced residential and commercial energy management systems. KCP&L will work with schools to educate children about energy efficiency and collaborate with community organizations to train and recruit workers from the urban core in green technologies.

Program Highlights

- Installation of neighborhood hybrid electric vehicle charging stations.
- Demonstrations of rooftop solar technology at selected commercial buildings, government facilities and residences.
- Installation of smart technologies that monitor and manage energy usage; and Energy Optimizer, a programmable thermostat with advanced features.
- Installation of advanced meters capable of delivering real-time usage information and price signals.
- Installation of more efficient heat-pump water heaters and other high-efficiency appliances in selected homes.
- Collaboration with community organizations to train and recruit workers from the urban core in green technologies.

P.1.1.4 SmartGrid demonstration project timeline

P.1.1.5 SmartGrid demonstration map



P.1.1.6 SmartGrid demonstration Q & A

SmartGrid demonstration Q & A

KCP&L
energizing life

What is a SmartGrid?

A SmartGrid consists of advanced technology that facilitates real-time two-way communication between a utility and its customers. The resulting information allows the utility to improve energy efficiency, reduce costs, improve reliability, generate more transparent and actionable information and reduce its environmental footprint. It also provides customers the opportunity to sell back to the grid power they generate through solar panels. KCP&L believes this project will serve as a blueprint for future SmartGrid implementation and will accelerate a realization that the "utility of the future" safely delivers reliable electricity with greater efficiency, reduced costs and improved environmental performance.

What is the SmartGrid demonstration?

The SmartGrid demonstration is a five-year project continuing through 2014 that will introduce new SmartGrid technologies and gather information to help KCP&L identify and test beneficial energy-efficiency measures, storage capabilities and supply and delivery processes. In the SmartGrid area, KCP&L will implement technologies and energy-efficient products and services to improve reliability, reduce energy delivery costs and enhance information flow.

Where will the demonstration be located?

KCP&L's SmartGrid demonstration will be located in Kansas City's Midtown urban core, reaching from Main St. to Swope Parkway and 37th St. to 52nd St.

Are the previously announced Green Impact Zone and the SmartGrid demonstration the same thing?

No, the Green Impact Zone covers a slightly smaller 150-block area inside the SmartGrid demonstration area, reaching from Troost to Prospect and 39th St. to 51st St. KCP&L's SmartGrid demonstration overlays the Green Impact Zone and extends beyond it to other circuit area Midtown homes and businesses in order to gather a larger sampling of customer needs and preferences. (See map)

Who is paying for the SmartGrid demonstration?

The Department of Energy's (DOE) Office of Electricity and Energy Reliability is providing KCP&L with a grant of just under $24 million to help fund the fully integrated SmartGrid demonstration. This award is part of the Department's federal stimulus funding to modernize the electric grid and enhance the security and reliability of the energy infrastructure. KCP&L is also funding part of the project, along with significant contributions from our technical partners.

What business partners are participating in the SmartGrid demonstration?

Current project partners include Siemens, OATI, Landis+Gyr, Intergraph, GridPoint and Kokam America Inc. (Dow Kokam), who will provide equipment, technical expertise and in-kind financial support. The project is also receiving the support of EPRI, an independent, non-profit company that performs research, development and design in the electricity sector for the benefit of the public.

What SmartGrid technology is KCP&L planning to launch?

Currently, KCP&L will focus SmartGrid efforts in three areas: smart generation, smart distribution and smart consumption. In each area, KCP&L will introduce and implement the latest in advanced utility technology. Some examples are rooftop solar panels, meters that enable two-way communications, customer education and energy management tools.

I live in the SmartGrid demonstration area. How can I participate in some of the initiatives?

As part of KCP&L's initiatives in the SmartGrid project, some homes will be eligible for an energy management system, home energy audit and other energy-efficiency upgrades. KCP&L will work directly with customers and community organizations to introduce customers to new programs.

Knowledge gained from the SmartGrid demonstration project will help KCP&L identify and test beneficial energy-efficiency measures, storage capabilities and supply and delivery processes.

I live outside the SmartGrid area. How will this project help me?

KCP&L customers already benefit from a variety of products and services that incorporate SmartGrid technologies, including energy audit services, energy-efficiency improvement rebates and programmable thermostats that integrate with the company's demand response goals to help KCP&L manage peak demand and protect the environment.

The SmartGrid demonstration will enable KCP&L to test emerging smart technologies and demonstrate to all customers its vision of how the advanced utility of the future will work. KCP&L will gain knowledge about customer needs, energy-efficiency measures, storage capabilities, supply and delivery, and the applications customers find most useful. This information will improve reliability, reduce energy delivery costs and enhance information flow for all of KCP&L's service territory. Also, the research collected will provide a regional advantage when determining where federal and private dollars should be invested.

Finally, KCP&L will work with schools to educate children about energy efficiency and collaborate with community organizations to train and recruit workers from the urban core in green technologies.

P.1.1.7 Current partners & vendors

Current SmartGrid partners & vendors

Siemens Energy, Inc.

Siemens will focus on the automation of the distribution network, Smart Substation controllers, and integration with Distribution SCADA, full Distribution Management System (DMS) capabilities as well as integration with the existing Geographic Information System (GIS), Advanced Metering Infrastructures (AMI), Meter Data Management Systems (MDMS), Distributed Energy Resource Management (DERM) Systems, and Demand Response Management (DRM) Systems. Siemens' extensive expertise, experience and leadership in the energy industry directly correspond to SmartGrid advancements. Overall, Siemens has embraced the SmartGrid paradigm shift and is dedicating significant resources to create lasting products and solutions for its customers.

Communication Contact:
Holly Bounds
(678) 427-6700
holly.bounds@siemens.com

Open Access Technology International (OATI)

OATI, which has been serving the energy industry since 1995, has had steady growth since its inception and currently has more than 400 staff members. Today, the privately owned OATI, headquartered in Minneapolis, Minn., with branch offices in San Mateo, Calif., and Houston, Texas, provides innovative solutions and services to the electric and gas industry to meet challenges in energy scheduling, trading, and risk management; transmission reservations, scheduling, and congestion management; and compliance monitoring. In addition, OATI and offers a variety of products under its web SmartEnergy suites of applications, which are modular solutions to address the requirements for the emerging SmartGrid. OATI web SmartEnergy products include software and services for Demand Response and Distributed Energy Distribution Resources Management, Renewable Management and Asset Management.

Communication Contact:
el Brooks
) 327-6209
nervel.brooks@oati.com

Electric Power Research Institute (EPRI)

EPRI will provide technical expertise and advice on defined portions of the project. In addition, EPRI is an active member on several national and international five-year EPRI SmartGrid Demonstration Initiatives, which support SmartGrid projects that integrate distributed energy resources (www.smartgrid.epri.com). One of the main objectives of this initiative is to identify approaches for interoperability and integration that can be used on a systemwide scale to help standardize Distributed Energy Resources (DER) as part of overall system operations and control. EPRI will support this project in several areas including cost-benefit analysis efforts, use case documentation per the IntelliGrid methodology, data analysis and benefits estimation, CO_2 impact assessment and technology transfer.

Communication Contact:
Matt Wakefield
(865) 218-8087
mwakefield@epri.com

Intergraph Corporation

Intergraph provides a suite of electric industry solutions to address work design, network asset management, outage management and integrated mobile work force management. The foundational component, a Geographic Information System (GIS), is a comprehensive, enterprise-capable, network asset infrastructure management platform that houses a connected data model of the entire energy network or communications infrastructure. This project will leverage an existing Intergraph (GIS) model in the development of the proposed advanced grid monitoring and control environment.

Communication Contact:
Angela Frechette
(404) 751-2553
angela.frechette@intergraph.com

Landis+Gyr (L&G)

Landis+Gyr has over 100 years of history in the energy space, including 60 years of direct load-management expertise and 25 years of smart metering innovation. It is also a leader in integrated energy management solutions, with a commitment to improving energy efficiency and environmental conservation. L&G operates in more than 30 countries on five continents, with over 15 million endpoints actively managed in long-term contracts.

Communication Contacts:
Vicki Trees
(218) 562-3850
Vicki.Trees@landisgyr.com

Dan Jacobson
(218) 562-5195
Dan.Jacobson@landisgyr.com

GridPoint

GridPoint will provide a residential Energy Resource Management (ERM) and Home Area Network (HAN) platform that will provide energy consumers and utilities with an intelligent network of distributed energy resources that can control load, store energy and produce power. The platform aggregates distributed energy resources and provides consumer and utility control through a single Web-based interface, giving the equivalent performance of central station generation.

Communication Contact:
Suzanne Lauer
(703) 862-3137
slauer@www.gridpoint.com

Kokam America Inc. (Dow Kokam)

Dow Kokam America will leverage existing lithium polymer battery technology development and manufacturing expertise to develop and deploy a grid-scale energy storage system that supplies peak shaving, demand-management and enhanced power quality Micro-Grid restoration capabilities to the KCP&L grid. The installation will be part of a larger distributed resource environment, Distribution Management System, controlled remotely and programmed to function automatically in conjunction with other SmartGrid components.

Communication Contact:
Don Nissanka
(816) 525-1153
don.nissanka@kokamerica.com

P.1.1.8 SmartGrid Overview

KCP&L

SmartGrid

the future of energy

overview

What is the KCP&L SmartGrid project?

It is a five-year initiative to develop a new electrical system that will improve the flow of communication and information between KCP&L and our customers. It will introduce a variety of new products and technologies and study how the different system parts best work together to benefit our customers and KCP&L. The project will also test new energy-efficiency measures, storage capabilities and supply and distribution options; improve reliability; lower energy delivery costs; and reduce environmental impact.

In particular, the SmartGrid project will provide customers with products and tools they can use to monitor and manage their electricity usage, which can potentially save them money on their monthly bills. SmartGrid also will help the company identify which combination of applications customers find most useful.

Like anything new, customers must learn how to use the system to enjoy its benefits. Multiple customer communications and events are planned, along with community support and targeted advertising.

Where will the project be located?

KCP&L's SmartGrid project will be located in a number of Kansas City neighborhoods, stretching roughly from Main Street (W) to Benton Blvd/Swope Parkway (E) and 35th Street (N) to 52nd Street (S).

What is the project's goal?

- Install and evaluate a complete smart grid system in a number of Kansas City neighborhoods.
- Educate customers on how to use the system's updated capabilities to better manage their energy use and budget.
- Identify the products and tools customers find most useful.
- Serve as a blueprint for introducing the smart grid technology across KCP&L's service area.

What benefits will the new smart grid provide?

KCP&L's SmartGrid project will provide customers with greater:

- *Choice:* Customers will be offered products and services not previously available to them, and they will be able to decide which they want to use.
- *Control:* The new SmartGrid products and tools will give customers the ability to manage their electricity use, which can help them save money on their monthly electric bills. As customers reduce their energy usage and use the SmartGrid's renewable energy options, the region's carbon footprint will also be reduced.
- *Convenience:* The new technology will enable KCP&L to provide faster customer service. For example, the updated system will instantly re-route service to prevent outages and restore service more quickly when problems occur. It will also enable our SmartGrid Support Team to view 15-minute interval data when customers have questions or need help.

Who is paying for KCP&L's SmartGrid project?

In 2009, KCP&L applied for and received a $24 million grant from the Department of Energy (DOE) Office of Electricity and Energy Reliability to install a fully integrated smart grid system in the project area. The DOE grant will be matched by KCP&L and our project partners for a total investment of approximately $50 million in the SmartGrid area.

SmartGrid Project partners

Who are KCP&L's SmartGrid Project partners?

KCP&L's technical partners on the SmartGrid project currently include: **Siemens**, **OATI**, **Landis+Gyr**, **Intergraph**, **Tendril** and **Dow Kokam**. These leading industry innovators will provide equipment, technical expertise and in-kind financial support.

SmartGrid project products

What is a smart meter?

Smart meters are advanced electric meters that work with a variety of smart grid products to help customers better manage their electricity use. They resemble the meters KCP&L has installed over the last decade, but they enable two-way communication that supports increased customer service, operational efficiencies and near real-time information flow.

What other SmartGrid products are included in the project?

As part of its SmartGrid project, KCP&L is focusing in three areas: smart generation, smart distribution and smart consumption. In each area, KCP&L is introducing and

KCP&L energizing life

MySmart Thermostat

MySmart Display

MySmart Portal

implementing the latest advanced technology. The first products and services to be introduced are:

- *MySmart Thermostat:* For homes with central air conditioning, MySmart Thermostat can be programmed to automatically set temperatures based on the season, time of day and customers' schedules, helping them save money on heating and cooling bills.
- *MySmart Display:* A hand-held electronic device for inside the customer's home that takes information directly from the meter and presents it in easy-to-understand screens. MySmart Display helps customers identify opportunities to reduce consumption and save money. Does not require an Internet connection.
- *MySmart Portal:* A personalized website that helps customers understand how they use electricity and enables them to make decisions that conserve energy, help the environment and save money.

How is privacy of my smart meter data managed?

Protecting our customers' information is a top priority. KCP&L applies the same rigorous privacy protection to all data collected by the company including usage data collected by the smart meter system. We treat your personal information and data as confidential in compliance with all regulatory requirements, including those of the Federal Energy Regulatory Commission, the Missouri Public Service Commission and the Kansas Corporation Commission.

Will smart grid business and residential customers receive the same equipment and benefits?

Most small businesses will qualify for the same products and services as our residential customers. Larger commercial customers will be contacted by their energy consultant to discuss the programs they qualify for through SmartGrid.

Who do I contact with questions or if I have an outage or service problems?

To report an outage or discuss your servs. call: **1-888-544-4852**

For smart grid service questions, call: **1-800-535-7687** or **(816) 737-7129** or e-mail *smartgridinfo@kcpl.com*. You can also learn more about the project at *www.kcplsmartgrid.com*.

What is the timeline for the SmartGrid project?

2010: Planning and outreach; meter installation and introduction of the online portal, in-home energy monitors and smart programmable thermostats; upgrades to the Midtown substation and distribution system

2011: Baseline customer usage study; introduction of additional new energy-saving product and service options; installation of commercial solar panels and electric vehicle charging stations

2012: Complete all system improvements and enhancements

2013-14: Complete system research; report findings to the Department of Energy

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221.

P.1.1.9 SmartGrid Demonstration Q & A

SmartGrid Demonstration

Q&A

Knowledge gained from the SmartGrid demonstration project will help KCP&L identify and test beneficial energy-efficiency measures, storage capabilities and supply and delivery processes.

green impact zone of MISSOURI

Where is the demonstration?

KCP&L's SmartGrid neighborhood demonstration location is within Kansas City's urban core and is bounded by Main St. on the west; Swope Parkway on the east; 37th St. on the north and 52nd St. on the south. The Green Impact Zone will cover a 150-block area within Kansas City's urban core from Troost to Prospect and 39th St. to 51st St. Within this area, KCP&L will implement SmartGrid technologies and energy-efficient products and services to improve reliability, reduce energy delivery costs and enhance information flow.

What organizations are participating in the Zone?

A large number of organizations are contributing resources and funding to make the Green Impact Zone a success, including the State of Missouri, Mid-America Regional Council, KCP&L, the city of Kansas City, Brush Creek Community Partners, University of Missouri-Kansas City, Metropolitan Energy Center and several neighborhood associations.

Who is paying for the SmartGrid demonstration?

KCP&L has filed a grant application with the Department of Energy for federal stimulus funding. KCP&L is also funding part of the project, along with significant contributions from technical partners.

What is a SmartGrid?

There are many different definitions of a SmartGrid. Basically, it consists of advanced technology that facilitates real-time two-way communication between the utility and the end-user. The resulting information allows the utility to improve energy efficiency, reduce costs, improve reliability, generate more transparent and actionable information and reduce its environmental footprint. KCP&L believes this project will serve as a blueprint for future SmartGrid implementation and will accelerate a realization that the "utility of the future" safely delivers reliable electricity with greater efficiency, reduced costs and improved environmental performance.

What SmartGrid technology is KCP&L planning to launch in the Green Impact Zone?

Currently, KCP&L will focus SmartGrid efforts in three areas: smart generation, smart distribution and smart consumption. In each of these areas, KCP&L will introduce and implement the latest in advanced utility technology. Some examples are rooftop solar panels, meters that enable two-way communications, customer education and energy management tools.

I live in the Green Impact Zone. How can I participate in some of the initiatives?

As part of KCP&L's initiatives in the Green Impact Zone, some homes will be eligible for an energy management system, home energy audit and other energy-efficiency upgrades. KCP&L will work directly with customers and community organizations to introduce customers to new programs.

I live outside the Green Impact Zone. How will this help me?

KCP&L customers already benefit from a variety of products and services that incorporate SmartGrid technologies, including energy audit services, energy-efficiency improvement rebates and programmable thermostats that integrate with the company's demand response goals to help KCP&L manage peak demand and protect the environment.

The SmartGrid demonstration will enable KCP&L to test emerging smart technologies and demonstrate to all customers its vision of how the advanced utility of the future will work. KCP&L will gain knowledge about customer needs, energy-efficiency measures, storage capabilities, supply and delivery, and the applications customers find most useful. This information will improve reliability, reduce energy delivery costs and enhance information flow for all of KCP&L's service territory. Also, the research collected will provide a regional advantage when determining where federal and private dollars should be invested.

Finally, KCP&L will work with schools to educate children about energy efficiency and collaborate with community organizations to train and recruit workers from the urban core in green technologies.

KCP&L

P.1.1.10 SmartGrid Demonstration Fact Sheet

SmartGrid Demonstration

Fact Sheet

KCP&L's SmartGrid demonstration will focus on introducing advanced technologies in Kansas City's urban core.

green impact zone of MISSOURI

Within the Green Impact Zone and surrounding areas, KCP&L plans to deploy a fully integrated SmartGrid demonstration of the latest technologies to show how the advanced utility of the future will work. KCP&L's project will invest approximately $48.1 million and deliver meaningful benefits to the 14,000 customers in this area.

Through this demonstration, KCP&L will gain knowledge about customer needs, energy efficiency measures, storage capabilities, supply and delivery, and the applications customers find most useful. This information will improve reliability, reduce energy delivery costs and enhance information flow for all of KCP&L's service territory. In addition to significant infrastructure and technology upgrades, KCP&L will provide all homes and businesses an advanced two-way interactive meter, and offer many homes in the community an energy management system, the Energy Optimizer programmable thermostat, energy audits, weatherization and other energy-efficiency upgrades.

The SmartGrid demonstration improvements will enhance service for the entire Midtown area through improved reliability, reduced energy delivery costs, more efficient-energy consumption, an improved carbon footprint and enhanced information flow.

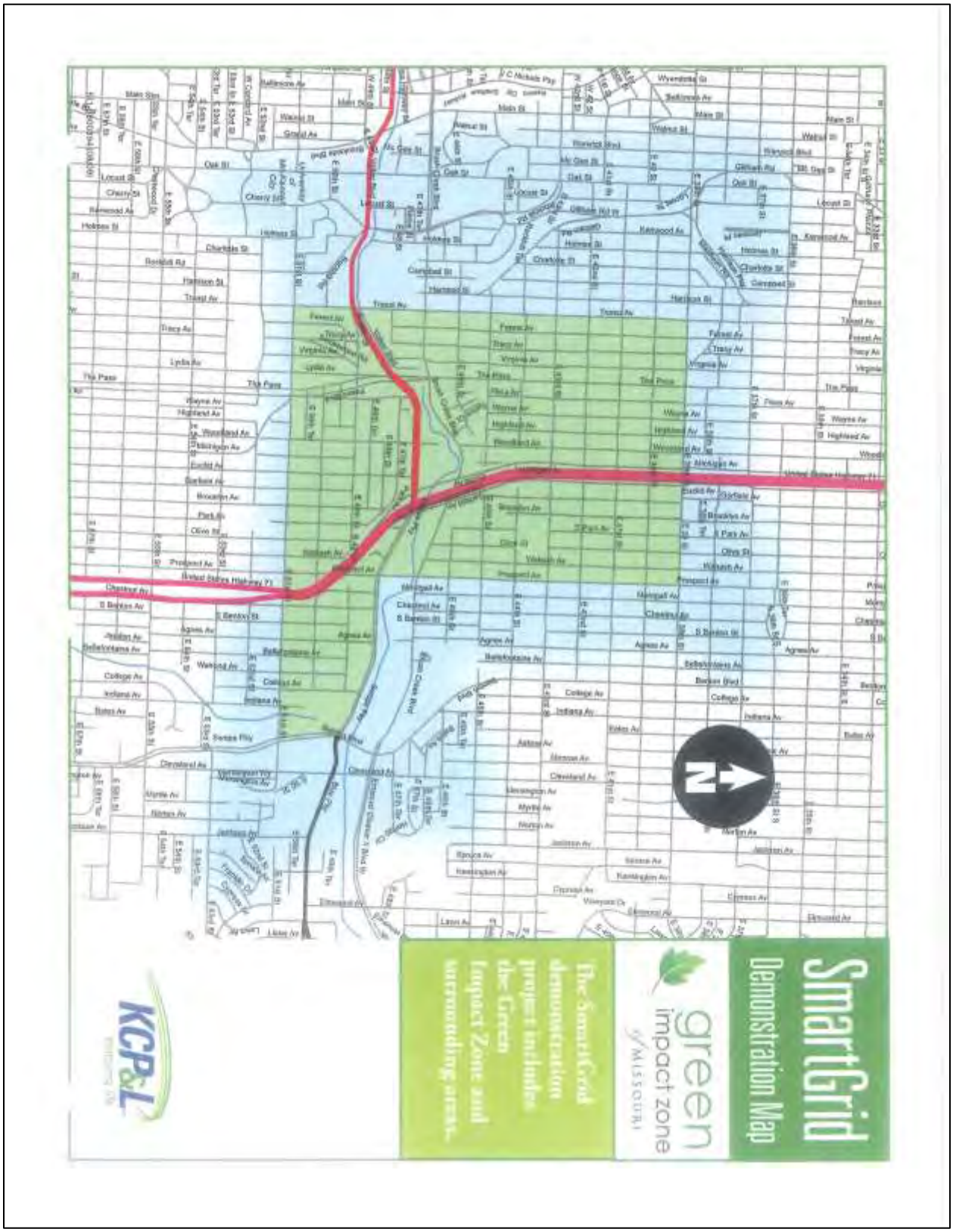
KCP&L's SmartGrid efforts will focus on three areas:

- **Smart Generation.** Within the Green Impact Zone and surrounding areas, KCP&L will work with residents, businesses and schools to pilot cost-effective solutions, such as rooftop solar systems and battery storage. These resources will be used to add renewable energy while supporting the grid for reliability.
- **Smart Distribution.** While KCP&L has already implemented smart applications—such as automated meter reading, smart switches and smart capacitors—improved customer delivery, reliability and service quality will result from future advanced technologies including a smart substation and SmartGrid monitoring and automation. This also allows for the ability to communicate with customers on prices and conditions of the system.
- **Smart Consumption.** Educating customers and giving them the tools to manage their electricity usage and cost are essential components to the success of the project. KCP&L will focus on updating the area's metering system to accommodate smart appliances, time-of-use pricing options, and advanced residential and commercial energy management systems. KCP&L will work with schools to educate children about energy efficiency and collaborate with community organizations to train and recruit workers from the urban core in green technologies.

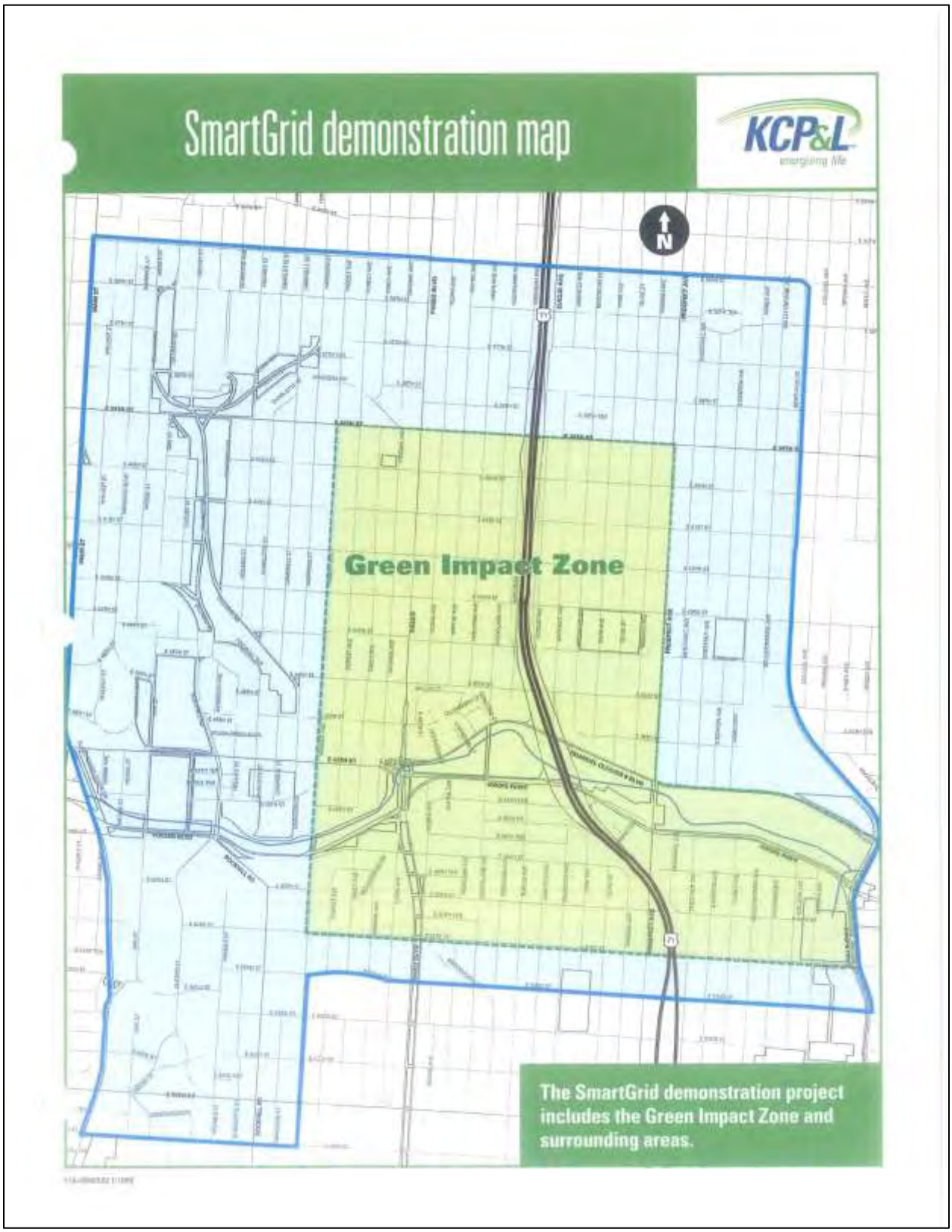
KCP&L

P.1.1.11 SmartGrid Demonstration (component map)

P.1.1.12 SmartGrid Demonstration Map (w/Green Impact Zone)



P.1.1.13 SmartGrid Demonstration Map (w/Green Blue Boundaries)



P.1.1.14 SmartGrid Demonstration Pilot Program

SmartGrid Demonstration Pilot Program

KCP&L's SmartGrid demonstration will showcase the utility of the future, while collaborating to improve the urban core.

green impact zone of MISSOURI

- Improvements to the distribution grid and the Midtown substation, located on 48th Street, will enhance reliability, efficiency and two-way communication.
- Installation of hybrid electric vehicle charging stations located throughout the neighborhoods.
- Addition of utility-scale battery storage for the Midtown substation.
- Demonstrations of rooftop solar technology at selected commercial buildings, government facilities and residences.
- Installation of smart technologies at select homes and businesses, including an energy management system, or information hub device, to monitor and manage energy usage; and Energy Optimizer, a programmable thermostat with advanced features.
- Installation of advanced meters capable of delivering real-time usage information and price signals.
- Installation of more efficient heat-pump water heaters and other high-efficiency appliances at selected homes.
- Demonstration of time-of-use pricing structures that shows the benefits these structures provide to consumers and the environment.
- Opportunities for each customer to take advantage of KCP&L's full portfolio of energy-efficiency products and services, including rebates for high-efficiency air conditioners, incentives for CFLs, weatherization programs, home energy audits and commercial rebates for improvements in lighting and efficiency.
- Pursuit of opportunities for solar applications, such as energy-efficient LED security lighting for residents and businesses and solar-powered bus stops.
- Establishment of a Green Impact Zone office that allows employees to be integrally involved in the Green Impact Zone revitalization, as well as financial contributions for Green Impact Zone ombudsmen and volunteers.
- Collaboration with schools to educate children about energy efficiency and community organizations to train and recruit workers from the urban core in green technologies.

KCP&L energizing life

P.1.1.15 Demonstration Project Overview

KCP&L SmartGrid
the future of energy

Demonstration Project Overview

For more information about KCP&L's SmartGrid demonstration project, visit www.KCPLSmartGrid.com or contact us at SmartGridInfo@KCPL.com or (800) 535-7687

Program Highlights

- **MySmart Meter Deployment.** Installation of advanced electric meters that deliver real-time information about electricity use and pricing to customers.
- **Free SmartGrid Products and Tools.** A variety of resources designed to help you manage energy use and monthly bills.
- **SmartSubstation Upgrade.** Located near the intersection of Troost Avenue and Brush Creek, offering improved real-time operating data on critical substation equipment, reduced relay operation and maintenance costs and improved reliability by enabling distribution automation.
- **Demonstration Facility.** Adjacent to the Substation near the intersection of Troost Avenue and Brush Creek, featuring energy-generating solar panels, a new battery technology for storing and distributing energy, an electric vehicle charging station and SmartGrid control technologies and sensors.
- **Project Living Proof.** A demonstration home at 917 Emanuel Cleaver II Blvd., where visitors can see MySmart Products and best energy conservation practices in action.

Helping Kansas City Get Smarter about Energy

With the help of a grant from the United States Department of Energy, KCP&L is investing more than $48 million in a SmartGrid demonstration project involving approximately 14,000 KCP&L customers in Kansas City's urban core. The project is designed to help improve service reliability, reduce energy delivery costs, encourage more efficient energy consumption, and improve the flow of customer information.

Through the SmartGrid demonstration project, KCP&L will gain knowledge about customer needs and usage patterns. In addition, the company will be able to gather information about SmartGrid storage capabilities, supply and delivery.

***GetSmarter** with Free SmartGrid Products from KCP&L*

Residents or small business owners in the SmartGrid demonstration area (see reverse for map of boundaries) are the first in KCP&L's service territory to have access to a suite of free products designed to help you manage your electricity usage and monthly bill. They include:

- *MySmart Portal.* Free web-based tool that allows you to monitor and manage your electricity usage.
- *Time of Use Rates.* Voluntary time-of-use rate structure that offers higher rates during peak electricity usage times and discounted rates during off-peak times.
- *MySmart Display.* Free portable electronic device that takes information directly from your electric meter and displays it for you in real-time.
- *MySmart Thermostat.* Free programmable thermostat that can be automatically set based on the season, time-of-day and your schedule.
- *MySmart Home.* Free virtual hub that connects your home's appliances and electronics while remotely monitoring and controlling your MySmart Thermostat and other appliances.

KCP&L

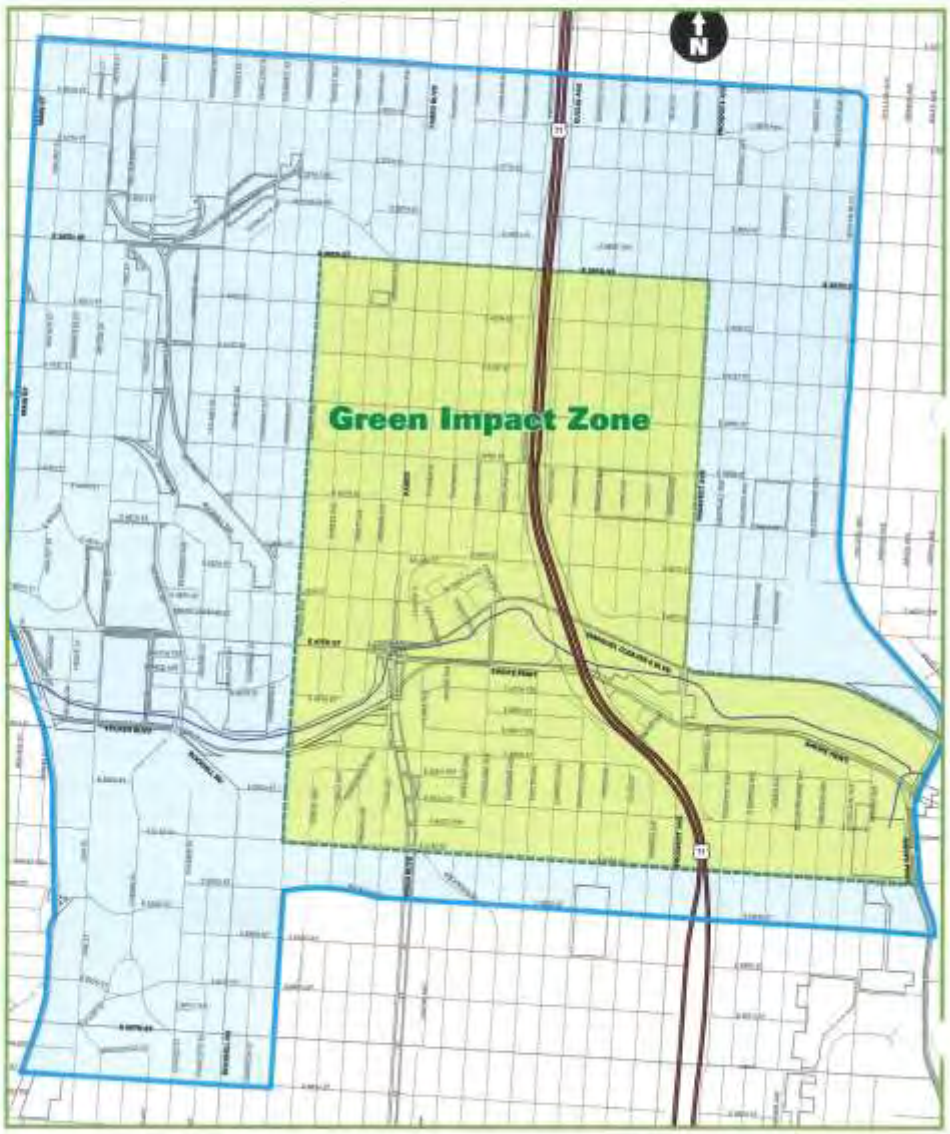
SmartGrid

the future of energy

Demonstration Area

KCP&L's SmartGrid project includes the Green Impact Zone and surrounding neighborhoods, shown here in blue.

The Green Impact Zone is a cooperative effort to focus federal stimulus funds on projects in a targeted area of Kansas City, Mo.



This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

KCP&L energizing life

P.1.1.16 SmartGrid Project Message Map

5. iGrid Project Message Map

"CONTEXT" MESSAGE	"BENEFITS" MESSAGE	"PRODUCTS" MESSAGE	"COMMUNITY" MESSAGE	"FINANCIAL" MESSAGE
KCP&L is building a next-generation smart grid in Midtown Kansas City that will showcase the advanced utility of the future.	**Project will reduce costs, improve reliability, increase energy efficiency and reduce environmental impact.**	**New products and tools will give customers the ability to manage their electricity use, which can help save money on their monthly bills.**	**KCP&L is partnering with the community in the SmartGrid area to ensure the project's success.**	**SmartGrid project will be funded through DOE grant matched by KCP&L and project partners**
Supporting Facts	Supporting Facts	Supporting Facts	Supporting Facts	Supporting Facts
Installing a complete state-of-the-art smart grid system in project area	Customers will have increased access to information that can help them save money on their monthly electric bills	Smart meter: the key that unlocks the advantages of the new smart grid technology	KCP&L has a long history of partnering to improve life in the communities we serve	$24 million DOE grant plus $24 investment from KCP&L and project partners
Project spans roughly from Main Street to Benton Boulevard/ Swope Parkway, and 35th Street to 52nd Street	Customers can choose the tools and services that are right for them	MySmart Portal: a customized website that enables customers to monitor and manage their energy use	We are collaborating with local organizations like the Green Impact Zone, plus various community organizations, home-owners associations and neighborhood groups located in the project area.	All products will be provided to SmartGrid project customers at no charge
Project will test new products and technologies, identify customer preferences and how various system parts work best together	Smart grid infrastructure will improve system reliability and allow us to respond more quickly when an outage occurs	MySmart Display: a small in-home device that allows customers to monitor and manage their electricity use without Internet access	Also partnering with the Metropolitan Energy Center on Project Living Proof). This demonstration house (917 Cleaver Blvd.) will allow customers to experience SmartGrid.	KCP&L costs will be recoverable only through a future rate case
KCP&L has a history of innovation: EEI Edison Award, Sierra Club agreement, CEP, AMR	Reducing customers' electricity use will lower their carbon footprint	MySmart Thermostat: Allows customer to preset temperatures based on season and personal preference, resulting in savings on monthly bills	Numerous community events will help area residents learn about the new technology and its benefits.	SmartGrid reflects KCP&L's continuing commitment to provide low cost, reliable energy for customers

SmartGrid Project Message Map

"CONTEXT" MESSAGE	"BENEFITS" MESSAGE	"PRODUCTS" MESSAGE	"COMMUNITY" MESSAGE	"FINANCIAL" MESSAGE
Supporting Facts	Supporting Facts	Supporting Facts	Supporting Facts	Supporting Facts
	This SmartGrid project will serve as the blueprint for future smart grid implementation.	Commercial Energy Management System: a tool for small business customers that allows them to monitor and manage their energy use		
		Beginning in 2011, KCP&L will be adding to the MySmart suite of products and services, including a home area network, electric vehicle charging stations, Time of Use Rates, and Pre-pay options		

P.1.1.17 SmartGrid Project Talking Points

SmartGrid Talking Points 12/14/10

Project Overview

What is the KCP&L SmartGrid project? KCP&L's SmartGrid project is a five-year initiative that will test a variety of new products and technologies and study how the different system parts best work together to benefit our customers and KCP&L. Specifically, KCP&L will introduce new technologies and test a variety of energy-efficiency measures, storage capabilities and supply and distribution options. The SmartGrid also will improve reliability, lower energy delivery costs, reduce the environmental impact and enhance information flow between KCP&L and our customers.

In particular, the SmartGrid project will provide customers with products and tools they can use to monitor and manage their electricity usage, which can potentially save them money on their monthly bills. SmartGrid also will help the company identify which combination of applications customers find most useful.

KCP&L's SmartGrid project will cover a number of Kansas City' neighborhoods, including the 150-square block Green Impact Zone (an initiative led by U.S. Rep. Emanuel Cleaver II to focus federal stimulus dollars on a targeted geographic area.)

In 2009, KCP&L applied for and received a $24 million grant from the Department of Energy (DOE) Office of Electricity and Energy Reliability to build a fully integrated smart grid system in the project area. Using federal stimulus funding, this award is part of the DOE's effort to modernize the electric grid and enhance security and reliability of the nation's energy infrastructure. The DOE grant will be matched by KCP&L and our project partners for a total investment of approximately $50 million in the SmartGrid area.

Project Benefits

KCP&L's SmartGrid project will provide customers with greater:

Choice: Customers will be offered products and services not previously available to them, and they will be able decide which they want to use and take advantage of.

Control: The new SmartGrid products and tools will give customers the ability to manage their electricity use, which can help them save money on their monthly electric bills. As customers reduce their energy usage and use the SmartGrid's renewable energy options, the region's carbon footprint will also be reduced.

Convenience: The new technology also will enable KCP&L to provide faster customer service:

- The updated system will instantly re-route service to prevent outages and restore service more quickly when problems occur.
- Our SmartGrid support team will be able to view 15-minute interval data when customers have questions or need help.

Products & Services

- **MySmart Portal:** A personalized website that helps customers understand how they use electricity and enables them to make decisions that conserve energy, help the environment and save money.
- **MySmart Thermostat:** For homes with central air conditioning, this thermostat can be programmed to automatically set temperatures based on the season, time of day and customers' schedule, helping them save money on heating and cooling bills.
- **MySmart Display:** A hand-held in-home electronic device that takes information directly from customer's meter and presents it in easy-to-understand screens that increase customer's awareness of their electricity use and identifies opportunities to reduce consumption and save money. Does not require an Internet connection.

SmartGrid Talking Points 12/14/10

- Beginning in 2011 KCP&L will be adding to the MySmart suite of products and services. Some of the potential products and serves are a home area network, plug-in electric vehicle charging stations, time of use rates and pre-pay options.

P.1.1.18 FAQs from Website

SmartGrid - Frequently Asked Questions Page 2 of 3

My Account Username Forgot your login? Register

Learn More » Frequently asked questions

Frequently Asked Questions

- How do MySmart Portal, MySmart Display and MySmart Thermostat communicate with me and KCP&L?
- How do I sign up to get the MySmart Portal, MySmart Display or MySmart Thermostat in my home?
- Do MySmart Portal, MySmart Display or MySmart Thermostat require an Internet connection?
- Do I have to replace my existing thermostat to get MySmart Thermostat?
- I have to have MySmart Portal, MySmart Display and MySmart Thermostat in my home?
- Can I buy these products in a store like Best Buy?
- How much do MySmart Portal, MySmart Display and MySmart Thermostat cost?
- Will KCP&L control MySmart Thermostat?
- Will I be notified in advance of a MySmart Thermostat cycling event?
- Can I cancel my participation in MySmart Portal, MySmart Display or MySmart Thermostat?
- How much can I expect to save on my electric bill with MySmart Portal, MySmart Display and MySmart Thermostat
- What is the difference between MySmart Portal and MySmart Display?
- How do I install MySmart Display?
- Where should I put MySmart Display?
- How do I use MySmart Portal, MySmart Display and MySmart Thermostat?
- How does MySmart Portal compare me to my community?

How do MySmart Portal, MySmart Display and MySmart Thermostat communicate with me and KCP&L?
They communicate wirelessly with your meter using a low-power wireless radio technology called ZigBee. ZigBee is similar to Wi-Fi but has a wider range and uses less power. In the future, they may also communicate via the Internet using a Gateway device.

How do I sign up to get the MySmart Portal, MySmart Display or MySmart Thermostat in my home?
For MySmart Display and MySmart Thermostat you can either visit our website at www.kcplsmartgrid.com and sign up with an online enrollment form or by calling 1(800) 535-7687. MySmart Thermostat requires an appointment for the technician to come in and install it. For MySmart Portal, you can sign up online via AccountLink at www.kcplsmartgrid.com. The registration is located in the top right-hand corner of the home page.

Do MySmart Portal, MySmart Display or MySmart Thermostat require an Internet connection?
Only MySmart Portal requires an Internet connection. MySmart Thermostat and MySmart Display do not. If you do not have a computer or Internet, we recommend logging in at a library or a friend's house.

Do I have to replace my existing thermostat to get MySmart Thermostat?
Yes. This thermostat works like all other thermostat and controls both your central air-conditioning and your furnace.

Do I have to have MySmart Portal, MySmart Display and MySmart Thermostat in my home?
No. These products are all voluntary. If you do not wish to have them, just simply let us know that.

Can I buy these products in a store like Best Buy?
No. Because the products work directly with your meter and are brand new technology, you need to receive them from KCP&L.

How much do MySmart Portal, MySmart Display and MySmart Thermostat cost?
of the products are free to KCP&L customers who live within the demonstration area.

Will KCP&L control MySmart Thermostat?
KCP&L will cycle your air conditioner to raise or lower the temperature a few degrees on days when demand is high on the electric grid or when there is distribution congestion in specific areas.. This helps keep costs low and avoids electricity shortages. You always have complete control over how the thermostat is programmed to fit your lifestyle.

Will I be notified in advance of a MySmart Thermostat cycling event?
Yes. When the decision is made to initiate a cycling event, a notice will be posted on the KCP&L SmartGrid Web site's MySmart Thermostat page. KCP&L will also send messages to the MySmart Thermostat, as well as, the MySmart Portal that provide notification of an event.

Return to Top

Can I cancel my participation in MySmart Portal, MySmart Display or MySmart Thermostat?
This program is voluntary, so you may cancel at any time. For MySmart Portal, you simply either don't log in to AccountLink or don't visit that page. MySmart Display will need to be returned to KCP&L if you no longer wish to have it. Call 1(800) 535-7687 to find out what to do. MySmart Thermostat will need to be removed from your wall. Call 1(800) 535-7687 to schedule an appointment and KCP&L will remove the thermostat at no cost to you.

How much can I expect to save on my electric bill with MySmart Portal, MySmart Display and MySmart Thermostat?
These products are designed as visual aids that help you see where and when you are using your electricity. With this information, you can change your behaviors and habits to help lower your consumption thus lowering your bill. Actual savings will vary depending on what action is taken.

What is the difference between MySmart Portal and MySmart Display?
The data shown on the MySmart Portal is a day behind, so if you are looking at it on Sunday, you will see Saturday's usage patterns. MySmart Display is near real-time usage data that shows how much you are using every 15 minutes.

How do I install MySmart Display?
MySmart Display communicates wirelessly with your home's smart meter via radio signals, and provides reliable transmissions with little interference, so all you have to do is plug it into an outlet.

Where should I put MySmart Display?
MySmart Display should be located within 30 to 60 feet of the meter, depending on the way your home is constructed. You can place it in a convenient and easy-to-view location, but for maximum benefit, we recommend placing in a high traffic area like a family room.

How do I use MySmart Portal, MySmart Display and MySmart Thermostat?
MySmart Portal and MySmart Display have online instructions you can view on www.kcplsmartgrid.com. You also should have received a DVD when you received your meter that has instructions on how to use the products. If you need more help using it our troubleshooting, please call our SmartGrid Support Team at 1(800) 535-7687. When MySmart Thermostat is installed, the technician will teach you how to program it to fit your lifestyle.

How does MySmart Portal compare me to my community?

http://www.kcplsmartgrid.com/products_and_services/Productfaqs.html 12/20/2010

of how you use energy compared to similar homes in your community. This allows you to think about ways you could change your electricity-using habits.

Return to Top

P.1.1.19 SmartGrid Solar

SmartGrid Solar

KCP&L SmartGrid
the future of energy

This project is coming soon

A key component of KCP&L SmartGrid and the future of energy is the addition of distributed renewable energy. As part of the SmartGrid project, KCP&L is working to install up to 180 kW of solar energy generation throughout the demonstration area. Solar panels will be primarily integrated into leased rooftop spaces of a limited number of schools, commercial buildings and neighborhood structures.

The solar energy generated from these installations will be connected directly to the electric grid, which will allow KCP&L to study the dynamics and availability of renewable energy. Over time, it is expected more and more customers will utilize on-site, or distributed, generation to provide power. By synchronizing this distributed energy with the grid, and providing real-time visibility and energy information to system operators, the SmartGrid can operate more efficiently and distribute power where it's needed.

Brightergy Solar Solutions

Kansas City, Missouri School District

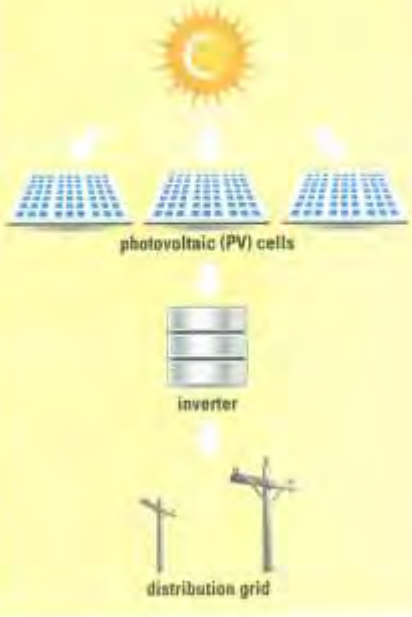
Showcase investment:

Paseo Academy of the Arts
4747 Flora
Kansas City, MO 64110

- 100 kW SunPower PowerGuard solar panel system
- Projected to produce 127,670 kWh of renewable energy per year
- Made in the USA
- Over a 25-year period, the system is expected to offset 2,500 tons of CO_2, the equivalent of planting 43 acres of trees
- To be installed by Brightergy and Alpha EE, in partnership with the IBEW Local 124

How Solar Panels Work

Solar panels are made up of photovoltaic (PV) cells. Similar to how a solar-powered calculator works, PV cells convert sunlight into electricity to help power homes and businesses. Typically, many, sometimes hundreds, of solar panels are wired together. The sunlight-produced energy is created and stored in the form of DC (direct current) power. The electricity is sent through an inverter that creates AC (alternating current) power so it can be used just like electricity supplied by KCP&L.



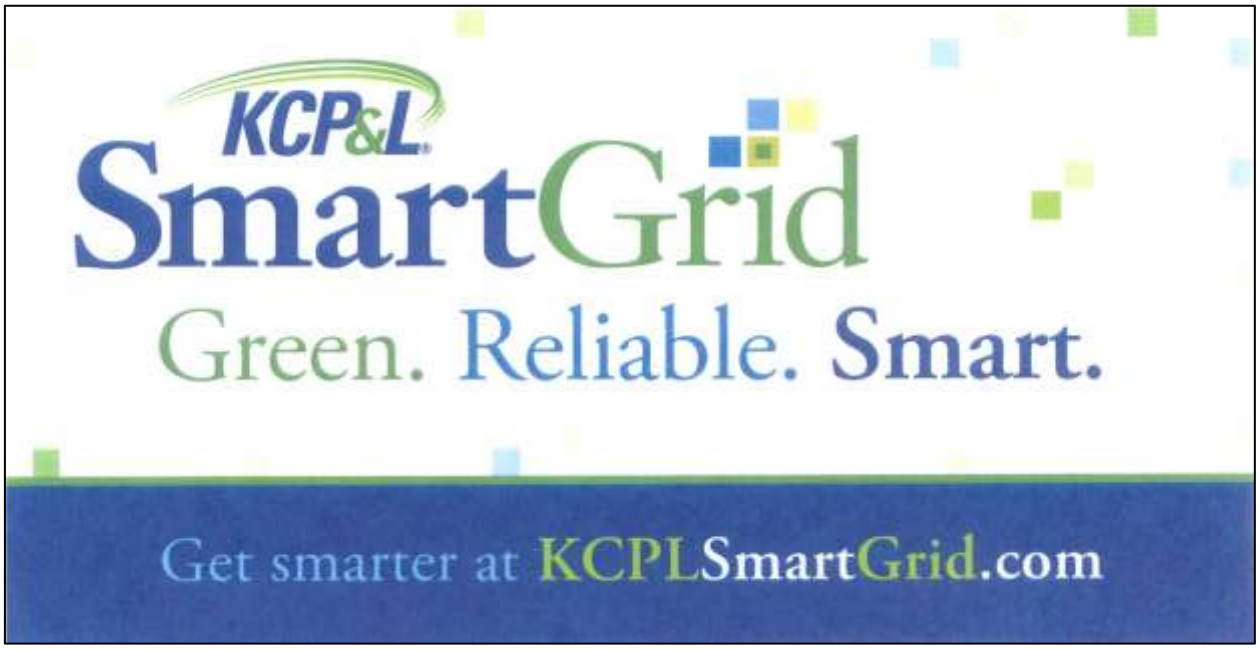
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

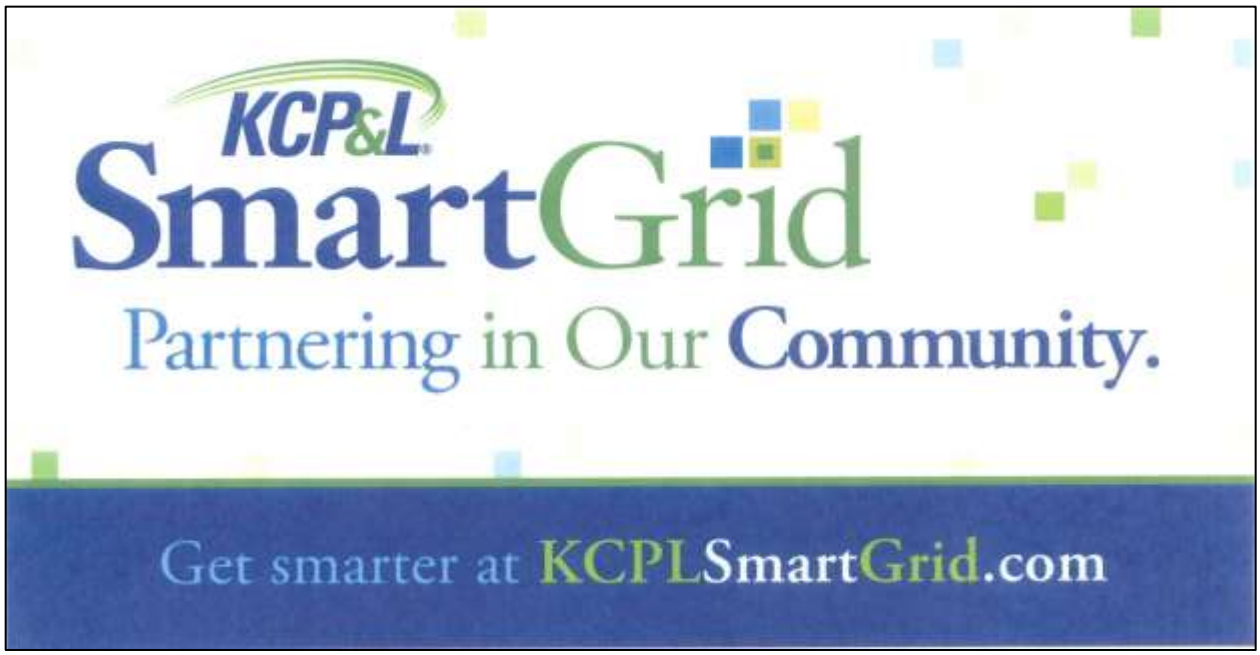
P.1.1.20 SmartSolar

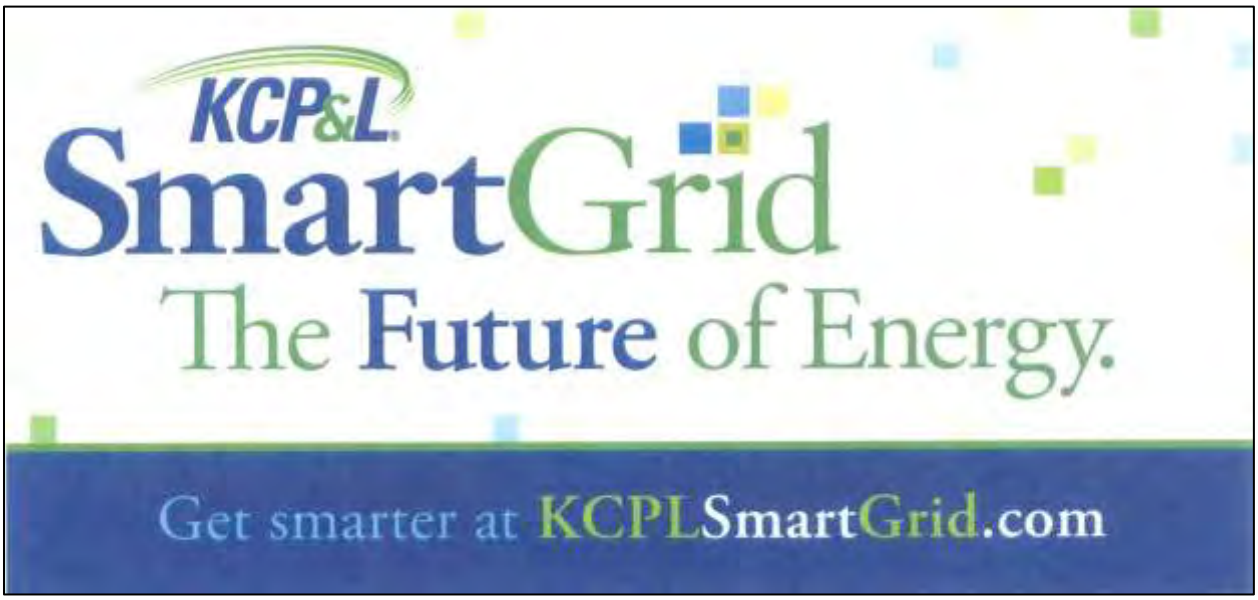
This page intentionally blank

P.1.2 Paid Advertising Initiatives

P.1.2.1 SmartGrid Billboards






KCP&L
SmartGrid
The Future of Energy.
Get smarter at KCPLSmartGrid.com

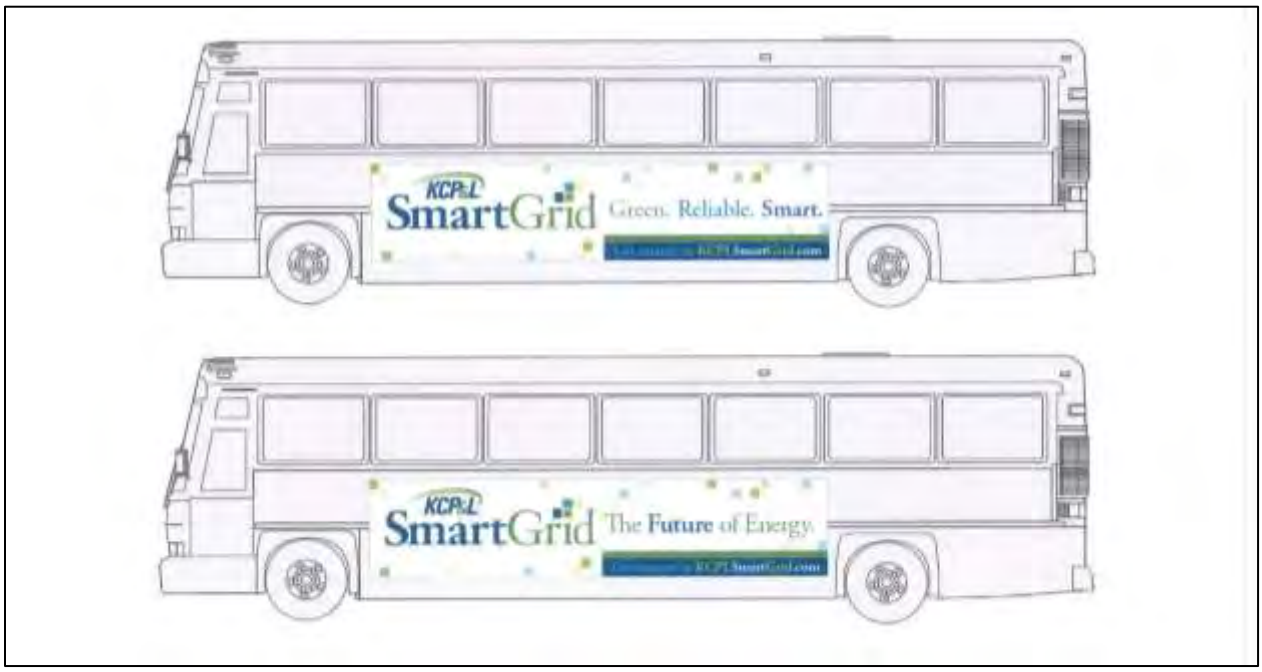

Get Smarter
Check out the Project Living Proof Home
at 917 Emanuel Cleaver II Blvd.
KCPLSmartGrid.com
KCP&L
SmartGrid
the future of energy


Get Smarter
Manage your energy use and save money with our free products and services.
KCPLSmartGrid.com
KCP&L
SmartGrid
the future of energy

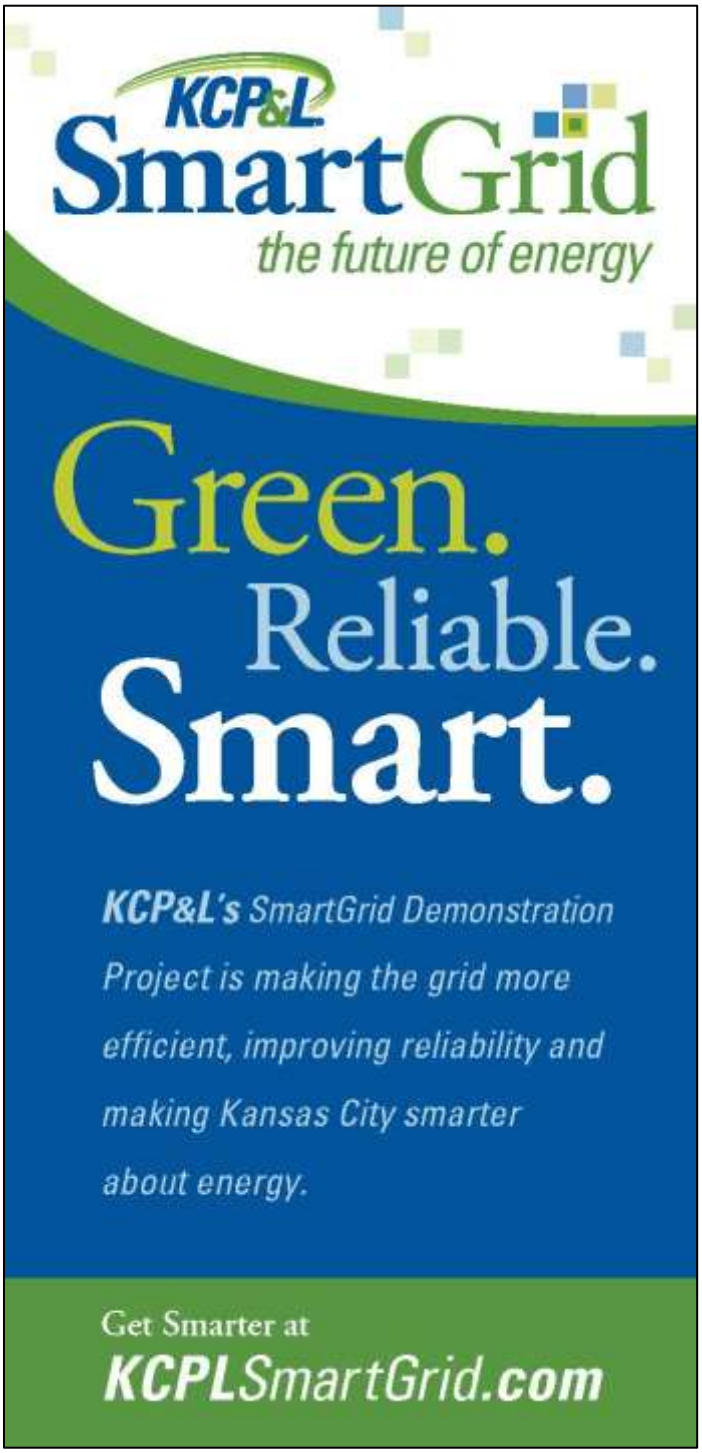

Get Smarter
Learn how we are improving the electric grid for a more reliable tomorrow.
KCPLSmartGrid.com
KCP&L
SmartGrid
the future of energy

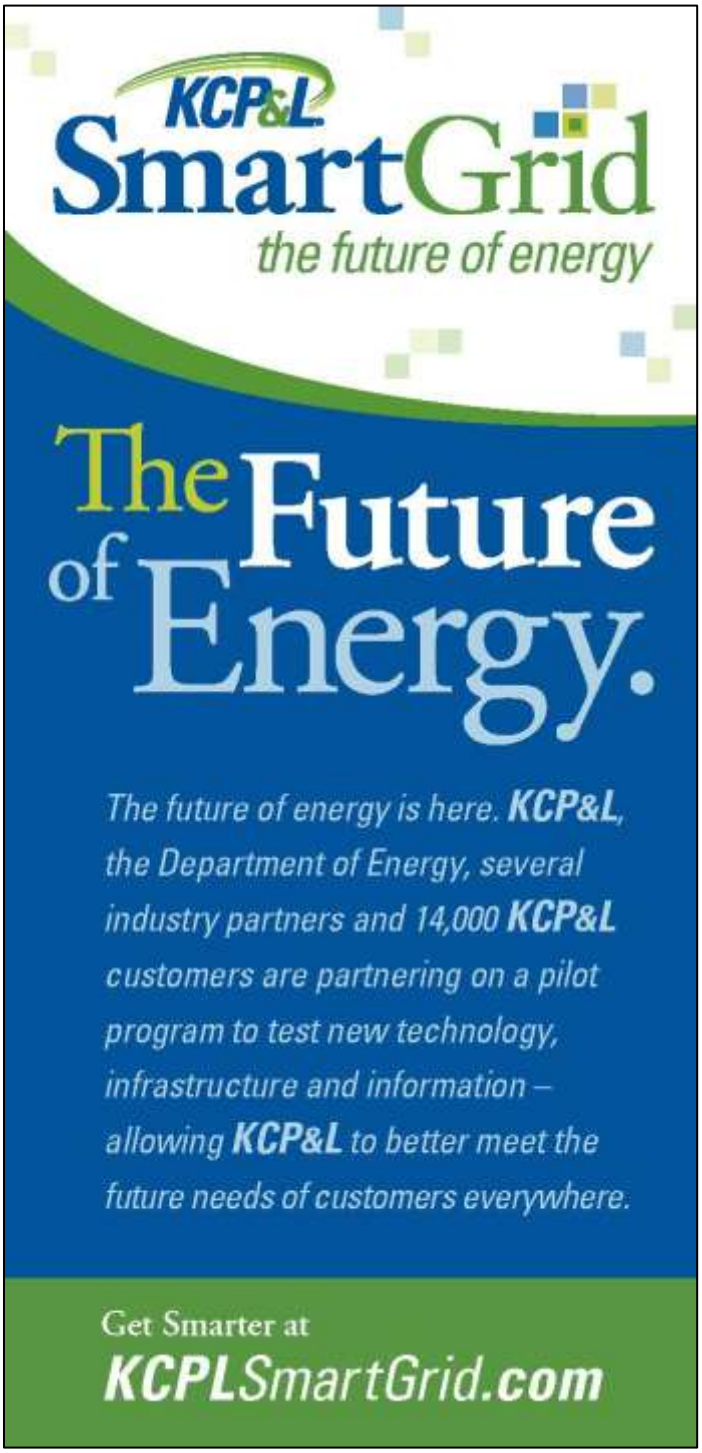

Get Smarter
Learn how your community is getting smarter.
KCPLSmartGrid.com
KCP&L
SmartGrid
the future of energy

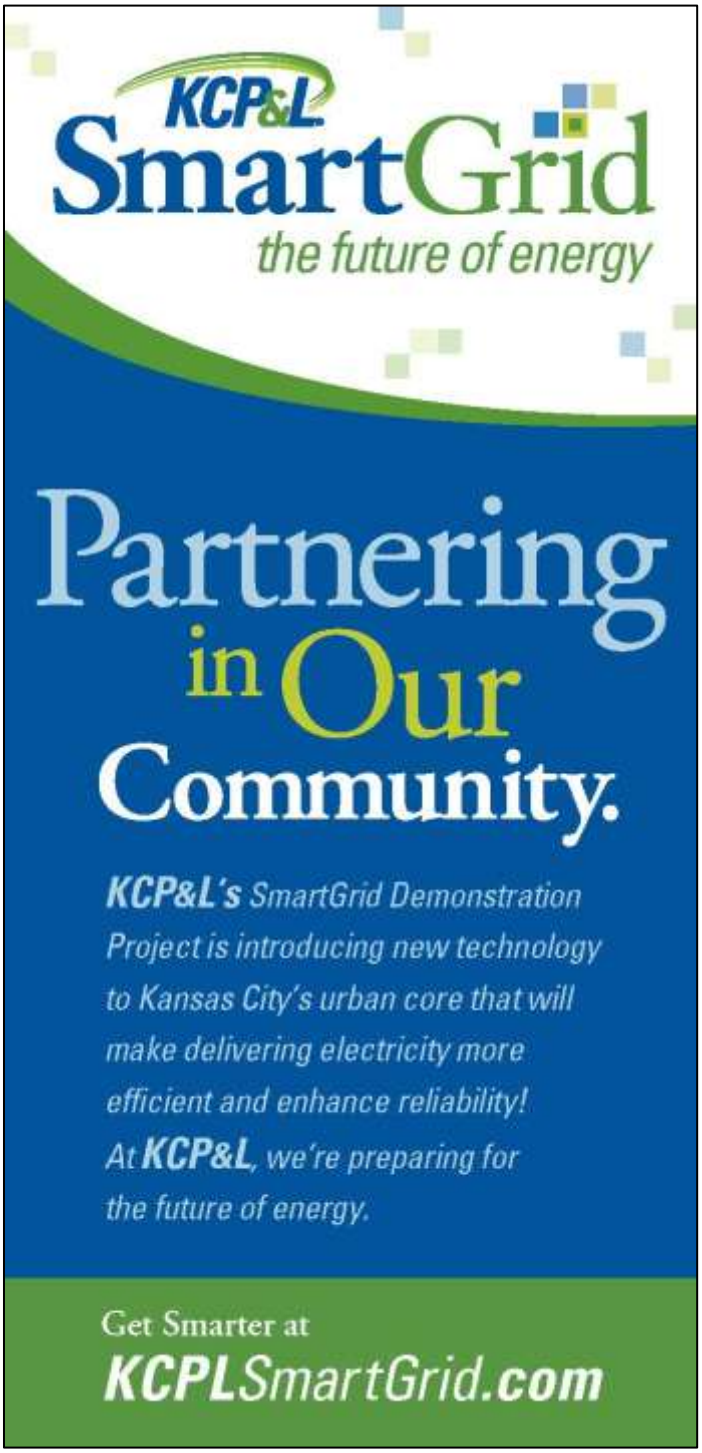
P.1.2.2 KCATA Bus SmartGrid Signage



P.1.2.3 Kansas City Star Newspaper Ads




KCP&L
SmartGrid
the future of energy
The Future of Energy.
The future of energy is here. KCP&L, the Department of Energy, several industry partners and 14,000 KCP&L customers are partnering on a pilot program to test new technology, infrastructure and information – allowing KCP&L to better meet the future needs of customers everywhere.
Get Smarter at
KCPLSmartGrid.com


KCP&L
SmartGrid
the future of energy
Partnering
in Our
Community.
KCP&L's SmartGrid Demonstration Project is introducing new technology to Kansas City's urban core that will make delivering electricity more efficient and enhance reliability!
At KCP&L, we're preparing for the future of energy.
Get Smarter at
KCPLSmartGrid.com

KCP&L

SmartGrid

the future of energy

Project Living Proof Home

OPEN HOUSE

Tour the home, see **SmartGrid** and other energy demonstrations, and learn about utility assistance and weatherization resources. **Food, face painting and activities for children!**

Saturday, April 30
11 a.m. to 2 p.m.

917 Emanuel Cleaver II Boulevard
Kansas City, Missouri

Please park in the Discovery Center parking lot at 4700 Troost.

MGE Missouri Gas Energy

EWK EnergyWorks KC

green impact zone

Metropolitan ENERGY CENTER

KCP&L energizing life

P.1.2.4 SmartGrid Innovation Park Battery Wrap

P.1.3 Kansas City Media Initiatives

P.1.3.1 The Green Impact Zone

Under the Clock: The Green Impact Zone Blog

Friday, March 27, 2009

The Green Impact Zone

Since the passage of the American Recovery and Reinvestment Act (ARRA), I have spent a great deal of time trying to help our community position itself in the best possible place to take advantage of this huge federal investment.

To that end, I have been meeting with community leaders, city staff, elected officials locally and Cabinet and administration officials in Washington, D.C. to advance the idea of targeting stimulus investments in a way that maximizes and deepens the impact of every dollar.

As a result of these meetings, Resolution No. 090254 has been introduced to the Kansas City Council that will target a portion of millions in stimulus funds to a hard hit area of Kansas City. We are calling the area the "Green Impact Zone."

Under this resolution the City Council commits to use a significant portion of the funds received under the ARRA for a focused area of the City bounded by 39th Street on the north, 51st Street on the south, Troost Avenue on the west and Prospect Avenue to 47th Street over to Swope Parkway on the east. Directly effected are the neighborhoods of Ivanhoe, Blue Hills, 49/63 and Manheim and Town Fork Creek, some of the City' strongest neighborhood organizations.

Through community discussions convened by the Mid-America Regional Council, an overarching goal of training and putting residents of these neighborhoods to work weatherizing every home that is eligible within the Zone has been suggested.

This is no small task, but has the potential of reducing utility bills, conserving electricity and creating sustainable jobs for a portion of our community where unemployment is hovering between 20-50 percent.

In a community where every dollar counts, reducing utility bills by half would be a significant achievement. Creating thousands of jobs would be a godsend and making neighborhoods east of Troost that have been historically last now be first should bring us all to our feet.

As the discussions of the Green Impact Zone have progressed, excitement has built and partnerships have been forged. Kansas City Power and Light has stepped up to the plate and committed that, if the city is willing to adopt this plan, KCP&L is willing to invest and deploy a "Smart Grid" in the Zone. In addition to making investments to put solar panels on newly weatherized homes, a "Smart Grid" would allow each home to receive a credit for unused solar energy that can be stored in batteries to be used for the rest of the grid. Their commitment is to create a model of the energy grid of the future unlike any in the country.

From Public Works to Parks and Recreation, both government and private dollars will be leveraged to create green sustainable jobs, enhance the neighborhoods and create a model for the rest of the nation.

This is a once in a lifetime opportunity and business as usual will not be good enough. For too long — and I am certainly guilty of perpetuating the problem — our City has drawn down federal dollars divided equally by six Council Districts and weakened the effect of the investments. We must target our funds. This Resolution No. 090254 will do just that. Those throughout the country who have the plans and are ready to go will

receive the most funding. The Green Impact Zone puts us at the front of the pack.

Thus far "green" investments have been reserved for those who can afford the upfront cost. In neighborhoods like these, where the median income is less than $20,000 a year, "greening" is simply not possible. This plan removes that burden and reduces the utility bills for those who need it most. With job training, neighborhood stabilization and infrastructure investments targeted here, "green" is no longer an academic concept for someone else — it becomes a means to change peoples lives right here in our urban core.

Let us seize this giant opportunity to create a better future and show America, when it comes to "green" we are in the lead.

Posted by Congressman Emanuel Cleaver, II at 4:22 PM

P.1.3.2 KCP&L to Receive Stimulus Grant for Kansas City SmartGrid Demonstration

NEWS RELEASE

KCP&L

MEDIA CONTACT:
Katie McDonald
Director of Corporate Communications
816-556-2365
katie.mcdonald@kcpl.com

INVESTOR CONTACT:
Ellen Fairchild
Director of Investor Relations
816-556-2083
ellen.fairchild@kcpl.com

FOR IMMEDIATE RELEASE

KCP&L TO RECEIVE STIMULUS GRANT FOR KANSAS CITY SMARTGRID DEMONSTRATION

Kansas City, Mo. (November 24, 2009) — Kansas City Power & Light Company ("KCP&L"), a subsidiary of Great Plains Energy Incorporated, (NYSE: GXP), is pleased to announce that the company has received a grant of just under $24 million to help fund a fully integrated SmartGrid demonstration project in the Green Impact Zone and Midtown areas of Kansas City, Mo. The grant was funded as part of the American Recovery and Reinvestment Act passed earlier this year. It is part of the Department of Energy's (DOE's) Office of Electricity and Energy efforts to modernize and strengthen the security and reliability of the nation's energy infrastructure.

"KCP&L has a long history of innovation, and we're proud to have this opportunity to continue developing new tools and programs for customers," stated Mike Chesser, KCP&L Chairman and CEO. "This project is one step on the road to creating the model for the electric utility of the future. It represents a tremendous opportunity for us to collaborate with our customers by providing them better service and far more control over their energy usage."

Unlike the traditional "one-way" electrical grid, the "two-way" SmartGrid will allow customers to better manage their electricity consumption by providing access to actual and predictive usage information, digital tools and innovative programs. The project will ultimately help KCP&L identify and improve beneficial energy-efficiency measures, electricity storage capabilities,

KCP&L energizing life

sustainable energy technology and electricity delivery systems. Customers should realize many benefits as a result, including improved service reliability, reduced outages and energy delivery costs.

"The Green Impact Zone is an exciting project that will provide an excellent opportunity to learn the potential for investments in SmartGrid technologies, energy efficiency and weatherization, distributed generation and demand response programs," said PSC Chairman Robert M. Clayton III. "The Missouri Public Service Commission will watch, with great interest, this project as it moves forward and the lessons to be learned from it, including best practices and what investments bring the most cost-effective return. Congressman Cleaver, MARC, KCP&L and the other participants should be commended for their leadership and vision for Kansas City."

"We are grateful that the Department of Energy saw the unique importance of this project that seeks to make a series of comprehensive technology investments in areas that are in the greatest need. The Green Impact Zone SmartGrid initiative will complement other efforts to weatherize homes and create jobs in the urban core, while providing a platform for us to expand SmartGrid technology to other parts of our system," Chesser added. "I would like to thank Congressman Cleaver for his vision in creating the Green Impact Zone and we look forward to partnering with the community to complete this project."

KCP&L's SmartGrid demonstration project will be located in Kansas City's Midtown urban core, bounded by Main St. on the west, Swope Parkway on the east, 37th St. on the north and 52nd St. on the south. It overlays the innovative Green Impact Zone that Congressman Emanuel Cleaver II announced last spring, but also extends beyond it to other area Midtown homes and businesses to gather a larger sampling of customer needs and preferences.

"Typically, 'green' investments have been reserved for those who can afford the upfront cost. In neighborhoods like these, where the median income is less than $20,000 a year, 'greening' is simply not possible," said Congressman Cleaver. "This plan removes that burden and reduces utility bills for those who need it most. We owe a debt of gratitude to KCP&L for taking the lead on this initiative and pulling together the right resources and partners to make the Green Impact Zone SmartGrid a reality. When you combine the SmartGrid with the job training, neighborhood stabilization and infrastructure investments also targeted here, 'green' is no longer an academic concept for someone else — it becomes a means to change people's lives right here in our urban core."

The total project is expected to cost more than $48 million, half of which is being paid for with stimulus funding through the U.S. Department of Energy. KCP&L, working with a coalition of SmartGrid industry partners, is planning to contribute an additional $24 million on the five-year project. Current project partners include Siemens, OATI, Landis+Gyr, Intergraph, GridPoint and Kokam America Inc. (Dow Kokam), who will provide equipment, technical expertise and in-kind financial support. The project is also receiving the support of The Electric Power Research Institute (EPRI), an independent, non-profit company that performs research, development and design in the electricity sector for the benefit of the public.

###

About KCP&L:
Headquartered in Kansas City, Mo., Great Plains Energy Incorporated (NYSE: GXP) is the holding company of Kansas City Power & Light Company and KCP&L Greater Missouri Operations Company, two of the leading regulated providers of electricity in the Midwest. Kansas City Power & Light and KCP&L Greater Missouri Operations use KCP&L as a brand name. More information about the companies is available on the Internet at: www.greatplainsenergy.com or www.kcpl.com.

Forward-Looking Statements:

Statements made in this release that are not based on historical facts are forward-looking, may involve risks and uncertainties, and are intended to be as of the date when made. Forward-looking statements include, but are not limited to, the outcome of regulatory proceedings, cost estimates of the Comprehensive Energy Plan and other matters affecting future operations. In connection with the safe harbor provisions of the Private Securities Litigation Reform Act of 1995, the registrants are providing a number of important factors that could cause actual results to differ materially from the provided forward-looking information. These important factors include: future economic conditions in regional, national and international markets and their effects on sales, prices and costs, including, but not limited to, possible further deterioration in economic conditions and the timing and extent of any economic recovery; prices and availability of electricity in regional and national wholesale markets; market perception of the energy industry, Great Plains Energy, KCP&L and GMO; changes in business strategy, operations or development plans; effects of current or proposed state and federal legislative and regulatory actions or developments, including, but not limited to, deregulation, re-regulation and restructuring of the electric utility industry; decisions of regulators regarding rates KCP&L and GMO can charge for electricity; adverse changes in applicable laws, regulations, rules, principles or practices governing tax, accounting and environmental matters including, but not limited to, air and water quality; financial market conditions and performance including, but not limited to, changes in interest rates and credit spreads and in availability and cost of capital and the effects on nuclear decommissioning trust and pension plan assets and costs; impairments of long-lived assets or goodwill; credit ratings; inflation rates; effectiveness of risk management policies and procedures and the ability of counterparties to satisfy their contractual commitments; impact of terrorist acts; increased competition including, but not limited to, retail choice in the electric utility industry and the entry of new competitors; ability to carry out marketing and sales plans; weather conditions including, but not limited to, weather-related damage and their effects on sales, prices and costs; cost, availability, quality and deliverability of fuel; ability to achieve generation planning goals and the occurrence and duration of planned and unplanned generation outages; delays in the anticipated in-service dates and cost increases of additional generating capacity and environmental projects; nuclear operations; workforce risks, including, but not limited to, retirement compensation and benefits costs; the ability to successfully integrate KCP&L and GMO operations and the timing and amount of resulting synergy savings; and other risks and uncertainties.

This list of factors is not all-inclusive because it is not possible to predict all factors. Other risk factors are detailed from time to time in Great Plains Energy's and KCP&L's most recent quarterly report on Form 10-Q and annual report on Form 10-K filed with the Securities and Exchange Commission. Any forward-looking statement speaks only as of the date on which such statement is made. Great Plains Energy and KCP&L undertake no obligation to publicly update or revise any forward-looking statement, whether as a result of new information, future events or otherwise.

P.1.3.3 KCP&L Launches SmartGrid Project

NEWS RELEASE

KCP&L

MEDIA CONTACT
KCP&L Media Hotline
(816) 392-9455

FOR IMMEDIATE RELEASE

KCP&L LAUNCHES SMART GRID PROJECT

Kansas City, Mo. (Nov. 10, 2010)— KCP&L announced today that the first stage of the company's SmartGrid project, a complete, two-way utility infrastructure upgrade in a number of Kansas City's Midtown and urban core neighborhoods, is currently underway. This project will be funded through a $24 million grant from the Department of Energy, which will be matched by KCP&L and the project partners.

In mid-October, KCP&L began installing new smart meters at residences and business located in the SmartGrid project area. The meter exchanges, which will affect 14,000 KCP&L customers, are anticipated to go through the beginning of 2011.

"This new meter unlocks the benefits of the smart grid for our customers living and working within the project area," said Mike Deggendorf, KCP&L senior vice president, delivery. "Customers will now have access to a suite of free products and tools that give them greater choice, convenience and control over how and when they use electricity. By using this information to manage their usage, customers can save money on their monthly bills.

KCP&L SmartGrid will also allow the company to test new products and technologies and better understand customer usage patterns and preferences. The SmartGrid project area includes Kansas City's Green Impact Zone. "This SmartGrid project is the first step toward creating the model for the electric utility of the future," said Deggendorf. "We expect it to serve as a blueprint for the industry as well as lay the groundwork for how we might introduce smart grid and its benefits to all of our customers, throughout our service region."

In addition, as part of the SmartGrid project, KCP&L will implement a number of energy-efficiency measures as well as test electricity storage capabilities, sustainable energy technologies and improved electricity delivery systems. These enhancements will result in benefits for all customers including improved service reliability, reduced outages and decreased energy delivery costs.

For more information about KCP&L SmartGrid please visit www.kcplsmartgrid.com.

####

About KCP&L:
Headquartered in Kansas City, Mo., Great Plains Energy Incorporated (NYSE: GXP) is the holding company of Kansas City Power & Light Company and KCP&L Greater Missouri Operations Company, two of the leading regulated providers of electricity in the Midwest. Kansas City Power & Light and KCP&L Greater Missouri Operations use KCP&L as a brand name. More information about the companies is available on the Internet at www.greatplainsenergy.com or www.kcpl.com.

P.1.3.4 KCP&L Completes Smart Meter Installation

NEWS RELEASE

KCP&L

MEDIA CONTACT
KCP&L Media Hotline
(816) 392-9455

FOR IMMEDIATE RELEASE

KCP&L COMPLETES SMART METER INSTALLATION

Successful completion of first phase of unique energy project

Kansas City, Mo. (April 29, 2010) — KCP&L announced today that it has successfully completed the installation of more than 14,000 smart meters at homes and businesses in the company's SmartGrid demonstration area*. This marks an important milestone for the project. During the process of installing new meters in the SmartGrid demonstration area, KCP&L hired several workers from the area. KCP&L utilized partnerships with QTI, Inc., The Full Employment Council and the Green Impact Zone to identify workers.

"These new meters, which we began installing in the SmartGrid project area last October, gave customers access to enhanced information about their electricity usage. Customers can use this information to change their behaviors resulting in monthly energy savings," said Mike Deggendorf, KCP&L senior vice president, delivery. "I want to thank all the customers, KCP&L employees and community partners who helped us complete this phase of the project. We look forward to helping both our residential and commercial customers realize the full potential and many benefits of this advanced technology."

For customers living in the SmartGrid project area, the smart meter is the key that unlocks the advantages of new smart grid technology. Customers now have access to several free innovative products*:

- **MySmart Portal**, a customized website that enables customers to manage their energy use.
- **MySmart Display**, a small in-home device that allows customers to monitor and manage their electricity use without Internet access.

- **MySmart Thermostat**, a programmable thermostat that can be used to preset temperatures based on season and personal preference.

KCP&L is partnering with a number of neighborhood and community organizations on the SmartGrid project, including the Green Impact Zone and the Metropolitan Energy Center. These organizations, along with Missouri Gas Energy, are all supporters of Project Living Proof, a demonstration house located at 917 Emanuel Cleaver Blvd that showcases KCP&L's SmartGrid as well as weatherization, landscaping and energy-efficient appliances. **Project Living Proof will host an open house on Saturday, April 30, from 11 a.m. until 2 p.m.**

"At the Project Living Proof house, customers can experience firsthand the full suite of SmartGrid products as well as learn more about how they can save energy and money," added Deggendorf. "We look forward to working with our community and project partners to introduce additional SmartGrid tools later this year, including a new MySmart Portal, a home area network, electric vehicle charging stations and several solar projects."

KCP&L SmartGrid was announced in November 2009 with the award of a $24 million grant from the Department of Energy, which is being matched by KCP&L and its SmartGrid project partners. This initiative is a five-year demonstration project that will serve as the blueprint for potential expansion of smart grid technology to other areas of the KCP&L service territory.

*For a map of the SmartGrid demonstration area, product feature videos and other additional information about KCP&L SmartGrid please visit www.kcplsmartgrid.com.

####

About KCP&L:
Headquartered in Kansas City, Mo., Great Plains Energy Incorporated (NYSE: GXP) is the holding company of Kansas City Power & Light Company and KCP&L Greater Missouri Operations Company, two of the leading regulated providers of electricity in the Midwest. Kansas City Power & Light and KCP&L Greater Missouri Operations use KCP&L as a brand name. More information about the companies is available on the Internet at www.greatplainsenergy.com or www.kcpl.com.

P.1.3.5 KCP&L Announces Solar Project in GIZ

NEWS RELEASE

KCP&L

MEDIA CONTACT:
KCP&L 24-hour Media Hotline
(816) 392-9455

FOR IMMEDIATE RELEASE

KCP&L ANNOUNCES SOLAR PROJECT IN GREEN IMPACT ZONE

Local high school solar installation will be largest in Kansas City metro

KANSAS CITY, Mo. (Oct. 28, 2011) — Today at an event with Congressman Emanuel Cleaver and school district leaders, Mike Chesser, Chairman and CEO of KCP&L, announced the largest solar energy system in the metro area. This system is being installed at the Paseo Academy of the Arts located in the Green Impact Zone.

KCP&L selected Brightergy Solar to install a 100 kW SunPower system, made in the USA, at the Paseo Academy (formerly Paseo High School). Once operational, teachers and students will learn how solar energy works by using an interactive display which will be connected inside the school by KCP&L. Including the system at Paseo Academy, KCP&L will be installing approximately 180 kW of solar energy generation as a part of its SmartGrid Demonstration in and around the Green Impact Zone.

One of KCP&L's goals for the solar installation is to create a partnership between solar vendors and the International Brotherhood of Electrical Workers (IBEW). Through this project, the IBEW Local 124 will partner with Brightergy to learn new renewable energy skills for its members. For the Paseo project, Brightery is partnering with Alpha EE, a minority-owned IBEW electrical contractor.

"Our commitment to the community drives everything we're trying to accomplish with our SmartGrid project," said Mike Chesser. "Creating partnerships with businesses and labor while engaging the youth of the community is a win for everyone involved."

1

"The Green Impact Zone is all about sustainability and making this area better tomorrow than it is today," said U.S. Congressman Emanuel Cleaver, II. "Some have called this area the 'Murder Factory'. Together, we are working to turn it into the 'Opportunity Factory', an energy-efficient community with more jobs, better housing and safer neighborhoods. A place we are proud to call home."

In late 2009, KCP&L received a grant from the Department of Energy through the American Recovery and Reinvestment Act to create a smart grid in and around the Green Impact Zone. The $48M project includes $24M from the federal government and $24M of private investment by KCP&L and its partners. KCP&L's SmartGrid is modernizing and automating the electric grid by integrating renewables and new technologies. Through a variety of tools, the SmartGrid is giving customers access to advanced energy information so they can manage their usage and potentially save money on their monthly bill.

In addition to installing more solar energy systems in 2011, future initiatives for the SmartGrid project include installing electric vehicle charging stations, connecting a large battery storage system, substation automation and additional customer tools.

####

About KCP&L
Headquartered in Kansas City, Mo., Great Plains Energy Incorporated (NYSE: GXP) is the holding company of Kansas City Power & Light Company and KCP&L Greater Missouri Operations Company, two of the leading regulated providers of electricity in the Midwest. Kansas City Power & Light and KCP&L Greater Missouri Operations use KCP&L as a brand name. More information about the companies is available on the Internet at www.greatplainsenergy.com or www.kcpl.com

About Brightergy:
Brightergy serves commercial and residential customers by providing solar energy design, financing, installation, and monitoring services. The company's BrighterFinance and BrighterLease financing options make it possible for building owners to switch to clean renewable energy without the high up-front cost. Headquartered in Kansas City, Brightergy's regional offices also serve St. Louis and Boston. Additional information about the company can be found online at www.brightergy.com.

P.1.3.6 KCP&L Officially Opens SmartGrid Innovation Park

NEWS RELEASE

KCP&L

MEDIA CONTACT:
KCP&L 24-hour Media Hotline
(816) 392-9455

FOR IMMEDIATE RELEASE

KCP&L OFFICIALLY OPENS SMARTGRID INNOVATION PARK

Educational kiosk and equipment showcase cutting-edge technology

KANSAS CITY, Mo. (Oct. 12, 2012) — Today, at an event with Congressman Emanuel Cleaver, II, KCP&L officially opened its SmartGrid Innovation Park. The park is open to the public and is located at 4727 Tracy Ave. in Kansas City, Mo.

KCP&L SmartGrid Innovation Park is an educational experience where visitors will learn about how KCP&L is piloting future energy technologies and enhancing the electric grid in Kansas City's urban core as a part of the SmartGrid Demonstration Project. At the park, visitors will see one of 13 SmartGrid solar arrays as well as a sophisticated, lithium ion battery storage system one of the largest of its kind in the country.

"Our SmartGrid project affects not only customers living and working in this area. What we are learning as part of this project about energy storage, advanced renewable energy technologies and improvements to our electric system will benefit all customers as we prepare for the future of energy," said Terry Bassham, KCP&L president & CEO. "It is an exciting time for the electric industry and we invite all customers to come out and see some of the new applications being piloted with customers and KCP&L."

One attraction for visitors to the park is an informational kiosk that explains several different aspects of the Demonstration Project including how power is delivered, the customer in-home experience and the history of electric meters.

"This exciting development captures the essence of the hard work going on in Kansas City's Green Impact Zone," said Congressman Cleaver. "This is a giant step forward and I commend the hundreds of people who have spent thousands of hours in this public/private partnership to get us to this day. For decades, this part of Kansas City has suffered from disinvestment and disappointment, but now continues the transformation into an economically thriving and energy-efficient treasure in the very heart of the city."

In addition to opening the park at the event, KCP&L also announced the future locations of its SmartGrid electric vehicle charging stations and solar arrays. For a list of these locations visit www.kcplsmartgrid.com.

With the help of a grant from the United States Department of Energy, KCP&L is investing more than $50 million in the SmartGrid Demonstration Project through 2015. The SmartGrid Demonstration Area includes several neighborhoods in and around Kansas City's Green Impact Zone. Approximately 14,000 customers live and own businesses in the SmartGrid Demonstration Area. For more information visit www.kcplsmartgrid.com.

#####

About KCP&L:
Headquartered in Kansas City, Mo., Great Plains Energy Incorporated (NYSE: GXP) is the holding company of Kansas City Power & Light Company and KCP&L Greater Missouri Operations Company, two of the leading regulated providers of electricity in the Midwest. Kansas City Power & Light and KCP&L Greater Missouri Operations use KCP&L as a brand name. More information about the companies is available on the Internet at www.greatplainsenergy.com or www.kcpl.com.

P.2 SmartGrid Demonstration Project Area Customers

P.2.1 Direct Mail Communications

P.2.1.1 Key Leaders Letter

August 31, 2010

(SAL) (FIRST NAME) (LAST NAME)
(STREET ADDRESS)
Kansas City, MO (INSERT ZIP)

Dear (INSERT SAL) (INSERT NAME):

As a recognized leader in our community, I want you to be among the first to know about a very exciting project at KCP&L. We recently received a grant from the United States Department of Energy to help us upgrade our electrical system in a number of Kansas City neighborhoods. The benefits of **KCP&L's SmartGrid** project include improved reliability and potential cost savings for customers. SmartGrid technology also allows for more efficient delivery of electricity, enabling cleaner, greener power.

In the coming days, all KCP&L SmartGrid customers will receive a letter about the new system and its benefits. In mid to late October, we will begin installing a new advanced communications network, including electric meters that connect area residences and businesses to the SmartGrid system. Customers also will receive a welcome kit that provides information on free smart grid tools and products to help them monitor and manage their energy use and costs.

Some elements of the SmartGrid project will be highly visible, including upgrades to our midtown substation, installation of electric vehicle charging stations and rooftop solar panels and an increased presence of KCP&L employees in the neighborhood. We know our customers will have questions about the project and, as a community leader, we need your help.

To familiarize you with SmartGrid, KCP&L and the Green Impact Zone will co-host a briefing for community leaders to introduce the project, answer your questions and discuss your ideas on how to make it a success. Please plan to join us.

Tuesday, September 14, 2010
5:30 pm – 7 pm
Green Impact Zone Office
4600 Paseo, Kansas City, Mo
Refreshments will be served
RSVP to rita.boyd@kcpl.com

A SmartGrid overview, including a map of the project area, is enclosed. You also can learn more at www.kcplsmartgrid.com. If you have any questions about SmartGrid, or to RSVP for the SmartGrid briefing, please contact Rita Boyd, KCP&L Community Outreach Manager, at 816-556-2971 or e-mail rita.boyd@kcpl.com.

We look forward to partnering with you on this project and hope to see you on September 14.

Sincerely,

Mike Deggendorf
Senior Vice President, Delivery

P.2.1.2 Welcome to SmartGrid Letter

All SmartGrid Customers Letter – Sept. 2010

(INSERT DATE)

(BUSINESS_NAME)
(ST_NBR) (PRE_DIR_CODE) (ST_NAME) (ST_SUFFIX) (APT_NBR) (BLDG_NAME)
(CITY_NAME), (STATE) (ZIP_CODE)

Dear KCP&L Customer:

I want to take this opportunity to share some very exciting news with you. With the support of a grant from the United States Department of Energy, KCP&L is preparing to make significant upgrades to the electric system in your neighborhood. You and your neighbors will be among the first customers to realize the benefits of KCP&L's **SmartGrid** project.

Our SmartGrid project will give you:

- More information about your electricity use,
- Greater control over how you use electricity, and
- Opportunities for cost savings.

Starting this fall, and continuing through the end of the year, KCP&L will install a new advanced communications network, including new electric meters, which is the first step in connecting you to the SmartGrid. Both before and after we install your meter, you will receive additional information about the free smart grid tools and products available to you. For small commercial customers, these tools will help you manage how and when you use electricity, which can result in lower monthly bills. For large commercial customers, a KCP&L energy consultant will be in touch with you to discuss SmartGrid benefits.

In addition, to make the SmartGrid project possible, KCP&L will be making major infrastructure upgrades to our SmartGrid substation and utility lines throughout the SmartGrid area, which will mean improved reliability, quicker outage response times and a reduced carbon footprint.

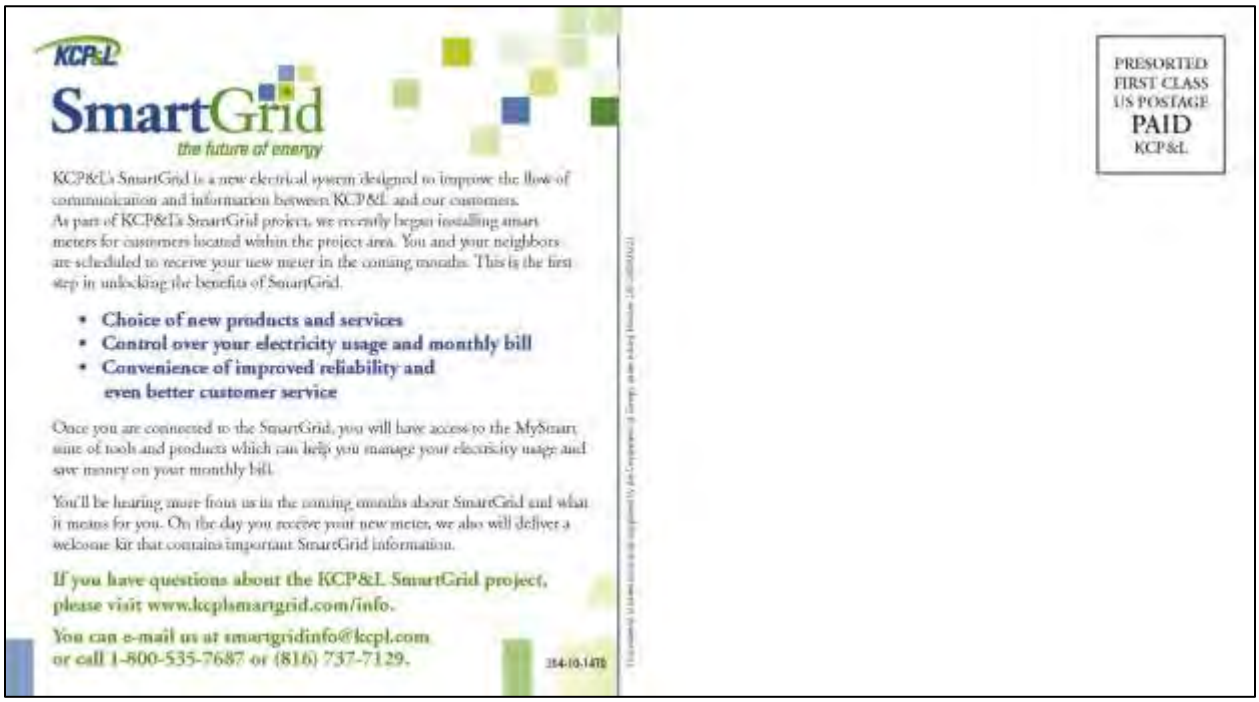
We promise to keep you fully informed as the SmartGrid project unfolds, so you know what to expect. In the meantime, to help you understand the many benefits of KCP&L's SmartGrid, we've included a project overview, including a map of the SmartGrid area. To learn even more about the SmartGrid project, please visit www.kcplsmartgrid.com.

We look forward to working with you on this important project.

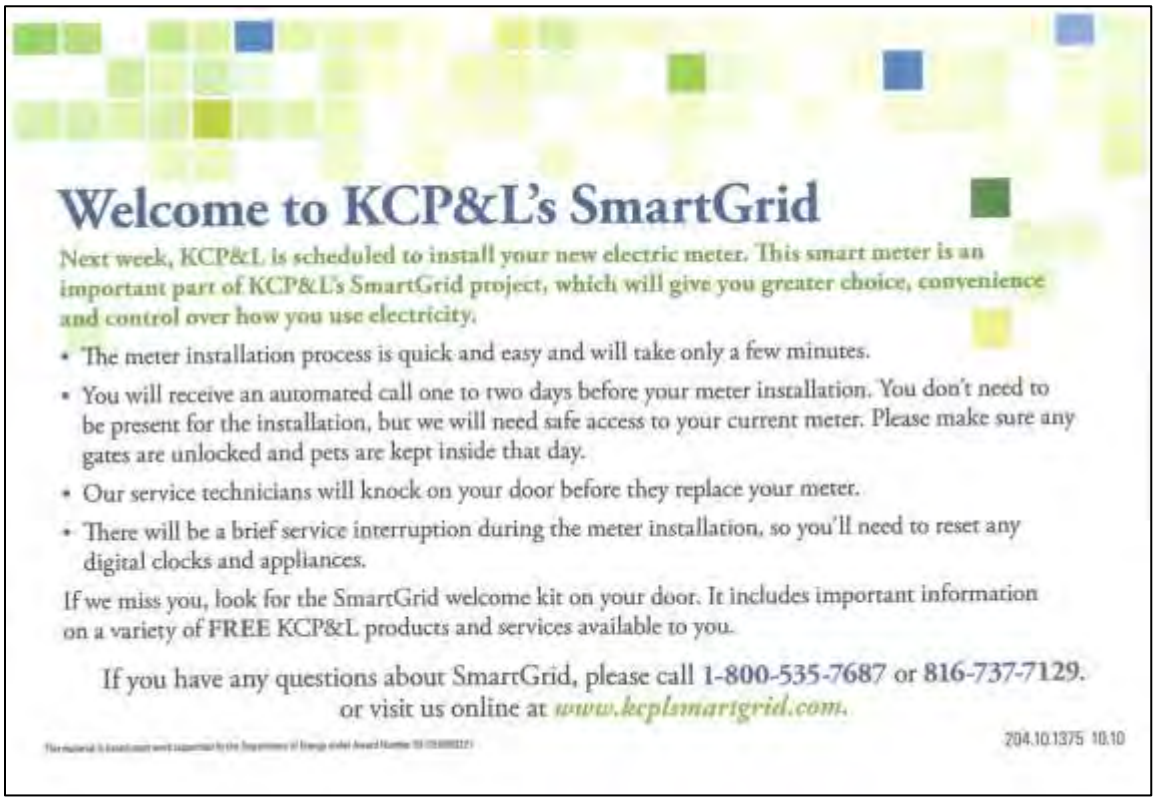
Sincerely,

Mike Deggendorf
Senior Vice President, Delivery

P.2.1.3 SmartGrid Postcard – Residential and Commercial



P.2.1.4 SmartGrid Meter Installation Postcard



P.2.1.5 Key Leader Update Letter

SmartGrid Key Leader Letter
DRAFT 1/5/11

(INSERT DATE)

(SAL) (FIRST NAME) (LAST NAME)
(STREET ADDRESS)
Kansas City, MO (Insert Zip)

Dear (INSERT SAL) (INSERT NAME):

As we begin 2011, we want to take this opportunity to provide you a brief update on the successful progress of KCP&L's SmartGrid project.

Just after Thanksgiving, we finished installing new SmartMeters at homes and businesses within the Green Impact Zone. These customers now have access to a suite of free products and services, providing greater choice, control and convenience over how they use electricity.

- **MySmart Portal** – A website that helps customers understand how they use electricity and enables them to make decisions that conserve energy, help the environment and save money.
- **MySmart Display** – A small wireless monitor that provides similar information as MySmart Portal without the need for an internet connection.
- **MySmart Thermostat** – A programmable thermostat that can automatically set temperatures based on the time and season, resulting in savings in monthly heating and cooling bills.

Over the last several months, we have visited with hundreds of people, visited neighborhood groups and held energy fairs within the project area to discuss the benefits of SmartGrid and proactively answer residents' questions. We've also contacted customers directly through a series of mailings, phone calls and the SmartGrid welcome kit that they received at the time of their meter installation. We have a dedicated SmartGrid Support Team available to answer questions and provide additional information to customers, and our website – www.kcplsmartgrid.com – is updated regularly and also now includes training videos for a number of our products. During this initial phase, we have partnered extensively with the staff of the Green Impact Zone. They have been particularly helpful as we launch the SmartGrid project.

We are now in the process of starting SmartMeter installation in the broader project area and we expect to have this phase completed in the next few months. In 2011, we also will undertake additional infrastructure projects related to SmartGrid, including upgrades to our midtown substation and installation of electric vehicle charging stations and solar demonstrations.

Later this month, you'll receive an invitation for an upcoming special event at Project Living Proof, the SmartGrid Demonstration House, located at 917 Emanuel Cleaver II Blvd., where you will be able to see firsthand the innovative products we're offering to SmartGrid customers.

As a recognized leader in our community, we hope to enlist your help in the SmartGrid project as we move forward. Thank you for your continued interest and support.

Mike Deggendorf
Senior Vice President

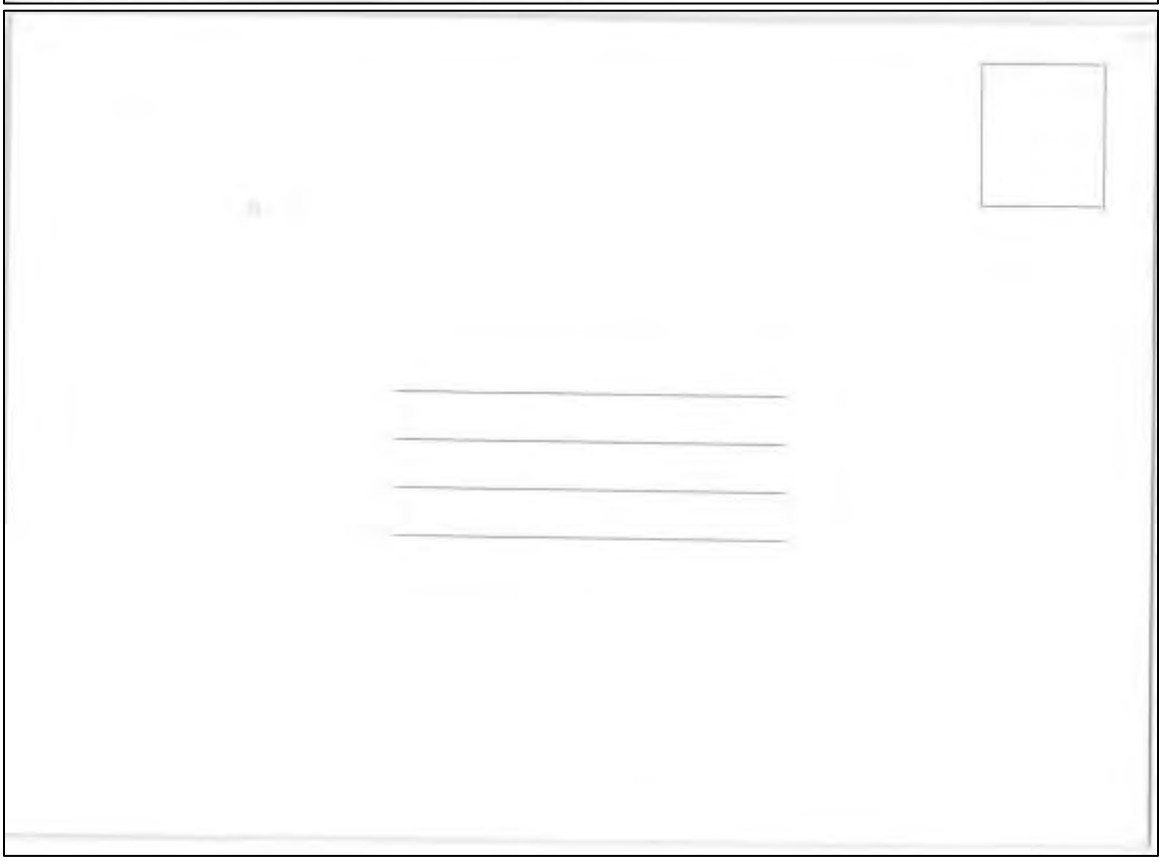
and

Bill Menge
SmartGrid Project Director

KCP&L | P.O. Box 418679 | Kansas City, MO 64141-9679 | 1-888-471-5275 (toll free) | www.kcpl.com

P.2.1.6 "Get Smarter" WebKey Teaser

P.2.1.7 "Get Smarter" WebKey Mailer



WHEN IT COMES TO SAVING ENERGY, KNOWLEDGE IS POWER.

As a resident of KCP&L's SmartGrid Demonstration Area, we are excited to put the key to smarter energy use in the palm of your hand. **It's as easy as 1-2-3.**

1. Pop out the webkey and attach it to your key ring (so you have it with you on a regular basis).
2. Plug the webkey into the USB port of any computer with Internet access.
3. Follow the registration instructions to activate your MySmart Portal account.

› You can access MySmart Portal as often as you like – the more you know about your energy use, the better you can manage it (and the more you can save on your monthly bills!).

The MySmart Portal webkey will launch KCP&L's web site and is safe for any computer.

MySmart Portal is a free online tool available exclusively to residents of KCP&L's SmartGrid demonstration area. MySmart Portal allows you to:

- View your estimated monthly bill and find out how much you've spent so far this month.
- Set energy saving goals and track your progress toward that goal.
- Get tips on what you can do in your home to reach your energy saving goal.
- Review dynamic charts showing your home's energy consumption and costs and how you're doing compared to your neighbors.
- Participate in discussions with your utility representatives and fellow SmartGrid participants.

› Log in to the MySmart Portal by inserting the webkey into the USB port of any computer with Internet access, or by visiting kcpl.com/webkey. You'll need your account number, which is found in the top right-hand corner of your bill.

› To learn more about the MySmartPortal and other SmartGrid resources available to you, visit www.kcplsmartgrid.com or contact us at smartgridinfo@kcpl.com or (800) 535-7687.

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221.

P.2.1.8 MySmart Product Letter

2012 SmartGrid Welcome Letter

Dear SmartGrid Customer,

As a valued KCP&L customer and a new resident in our SmartGrid demonstration area, I want to share some exciting news with you. In the fall of 2010, with the support of a grant from the United States Department of Energy, KCP&L began making significant investments in the electrical system in your neighborhood. The project is designed to provide you with more frequent and enhanced information about how you use electricity. The SmartGrid demonstration project's free products and resources will:

- Give you tools to use energy more efficiently;
- Help you make changes around your home or business that can save you money;
- Improve reliability in delivering electricity to you
- and shorten KCP&L's response time to power outages.

In addition, KCP&L is making significant infrastructure upgrades to its Midtown substation and network within the SmartGrid demonstration area to improve electrical service.

Because your home has been equipped with a SmartMeter, you have the opportunity to receive free tools to help you manage your energy use, including:

- **MySmart Portal** - Free web-based tool that allows you to monitor and manage your electricity usage.
- **Time of Use Rates** - Voluntary rate program designating "off peak" hours (when rates are discounted from standard) and "peak" hours (when rates are above standard). Designed to encourage customers to think about when they use electricity rather than just how much electricity they use, ultimately shifting electricity usage (grid load) from peak to off-peak periods.
- **MySmart Display** - Free portable electronic device that takes information directly from your electric meter and displays it for you in real-time.
- **MySmart Thermostat** - Free programmable thermostat that can be automatically set based on the season, time-of-day, and your schedule.
- **MySmart Home** - Free virtual hub that connects your home's appliances and electronics while remotely monitoring and controlling your MySmart Thermostat and other appliances

To help you better understand the many benefits of KCP&L's SmartGrid, we've included a welcome booklet about the project with this letter. Visit www.kcplsmartgrid.com to learn more about the SmartGrid Demonstration Project; or www.kcplsmartgrid.com/qualify to determine which free SmartGrid products would be best for you.

We look forward to partnering with you on this exciting project. KCP&L's dedicated SmartGrid Support Team is available to answer your questions at 1-800-535-7687 or SmartGridInfo@kcpl.com.

Sincerely,

Bill Menge
Director, SmartGrid

P.2.1.9 Time-of-Use Rates Letter

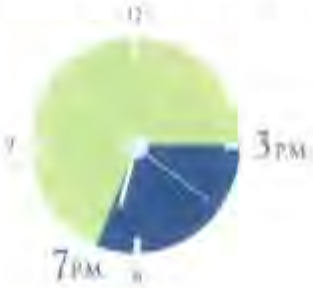
Time of Use Rates – Letter and Email Copy – W/ Guarantee
FINAL

Dear Customer,

As a resident of KCP&L's SmartGrid Demonstration Area, we are pleased to offer you another exciting opportunity to **Get Smarter** about your energy usage with the option to take advantage of **Time of Use rates.**

KCP&L's Time of Use rate pilot program allows customers to better manage their electricity costs while providing KCP&L information about customer behavior. The program designates "off peak" hours (when rates are discounted from standard) and "peak" hours (when rates are above standard). Time of Use rates are designed to encourage customers to think about when they use electricity rather than just how much electricity they use, ultimately shifting electricity usage (grid load) from peak to off-peak periods.

Time of Use rates are only active during summer months (May 16 – September 15). During that time peak hours (when rates are raised to about $.38/kWh) apply on non-holiday* weekdays from 3 to 7 pm. All other days and times during the summer months are designated as off-peak hours (when rates are discounted to about $.06/kWh).



You can try out Time of Use rates with no risk. If you notice that your bill has increased after enrollment, you may opt out of the program and request to be rebilled at standard rates for your most recent billing period.

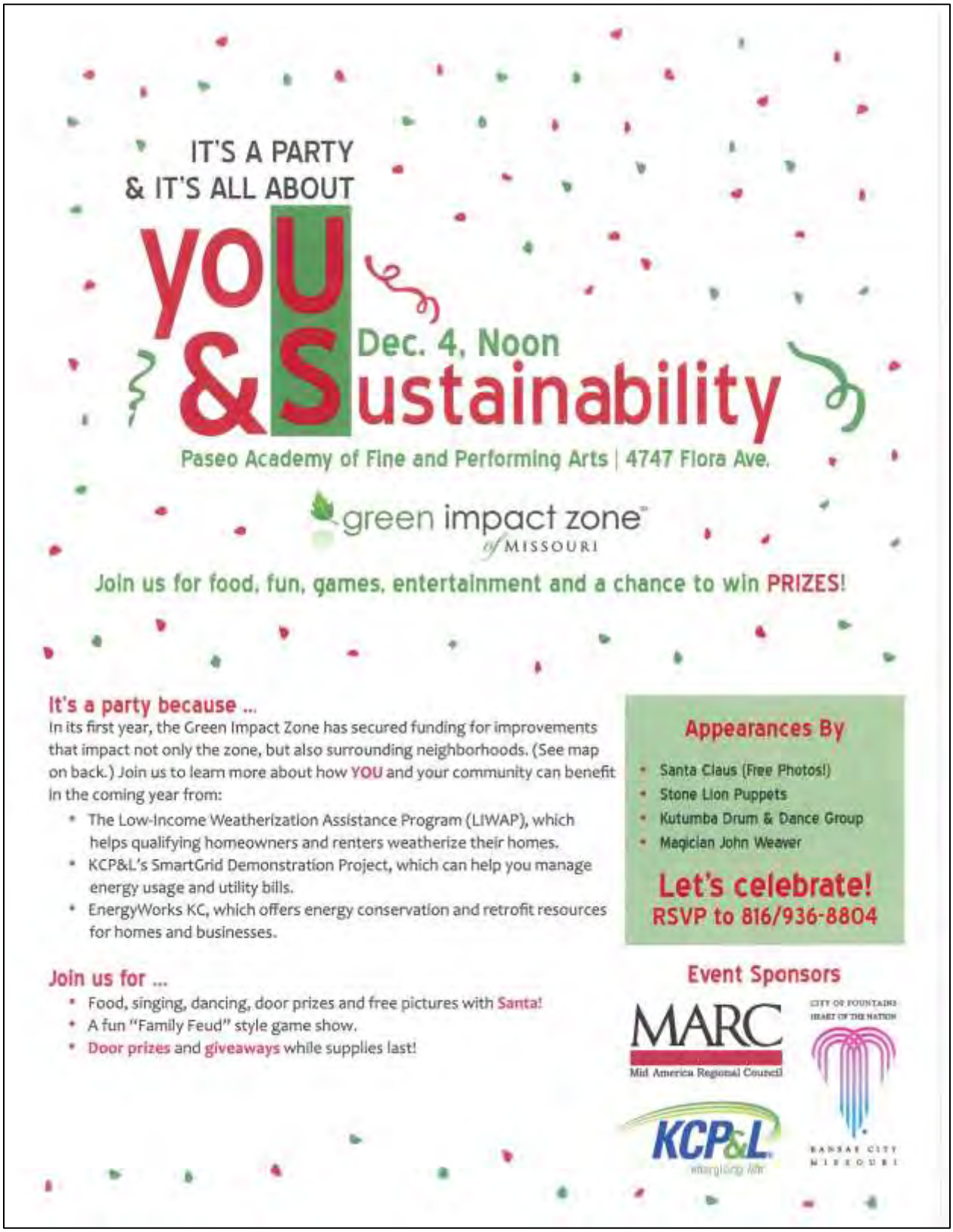
Are you interested in being among the first in Kansas City to take advantage of **Time of Use rates**? Call the SmartGrid Support Team at (800) 535-7687 to sign up. Then, look into other free SmartGrid Demonstration products at www.KCPLSmartGrid.com. These products can help you better manage your energy usage and monthly bill and make the most of **Time of Use rates**:

- ✓ **MySmart Portal** – Plan your Time of Use rates strategy by accessing MySmart Portal at www.KCPL.com/MySmartPortal, a free online tool that allows you to better monitor and manage your energy usage and make the most of off-peak rates.
- ✓ **MySmart Display** – Set alerts to remind you of changes in rates throughout the day and access real-time information about energy usage to help you reduce energy consumption and save money on your monthly bill.
- ✓ **MySmart Thermostat** – Maximize the impact of Time of Use rates by programming your thermostat to automatically adjust cooling based on peak hours (requires central air).
- ✓ **MySmart Home** – Connect your home's appliances and electronics to monitor and manage your energy use, while remotely monitoring and controlling your MySmart Thermostat and other appliances (requires central air and high-speed internet access).

To learn more about other SmartGrid resources available to you, visit www.KCPLSmartGrid.com or contact us at SmartGridInfo@KCPL.com or (800) 535-7687.

Sincerely,

P.2.1.10 You and Sustainability



P.2.1.11 TOU Renew for 2013 Letter

KCP&L SmartGrid
TOU Renew for 2013 Letter
5-8-13 DRAFT

INSERT DATE

INSERT NAME
INSERT ADDRESS
INSERT ADDRESS

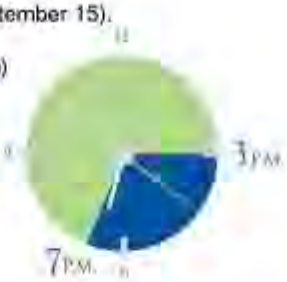
Dear KCP&L Time of Use Customer,

As a resident of KCP&L's SmartGrid Demonstration Area, you took advantage of the opportunity to **Get Smarter** about your energy usage by signing up for **Time of Use rates** last year. The program will begin again on May 16. As you prepare to participate, below is helpful information that describes the program.

As a reminder, KCP&L's Time of Use program allows customers to better manage their electricity costs while allowing us to better manage the demand for electricity across our system. The program designates "off-peak" hours (when rates are discounted from standard) and "peak" hours (when rates are above standard). Time of Use rates are designed to encourage customers to think about when they use electricity in addition to how much electricity they use, ultimately shifting usage to off-peak times.

Time of Use rates are only active during summer months (May 16 – September 15).

Peak hours = non-holiday weekdays from 3-7 p.m. (cost about $.38/kWh)
Off-peak hours = all other days/times (cost about $.06/kWh)



Remember, you can try out Time of Use rates with no risk. If you notice that your bill has increased after enrollment, you may opt out of the program and request to be rebilled at standard rates for your most recent billing period.

We look forward to your participation in the program again this year. As always you can call the SmartGrid Support Team at (800) 535-7687 with any questions. Also, take a look into other free SmartGrid Demonstration products at www.KCPLSmartGrid.com.

Sincerely,

Bill Menge
Director of SmartGrid
KCP&L