EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Remote Device Management Assessment

3002012588

Remote Device Management Assessment

3002012588

Technical Update, August 2018

EPRI Project Manager

P. Myrda

ELECTRIC POWER RESEARCH INSTITUTE
3420 Hillview Avenue, Palo Alto, California 94304-1338 ▪ PO Box 10412, Palo Alto, California 94303-0813 ▪ USA
800.313.3774 ▪ 650.855.2121 ▪ askepri@epri.com ▪ www.epri.com

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

This is an EPRI Technical Update report. A Technical Update report is intended as an informal report of continuing research, a meeting, or a topical study. It is not a final EPRI technical report.

NOTE

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

ACKNOWLEDGMENTS

The Electric Power Research Institute (EPRI) prepared this report:

Principal Investigator
P. Myrda

This report describes research sponsored by EPRI.

This publication is a corporate document that should be cited in the literature in the following manner:

Remote Device Management Assessment. EPRI, Palo Alto, CA: 2018. 3002012588.

ABSTRACT

Utilities are continuing to deploy ever increasing numbers of intelligent electronic devices (IEDs) across their systems with growing capabilities to capture, process, store, and communicate a wide range of data types. These IEDs fulfill a critical function by monitoring utility assets to provide the utilities with the data needed to operate the grid reliably, securely and efficiently. Historically there have been and continue to be challenges associated with both real-time and non-real-time communications, and the communications of non-real-time data with and between IEDs remains a difficult challenge. The difficulty is due to a number of factors, including disparate data types, multiple vendors with different solutions, lack of standards, the remote location of the devices, the need for secure communications, and the growing range of device management tasks that must be performed. Non-real-time data includes device management data, pass-through communications, and a variety of measurement-related data such as fault records. This research and report are focused on the data types involved with device management, which may be referred to as Secure Remote Access, Remote Substation Access, or Remote Device Management. For the purposes of this report we will use the term Remote Device Management (RDM).

Across the industry there is growing recognition of the substantial reductions in operations and maintenance costs, as well as improved security and reliability that can be achieved with effective RDM. The goal of an RDM system is to fully manage, update, secure, monitor and analyze all the remote IEDs of all types at all locations. Currently at many utilities there is limited or no RDM capability deployed. Therefore, field personnel may be required to drive to the substation, possibly in remote areas, to retrieve IED event files for fault location and event analysis. This additional activity can hamper restoration efforts and ultimately affect overall reliability performance. Other challenges include the lack of standard protocols for some functions and the lack of industry consensus on requirements, leading to a wide range of approaches between suppliers, and even with a single supplier’s products.

The purpose of this research and report is to assess the current state of RDM as implemented by the leading suppliers in this area. The topic is broken into two categories of enabling technologies and key functionality. Each of the two enabling technologies and five key functions are addressed with their own section in this report.

Keywords

Remote Device Management
Password Management
Firmware Management
Configuration Management
Asset Discovery

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1
INTRODUCTION

Utilities are continuing to deploy ever increasing numbers of intelligent electronic devices (IEDs) across their systems with growing capabilities to capture, process, store and communicate a wide range of data types. These IEDs fulfill a critical function by monitoring utility assets to provide the utilities with the data needed to operate the grid reliably, securely and efficiently.

Historically there have been and continue to be challenges associated with both real-time and non-real-time communications. For many years' real-time communications was difficult due to the lack of well-maintained industry standards that supported the needed functionality, required conformance testing and were widely adopted by manufacturers to be readily available to utilities. Although some challenges do remain, interoperable real-time communications between IEDs is now largely solved. However, the communications of non-real-time data with and between IEDs remains a difficult challenge. The difficulty is due to a number of factors including disparate data types, multiple vendors with different solutions, lack of standards, the remote location of the devices, the need for secure communications and the growing range of device management tasks that must be performed. Non-real-time data includes device management data, a variety of measurement-related data such a fault records and pass-through communications. This research and report are focused on the data types involved with device management which may be referred to Secure Remote Access, Remote Substation Access or Remote Device Management. For the purposes of this report we will use the term, Remote Device Management (RDM).

A Preferred Future for RDM

Across the industry there is growing recognition of the substantial reductions in operations and maintenance costs as well improved security and reliability that can be achieved with effective RDM. The goal of an RDM system is to fully manage, update, secure, monitor and analyze all the remote IEDs of all types at all locations.

Summary of the Current State

The current situation at many utilities is that there is a limited or no RDM capability deployed. Therefore, field personnel may be required to drive to the substation, possibly in remote areas, to retrieve IED event files for fault location and event analysis. This additional activity can hamper restoration efforts and ultimately affect overall reliability performance.

Other challenges include the lack of standard protocols for some functions and the lack of industry consensus on requirements leading to a wide range of approaches between suppliers and even with a single supplier's products. Therefore, one of the key considerations in choosing a supplier of an RMD system is whether and to what extent a specific IED is supported. This is referred to as multi-vendor support.

Unfortunately, it is difficult to deploy the ideal RDM multi-vendor solution today because the full range of standards, IEDs, systems and methods to support such a solution does not exist today. In addition, many utilities do not have the communications infrastructure in place to enable the full RDM functionality that is possible.

The following is a summary of the factors driving the challenge in addressing full RDM functionality:

- Different data types
- Multi-vendor environment
- Different communications methods (dial-up, serial, local area network (LAN))
- Inadequate communications architecture and infrastructure
- Lack of protocol standards that addressed the full range of needs
- Proliferation of vendor-specific protocols and data formats
- No uniform supplier practices for passwords, security protocols, faceplate designs and display formats.
- Lack of consensus on the requirements
- Departmental (utility) specific approach to requirements
- Growing security requirements and NERC CIP (Critical Infrastructure Protection) regulations

Utility deployments of RDM will generally fall into one of three situations:

- Little or no capability
- Limited functionality
- Improved functionality

Defining RDM

The goal of an RDM system is to fully manage, update, secure, monitor and analyze all the remote IEDs of all types at all locations. With that objective in mind, an RDM system will typically support the following functions.

Core Functions

1. Asset discovery
2. Asset inventory
3. Configuration management
4. Firmware / patch management (this report)
5. Password management
6. Pass-through or proxy connection for engineering access
7. Data collection (including alarms and alerts)
8. Device health
9. Compliance reporting

10. Ability to manage all available IEDs
11. Comprehensive security features
12. Support of NERC compliance

Other Functions

1. Secure remote “engineering” (manual) access to all substation devices (IEDs)
2. Integrated with (automated) file extraction as part of an overall data integration solution.
3. Automated data file “push” to the central remote access server.
4. Serve as a replacement for a Windows Terminal Server (jump host).
5. Tool to aid in NERC CIP compliance.

Overview of this Report

The purpose of this research and report is to assess the current state of RDM as implemented by the leading suppliers in this area. The topic is broken into two categories of enabling technologies and key functionality. Each of the two enabling technologies and five key functions are addressed with their own section in this report.

a. Enabling technologies:
   - Architecture
   - Communications
b. Key functionality:
   - Asset discovery
   - Asset inventory
   - Configuration management
   - Firmware / patch management
   - Password management

Future work may address a comprehensive set of requirements including security provisions, protocol standards and tools and a utility of survey deployments, needs and wants. More detail on possible future research is included in Section 12 of this report.

2
SYSTEM ARCHITECTURES FOR REMOTE DEVICE MANAGEMENT

This section describes three of the most common system architectures used for RDM. Each architecture has advantages and disadvantages however clearly the Modern RDM Method provides by far the greatest benefits.

Dial-up with Supervised Switch Method

In its most basic form, remote access to a device can be implemented with dial-up capability, a "Supervised Phone Switch", a serial connected data concentrator and the end device itself. This system is illustrated in Figure 2-1 below. With this system a user would call into a system

operator and provide some identifying and authorizing information. This would normally include a verbal password which would be checked for validity. The system operator would then log the reported identity of the user and the time the authorization was being granted. The operator would then actuate the closure of a contact on a relay to physically close the connection on the copper phone line. This would then allow the user to connect a phone line to their computer and directly dial the substation or IED. The user would then launch a connection to the IED from their computer using a vendor specific application or in some cases, a generic terminal program. (Source: EPRI)

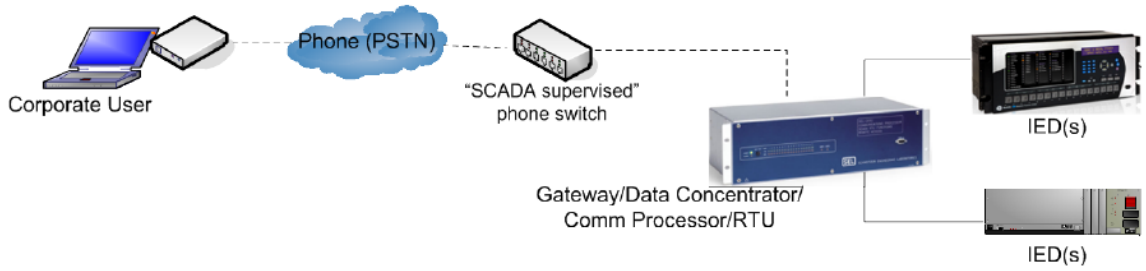

Figure 2-1
Dial-up with Supervised Switch Method (Source: EPRI)

Windows Terminal Server Method

An improvement on the Supervised Switch Method is shown in Figure 2-2 and utilizes a Windows Terminal Server within the utility DMZ (Demilitarized Zone) to host the devices native configuration and maintenance software. In this case the user would log in using network credentials or a two-factor authentication method using a token. A connection to the IED would then be launched from the server using a vendor specific application or in some cases, a generic terminal program.

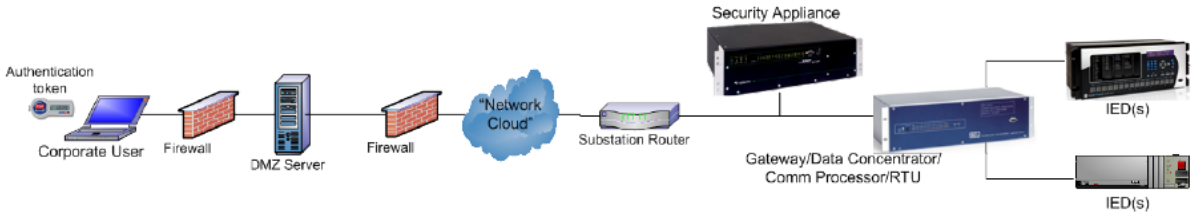

Figure 2-2
Windows Terminal Server Method (Source: EPRI)

Modern RDM Method—Integrated Architecture

To implement a modern RDM system several elements are required including the IED, substation gateway or data concentrator, communications and/or network components, one or more communication paths, secure remote access server, file repository (optional) and a secure remote access client. This method provides significant advantages over the other methods above in that this approach comes closer to the ideal RDM system allowing for more complete management and the device and retrieval of data.

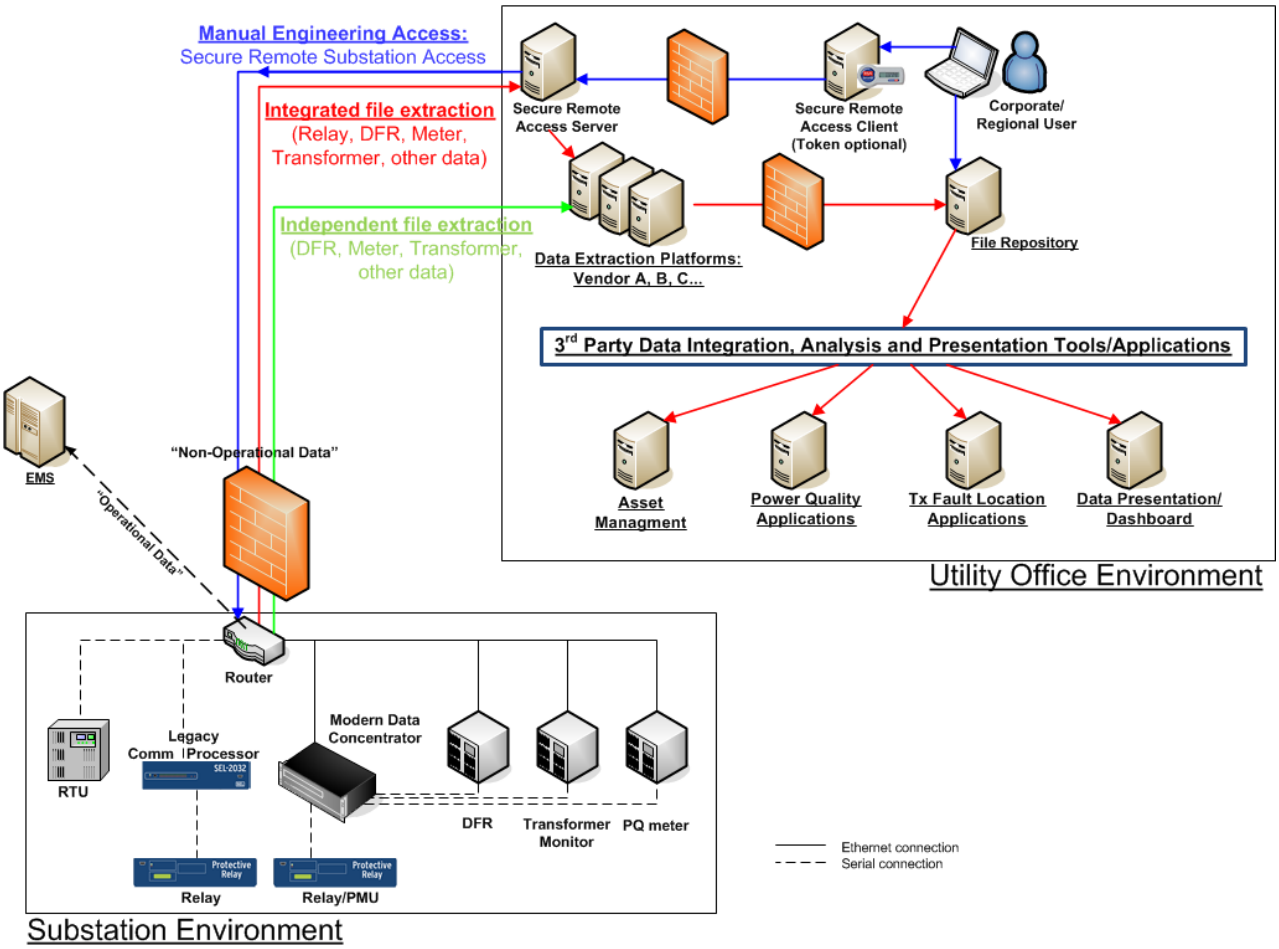

Figure 2-3
Modern RDM Method—Integrated Architecture (Source: EPRI)

3
DEVICES TO BE MANAGED

This section documents examples of the substation devices that may be considered for RDM using the methods described elsewhere in this report. In addition, feeder devices may be considered for RDM once or assuming an adequate communications infrastructure is in place.

Substation OT (Operational Technology) Devices to be Managed

Examples of power system related devices that come equipped with configuration and/or maintenance ports are as follows:

- Remote terminal units (RTUs)
- Gateways and data concentrators
- Digital relays
- Digital fault recorders (DFRs)
- Phasor measurement units (PMUs)
- Phasor data concentrators (PDCs)
- Substation meters and power quality meters
- Transformer and circuit breaker monitors
- Bushing monitors
- Load Tap Changers (LTC) monitors
- Tap changers
- Line reclosers
- Cap bank controllers
- Powerline carrier sets
- Sequence of event recorders (SERs)

Substation IT (Information Technology) and Security Devices to be Managed

Examples of IT and communications related devices that come equipped with configuration and/or maintenance ports are as follows:

- OT security gateways
- Network switches
- Routers
- Firewalls
- Security cameras
- Badge readers
- Local computing platforms
    - Historian

  - Automation platforms
  - Local data analytics
- Wireless access points (WAPs)

Other Substation Devices

Examples of IT and communications related devices that come equipped with configuration and/or maintenance ports are as follows:

- Security devices such as card readers
- Security cameras
- Digital video recorders

Feeder Automation Devices

In the future we should anticipate the need to manage devices installed on the feeder once an adequate communications infrastructure is in place including:

- Remote inverters
- Line reclosers
- Switch controllers
- Cap bank controllers
- Feeder RTUs

4
ARCHITECTURE ASPECTS

An effective architecture is key in enabling RDM. The extent of the benefits that can be realized from RDM are directly the result of the decisions made with the architecture. An effective architecture design starts with the business drivers and needs, incorporates cross-functional requirements, leverages best in class supplier offerings, adopts standards whenever possible, and considers limitations from the infrastructure, standards and supplier offerings when necessary. In addition, it is important to mandate, and drive changes where needed.

The focus of this research and this report is to assess the current state of the supplier offerings. Products and systems from the following six suppliers were reviewed:

1. Eaton (Cooper)
2. NovaTech
3. SEL
4. Siemens (Ruggedcom)
5. Subnet
6. TDi

In evaluating the offerings from the above suppliers, it is evident that there are three different architectural approaches, centralized, distributed and hybrid.

Table 4-1
Comparing Centralized and Distributed Architectures (Source: EPRI)

Centralized	Distributed
Fewer authorized computers allows for much tighter firewall filtering between enterprise and control networks	Less secure connections can be made physically closer to legacy equipment that lacks security features, and limited to within the physical security perimeter
All logs from device interactions can be retrieved through a single, centralized system	Maintains controlled access even if the substation backhaul is lost
No additional hardware/software is required at remote sites	One-time hardware costs, potentially no software licensing cost

Distributed Architecture

A distributed architecture is one that requires a remote hardware device containing RDM related applications including security installed in the substation or other location. In this example of a distributed architecture, Figure 4-1shows the SEL system offering with the SEL 3622/3620

Security Gateway installed at each substation and providing secure pass-through access using serial communications to the IEDs.

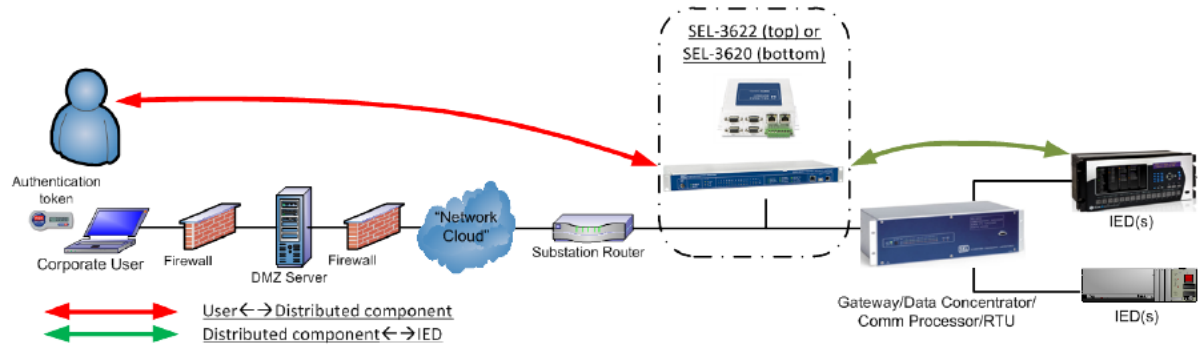

Figure 4-1
Example Distributed Architecture—SEL 3622/3620 (Source: EPRI)

Centralized (and Hybrid) Architecture

A centralized architecture is able to perform many of the defined RDM functions with only a remote access server (usually DMZ) server. A hybrid architecture is one that incorporates both a remote access server and optionally substation gateway devices. A hybrid architecture gives greater flexibility for situations where installing a substation gateway may not be practical and direct connection to the central host is necessary such as on a feeder. Figure 4-2 is an example of this architecture and shows the Subnet system which can operate with or without the substation gateway that is shown. The diagram includes all possible communication paths although all may not be needed. For instance, the blue line shows a direct connection between the central host (PowerSystem Center) and the IED which would only be used in the case of a location with no gateway. The green line depicts the logical connection between the remote access server and the substation gateway device (containing the SubstationSERVER.NET application suite) which carries all RDM related data including pass-through, passwords, configuration updates, firmware version, fault records and synchrophasor data etc. This communication path may include a wide range of other data types such as equipment condition data. Finally, the black line shows the logical communication path for real-time data and LAN-based time sync.

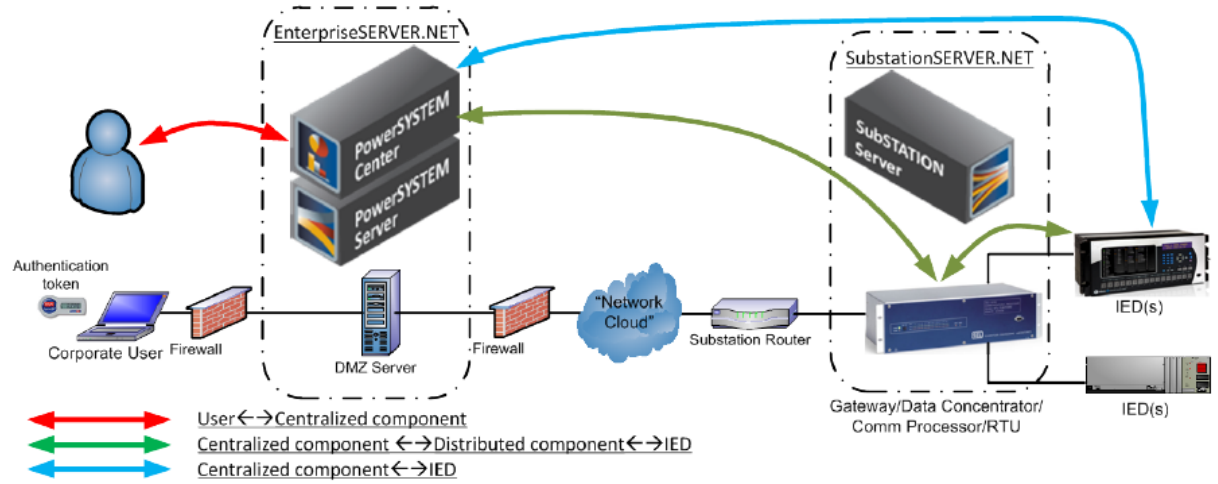

Figure 4-2
Example Centralized (and Hybrid) Architecture – Subnet (Source: EPRI)

Current State Assessment

A primary purpose of this research and report is to assess the current state of supplier offerings for RDM systems. A total of six supplier's RDM systems were reviewed. The result of this assessment is summarized in a series of five tables addressing five functional areas, with the first being Architecture and summarized in Figure 4-2 and the narrative below:

1. **Architecture**

   Of the six suppliers reviewed, five provide a centralized system that also support substation gateways so can function as centralized or hybrid as described above. The SEL system is the only one that requires a substation gateway to operate. The TDi does not have a substation gateway product offering but may offer a third-party product if requested.

2. **Tiered architecture of 'core' product**

   This criterion, also known as multilayered architecture, refers to a client-server architecture with the separation of presentation, application processing and data management functions. At the time of the review, only TDi provided a tiered architecture while Siemens indicated that development was occurring. In the case of Subnet and Eaton the "?" with the "No" may indicate that development was also occurring for their next generation offerings.

3. **Dedicated field product**

   Of the six suppliers reviewed, five offer a substation gateway product. Four of the suppliers offer their own substation gateway that can also serve as traditional data concentrators and RTUs. The Subnet SSNET shown in the table is an acronym for Subnet's SubstationSERVER.NET shown on Figure 4-2 which runs on SEL hardware platforms.

4. **Compatible RTU (Remote Terminal Unit) component**

   All the suppliers that offered substation gateway products also indicate that they offer traditional RTU functionality with direct input/output options.

5. **High availability/Redundant servers**

   All suppliers but NovaTech mention support for high availability with redundant servers. Although not stated in the literature as rapid or hot-standby, it is expected that the redundant servers are running in parallel. Therefore, the switch-over time should be acceptable depending on the application.

Table 4-2
Current State Summary of Suppliers —Architecture

Vendor:		Siemens	Subnet Solutions	SEL	Eaton	TDi Technologies	NovaTech
Product:	Architecture Aspects	CrossBow Secure Access Manager	Power System Center	SEL 3620	IED Management System (IMS)	ConsoleWorks	NovaTech Connection Manager (NCM)
	Architecture	Centralized	Centralized	Distributed	Centralized	Centralized	Centralized
	Location of 'core' product	Centralized	Centralized	Distributed	Centralized	Centralized	Centralized
	Tiered architecture of 'core' product	In development / Partial functionality	No	N/A	No	Yes	No
	Dedicated field product	Yes. Station Access Controller	Yes. SSNET	N/A. Only field product	Yes. SMP Gateway	No. Same platform	Yes. OrionLX
	Compatible RTU component	Yes.	Yes. SSNET	Yes. RTAC	Yes. SMP Gateway	No	Yes. OrionLX
	High availability/Redundant servers	Optional	Optional	Optional	Optional	Optional	

Summary

The preferred architecture is a hybrid which gives the most flexibility by allowing the utility to choose whether to install substation gateways. This is illustrated in Table 4-2 above showing the comparative advantages of the centralized vs distributed Architecture. In the case where minimal remote hardware is desired along with the associated cost savings, this is possible with a hybrid approach. At the same time, connections to legacy IED equipment can be made secure by locating substation gateways at the remote locations. The only gap of note in terms of architecture is a lack of tiered architecture offerings however this is being addressed by the suppliers with their next generation systems.

5
COMMUNICATIONS

Closely linked to and specified as part of the architecture, the capabilities of the communication interfaces between devices, systems and tools are a major enabler for an RDM system. Although the communications infrastructure is an important determinant in communications performance, the focus of this section is on the protocols and hardware interfaces used for RDM.

Figure 5-1 shows the internal and external communications connections of a typical substation with a wide range of devices installed and that supports RDM using the Supervised Switch Method which is summarized in Section 2 above.

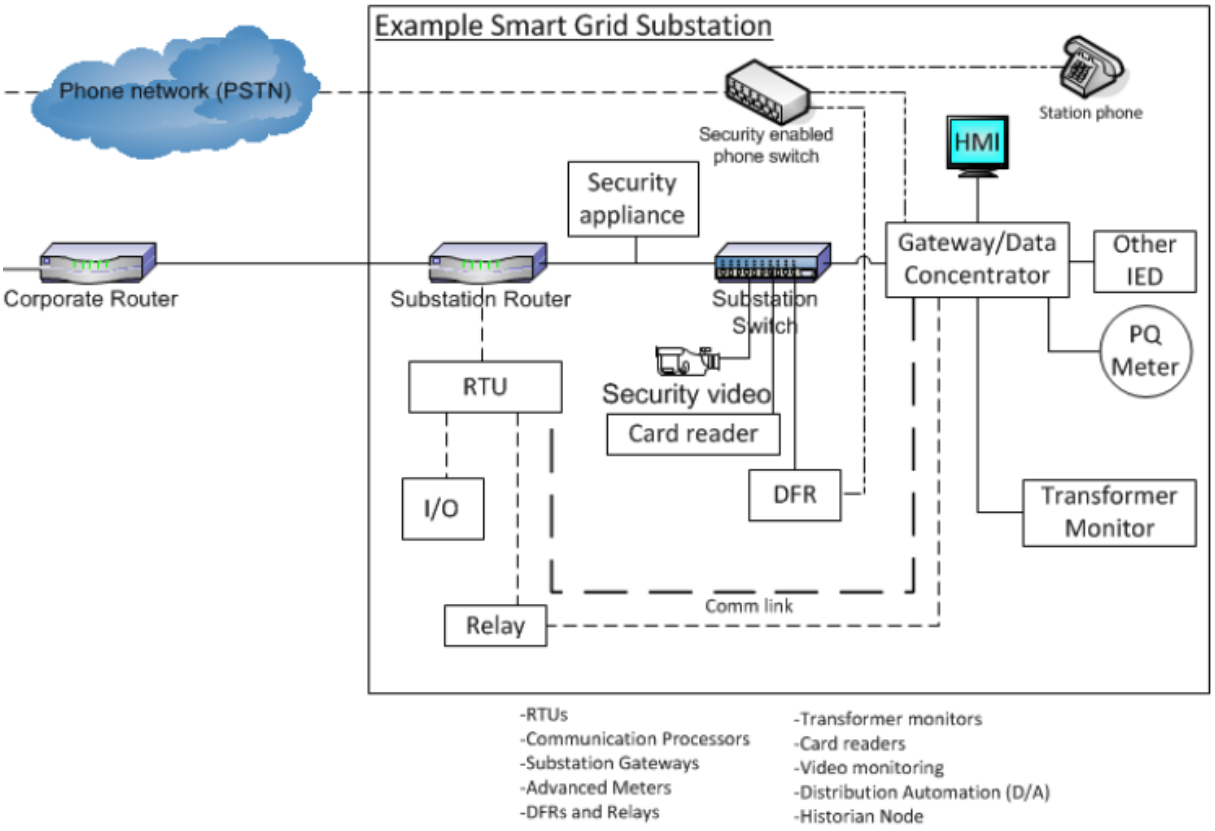

Figure 5-1
Example Smart Grid Substation Communications (Source – EPRI)

Sample Communications Requirements

Much of the communications within and external to a substation is handled by the substation gateway. The following is a basic sample list of requirements for communications related to RDM:

- TCP/IP (Transport Control Protocol/Internet Protocol) and UDP/IP (User Datagram Protocol/ Internet Protocol)
- ICMP (Internet Control Message Protocol)
- AH (Authentication Header) protocol and ESP (Encapsulating Security Payload) protocols
- SEL protocol communication support and enabling of auto-configuration
- Library of IED protocols including standard (eg. IEEE Std 1815) and vendor specific – serial and LAN (Local Area Network)
- Flexible parsing of SEL ASCII (American Standard Code for Information Interchange), generic ASCII and binary-based communications for unique devices
- Channel redundancy
- Up to date implementation of IEEE Std1815 (DNP3) including Secure Authentication Version 5
- IEC 61850 including associated specifications such as GOOSE (Generic Object Oriented Substation Event) and Sampled Values
- SNMP (Simple Network Management Protocol) - so network and IT assets within substations can be monitored
- FTP – File Transfer Protocol
- LDAP (Lightweight Directory Access Protocol)
- Radius (Remote Authentication Dial-In User Service
- Terminal server
- Security protocols such as TLS (Transport Layer Security), IPSec (Internet Protocol Security), SSH (Secure Shell)
- Syslog (System Log) protocol
- HTTPS (Hyper Text Transport Protocol Secure)
- X.509 Certificates
- OCSP (Online Certificate Status Protocol)
- IRIG-B (Inter-Range Instrumentation Group - Time Code Format B)
- NTP (Network Time Protocol)
- IEEE C37.238 (IEEE 1588)
- Additional protocols that are not directly used for RDM:
- Event file collection protocols
- Traditional SCADA (Supervisory Control and Data Acquisition) Master and Slave Protocols – serial and LAN
- Synchrophasor data protocols (IEEE Std. C37.118.1,2)

Current State Assessment

The assessment of the current state of supplier offerings looked at communications support for RDM systems. A total of six supplier's RDM systems were reviewed. The result of this assessment is summarized in Table 5-1 and the narrative below:

1. **Supports IP devices**

   All the suppliers support IP to their remote access servers and substation gateways.

2. **Supports serial devices**

   All the suppliers support serial interfaces to their remote access servers and substation gateways.

3. **Supports dial-up devices**

   Two suppliers (Siemens and Subnet) support dial-up interfaces to their remote access servers and substation gateways.

4. **Protocols used for device management**

   - **SCADA protocol** (Where supported) Modbus, IEC 61850, DNP3 or Other?

     All suppliers indicate that they support at least some of the list SCADA protocols.

   - ASCII

     All suppliers support at least some of the ASCII protocols in the industry.

   - Web interface

     All suppliers indicate that they support a web interface.

Table 5-1
Current State Summary of Suppliers—Communications

Vendor:			Siemens	Subnet Solutions	SEL	Eaton	TDi Technologies	NovaTech
Product:	Communications	Detail	CrossBow Secure Access Manager	Power System Center	SEL 3620	IED Management System (IMS)	ConsoleWorks	NovaTech Connection Manager (NCM)
	Supports IP devices		Yes	Yes	Yes	Yes	Yes	Yes
	Supports serial devices		Yes	Yes	Yes	Yes	Yes	Yes
	Supports dial-up devices		Yes, with Gauntlet gateway	Yes	No	No	No	No
	Protocols used for device management							
		SCADA protocol (Where supported) Modbus, IEC 61850, DNP or Other	Yes	Yes	Yes	Yes	Yes	Yes
		ASCII	Yes	Yes	Yes	Yes	Yes	Yes
		Web interface	Yes	Yes	Yes	Yes	Yes	Yes

Summary

As stated the supplier's RDM product offerings support communications criteria shown in the table above except for dial-up which is supported by two of the suppliers. However, one of the biggest challenges in implementing RDM for both the suppliers and the utilities is the proliferation of unique and vendor specific interfaces and methods in the IEDs. The worst examples of this are the ASCII interfaces needed for the older SEL relays. One supplier lists their supported IED interfaces according to the following functions in a six page document (in addition to standard real-time communications):

- Pass-through
- Password management

- Configuration management
- Fault and event retrieval

The result of this proliferation of non-standard interfaces is extra cost and complexity and reduced functionality in many cases.

6
ASSET DISCOVERY

Asset Discovery refers to the ability of the RDM system to automatically detect the connection of an IED to the substation gateway and/or the remote access server in the case that a gateway is not used.

Current State Assessment

The assessment of the current state of supplier offerings looked at asset discovery support for RDM systems. A total of six supplier's RDM systems were reviewed. The result of this assessment is summarized in Table 6-1 and the narrative below:

1. **Auto-Discover IP devices**

   Of the six systems reviewed, two indicate that they support auto-discovery for IP connected devices – TDi and NovaTech.

2. **Auto-Discover serial devices**

   Three of the systems reviewed indicate that they support auto-discovery for IP connected devices – Siemens (for SEL gateways), SEL and NovaTech.

3. **Confirm asset connectivity – IP**

   All six of the reviewed systems support confirmation of connectivity over IP. Four of the six specifically state that this is by polling or if the IED is used for SCADA.

4. **Confirm asset connectivity – Serial**

   All six of the reviewed systems support confirmation of connectivity over serial. Four of the six specifically state that this is by polling or if the IED is used for SCADA.

Table 6-1
Current State Summary of Suppliers—Asset Discovery

Vendor:		Siemens	Subnet Solutions	SEL	Eaton	TDi Technologies	NovaTech
Product:	Asset Discovery	CrossBow Secure Access Manager	Power System Center	SEL 3620	IED Management System (IMS)	ConsoleWorks	NovaTech Connection Manager (NCM)
	Auto-Discover IP devices	No	No	No	No	Yes	Yes
	Auto-Discover serial devices	Yes - for devices connected to SEL gateways		Yes			Yes
	Confirm asset connectivity - IP	Only by polling	By polling, or if asset is used for SCADA	Yes	By polling, or if asset is used for SCADA	Yes	By polling, or if asset is used for SCADA
	Confirm asset connectivity - Serial	Only by polling	By polling, or if asset is used for SCADA	Yes	By polling, or if asset is used for SCADA	Yes-Alerts on loss of connectivity	By polling, or if asset is used for SCADA

Summary

All the RDM systems support confirmation of connectivity over IP and serial. This is a straightforward function and is accomplished by polling as in the periodic interrogation of the device by the substation gateway or the remote access server. If a device loses connectivity an alert is normally sent to the operations and/or maintenance staff. Fewer systems support auto-discovery which is a very useful function but far more technically challenging. This capability assumes a way for a device to describe itself to the other components of the system either by the protocol or by prior configuration of a set of optional IED templates.

7
ASSET INVENTORY

Asset inventory refers to the ability of the RDM system to automatically retrieve and store details about the IED such as model number, type, firmware version and date etc. In addition, it would be preferable for the systems to provide device health information. Configuration version change management is addressed in more detail in Section 8. Ideally the RDM systems would also be able to integrate with Asset Management systems so the IED asset information can be maintained as part of the utility's overall asset management activity.

Current State Assessment

The assessment of the current state of supplier offerings looked at support for asset inventory data retrieval for RDM systems. A total of six supplier's RDM systems were reviewed. The result of this assessment is summarized in Tale 7-1 and the narrative below:

1. **Device information received**
   - **IED Model Number**

     All six systems support retrieval of IED model number.
   - **IED 'Category' (Transmission, Distribution, etc.)**

     It appears that only the NovaTech offerings can retrieve and store this information.
   - **IED 'Sub Category' (Protection, Automation and Control System)**

     Like the "Category" question above, it appears that only the NovaTech offerings can retrieve and store this information.
   - **Current IED Firmware**

     All six systems support retrieval of the current version number of the IED firmware.
   - **Latest Firmware version/Date (obtain and store from the supplier)**

     It appears that only the NovaTech offerings can obtain and store this information.
2. **Designed for Single vs Multiple locations/facilities (substations)**

   Four of the six systems can handle devices from multiple locations. The SEL system however handles device information from a single location. This makes sense as the SEL system is not designed to be centralized but requires a dedicated substation gateway at each location.
   - **Grouping categories**

     Only the Siemens solutions support grouping categories.
3. **Import from existing asset inventory (CSV—Comma Separated Variables)**

   Four of the systems support importing of device information in .csv format.

4. **Sync/Integration (API—Application Programming Interface) with Asset Management systems**

   None of the systems support integration with Asset Management systems.

   - **Cascade, Maximo, SAP, Other**

     See above

Table 7-1
Current State Summary of Suppliers—Asset Inventory

Vendor:			Siemens	Subnet Solutions	SEL	Eaton	TDi Technologies	NovaTech
Product:	Asset Inventory	Detail	CrossBow Secure Access Manager	Power System Center	SEL 3620	IED Management System (IMS)	ConsoleWorks	NovaTech Connection Manager (NCM)
	Device information received							
		IED Model Number	Yes	Yes	Yes	Yes	Yes	Yes
		IED 'Category' (Transmission, Distribution, etc)	N/A	N/A	N/A	N/A	N/A	Yes (from SEL website)
		IED 'Sub Category' (Protection, Automation and Control System)	N/A	N/A	N/A	N/A	N/A	Yes (from SEL website)
		Current IED Firmware	Yes	Yes	Yes	Yes	Yes	Yes
		Latest Firmware version/Date	No	No		No		Yes
	Designed for Single vs Multiple locations/facilities (substations)		Multiple	Multiple	Single	Multiple	Multiple	
	Import from existing asset inventory (CSV)		Yes	Yes	No	Yes	Yes	
	Sync/Integration (API) with Asset Mgmt systems		None	None	None	None	None	None
		Cascade, Maximo, SAP, Other	None	None	None	None	None	None

Summary

Overall the systems provide a rudimentary capability in support of Asset Inventory management. Basic capabilities such as model number and firmware version numbers are captured but very little functionality beyond that is provided. It would be preferable for the systems to provide device health information. In addition, the RDM systems should be able to integrate with Asset Management systems such as Cascade, Maximo, SAP and other so the IED asset information can be maintained as part of the utility's overall asset management activity.

8
CONFIGURATION MANAGEMENT

The management of device configurations is an important capability for RDM systems and contributes to overall system reliability and security. Key aspects include the ability to remotely download and compare configurations to an approved version. Configuration files may include core configuration files, settings files, logic files and custom pages. In the future this may also include uploading new configurations and/or on-line configuration changes however the obvious risk must be mitigated by sophisticated device and system designs, and security.

Current State Assessment

The assessment of the current state of supplier offerings looked at configuration management support for RDM systems. A total of six supplier's RDM systems were reviewed. The result of this assessment is summarized in Table 8-1 and the narrative below:

1. **Ability to retrieve IED configuration**

   All suppliers support the ability to retrieve the IED configuration.

   - Although it was not possible to determine whether the systems supported the detailed criteria it is very likely that parameters such as communication, device and security settings is included in retrieved configuration files however it may be necessary to use the IED's native configuration tool software to view this information.

2. **Feature: Comparison to baseline/approved version**

   All suppliers support the ability to compare the IED configuration to an approved or baseline configuration.

   - Generate alert regarding differences

     In addition, four of the six suppliers support generating an alert when a comparison between configurations indicates a difference.

3. **Feature: Reviewing/approving versions**

   Four of the six suppliers support generating an alert when a comparison between configurations indicates a difference.

   - Multiple (historical) versions stored

     Four of the six suppliers support storing of multiple historical versions of the device configurations.

   - Feature: Workflow functionality

     Four of the six suppliers support workflow functionality.

Table 8-1
Current State Summary of Suppliers—Configuration Management

Vendor:			Siemens	Subnet Solutions	SEL	Eaton	TDi Technologies	NovaTech
Product:	Configuration Management	Detail	CrossBow Secure Access Manager	Power System Center	SEL 3620	IED Management System (IMS)	ConsoleWorks	NovaTech Connection Manager (NCM)
	Ability to retrieve IED configuration		Yes	Yes	Yes	Yes	Yes	Yes
		Comm settings	Yes	Yes	Yes	Yes	Yes	Yes
		Device settings	Yes	Yes	Yes	Yes	Yes	Yes
		Security settings						
		Other						
	Feature: Comparison to baseline/approved version		Yes	Yes	Yes	Yes	Yes	Yes
		Generate alert regarding differences	Yes	Yes		Yes	Yes	
	Feature: reviewing/approving versions		Yes	Yes		Yes	Yes	
		Multiple (historical) versions stored	Yes	Yes		Yes	Yes	
		Feature: Workflow functionality	Yes	Yes		Yes	Yes	

Summary

The reviewed systems do a reasonable job of managing device configurations including retrieval and comparison. This is an important function for security and reliability. Generally, the hybrid or centralized systems are better suited to managing many device configuration files. Future capabilities should include the ability to automatically verify the correct configuration version without human intervention and the ability to retrieve and store the configuration change history with dates and names. As stated above, we may at some point also want to be able to safely and reliably upload configuration files once the necessary system capabilities are in place.

9
FIRMWARE MANAGEMENT

The management of device firmware including patch management is a capability for RDM systems that is growing in importance along with the recognition that managing firmware contributes to overall system reliability and security. Key aspects include the ability to retrieve the current IED firmware version number, determine if that is the latest version number from the supplier and generate an alert if the firmware version is not the latest. In the future this may also include uploading new firmware however the obvious risk must be mitigated by sophisticated device and system designs, and security.

Current State Assessment

The assessment of the current state of supplier offerings looked at firmware management support for RDM systems. A total of six supplier's RDM systems were reviewed. The result of this assessment is summarized in Table 9-1 and the narrative below:

1. **Identify existing IED firmware version**

   All six systems support retrieval of the current version number of the IED firmware.
2. **Identify latest IED firmware from vendor**

   It appears that only the NovaTech offerings can obtain and store this information.
3. **Generate alert if existing < latest version**

   None of the offerings support this.
4. **Apply new firmware version**

   None of the offerings support this. Implementing the uploading of new firmware carries obvious risk which must be mitigated by sophisticated device and system designs, and security.

Table 9-1
Current State Summary of Suppliers—Firmware Management

Vendor:			Siemens	Subnet Solutions	SEL	Eaton	TDi Technologies	NovaTech
Product:	Firmware Management	Detail	CrossBow Secure Access Manager	Power System Center	SEL 3620	IED Management System (IMS)	ConsoleWorks	NovaTech Connection Manager (NCM)
	Identify existing IED firmware version		Yes	Yes	Yes	Yes	Yes	Yes
	Identify latest IED firmware from vendor		No	No		No		Yes
	Generate alert if existing < latest version	Notification: Alert, Warning, Email.						
		Able to document and acknowledge alert, if upgrade is not planned.						
	Apply new firmware version	Directly vs. through vendor tool						
	Other? (Backup/Restore to earlier version)							

Summary

The reviewed systems, with one exception, are only capable of identifying the existing IED firmware version number. There is a lot more that needs to be done in this area as this is an important function for security and reliability. Generally, the hybrid or centralized systems are better suited to managing many device firmware files. Future capabilities should include the ability to automatically verify the correct firmware version without human intervention and store the firmware change history with dates. As stated above, we may at some point also want to be able to safely and reliably upload firmware files once the necessary system capabilities are in place.

10
PASSWORD MANAGEMENT

Traditionally IEDs had hard coded passwords that were rarely if ever changed. Default passwords were common across hundreds if not thousands of devices and may have be written on the faceplate of the device to speed up maintenance access. Modern password management includes a potentially large set of requirements when considering NERC CIP mandates, system integration with security applications, local storage, remote updating etc. The topic of password management can be broken into two categories:

- IED Password Management- which may include support for local and remote updates, automatic system wide password updates, device specific password policy, support for multiple passwords and levels per device, alerts when certain passwords are used such as default passwords and password checkout (each time a device is accessed). Operations during emergencies is an aspect that must be considered as well.
- User password management - which may include centralized password administration, individual user privileges, role-based access controls, and two-factor authentication.

The focus of this research and report is IED password management.

Current State Assessment

The assessment of the current state of supplier offerings looked at password management for RDM systems. A total of six supplier's RDM systems were reviewed. The result of this assessment is summarized in Table 10-1 and the narrative below:

1. **Supports multiple passwords/device**

   All six systems support multiple passwords per device.

   - **# of p/w supported per IED**

     Two of the six systems support up to eight password per device. It is not clear how many passwords the other suppliers support

   - **# of p/w: Fixed vs. User configurable?**

     It appears that the number of passwords is not configurable for the supplier's systems.

   - **(SEL) Support different p/w complexity by firmware version**

     Four of the six suppliers support a different password complexity for SEL firmware versions.

   - Manage pw on IED + Comm Proc/RTU devices

     Five of the six suppliers support passwords for IEDs as well as substation gateways, data concentrators and RTUs.

2. **Configurable IED password policy/rules**

   All six systems support configurable IED password policies and/or /rules.

3. **User alert when using default passwords**

   Only SEL supports alerting the user when a default password is used.

Table 10-1
Current State Summary of Suppliers – Password Management

Vendor:			Siemens	Subnet Solutions	SEL	Eaton	TDi Technologies	NovaTech
Product:	Firmware Management	Detail	CrossBow Secure Access Manager	Power System Center	SEL 3620	IED Management System (IMS)	ConsoleWorks	NovaTech Connection Manager (NCM)
	Identify existing IED firmware version		Yes	Yes	Yes	Yes	Yes	Yes
	Identify latest IED firmware from vendor		No	No		No		Yes
	Generate alert if existing < latest version	Notification: Alert, Warning, Email.						
		Able to document and acknowledge alert, if upgrade is not planned.						
	Apply new firmware version	Directly vs. through vendor tool						
	Other? (Backup/Restore to earlier version)							

Summary

The reviewed systems do a reasonable job of managing passwords based on the criteria for this report however based on a broader set of requirements, there is a lot more work to be done. Future requirements should include support for local and remote updates, automatic system wide password updates, support for multiple passwords and levels per device, alerts when certain passwords are used such as default passwords and password checkout (each time a device is accessed). Operations during emergencies is an aspect that must be considered as well.

11
CONCLUSIONS

The investigation into the current state of supplier offerings for RDM has produced some interesting results and identified a number of key areas where further research may be warranted in the future. Take-ways and learnings from this effort include:

- The preferred architecture is a hybrid which gives the most flexibility by allowing the utility to choose whether to install substation gateways. The only gap of note in terms of architecture is a lack of tiered architecture offerings however this is being addressed by the suppliers with their next generation systems.
- In terms of communications, one of the biggest challenges in implementing RDM for both the suppliers and the utilities is the proliferation of unique and vendor specific interfaces and methods in the IEDs. It is difficult to deploy the ideal RDM multi-vendor solution today because the full range of standards, IEDs, systems and methods to support such a solution does not exist today. In addition, many utilities do not have the communications infrastructure in place to enable the full RDM functionality that is possible.
- Asset Discovery is a practical capability. All the RDM systems evaluated support confirmation of connectivity over IP and serial. However, fewer systems support auto-discovery which is a very useful function but far more technically challenging. This capability assumes a way for a device to describe itself to the other components of the system either by the protocol or by prior configuration of a set of optional IED templates.
- Overall the evaluated systems provide a rudimentary capability in support of Asset Inventory management. Basic capabilities such as model number and firmware version numbers are captured but very little functionality beyond that is provided. It would be preferable for the systems to provide device health information. In addition, the RDM systems should be able to integrate with Asset Management systems such as Cascade, Maximo, SAP and other so the IED asset information can be maintained as part of the utility's overall asset management activity.
- The reviewed systems do a reasonable job of managing device configurations including retrieval and comparison. This is an important function for security and reliability. Generally, the hybrid or centralized systems are better suited to managing many device configuration files.
- Regarding firmware management, the reviewed systems, with one exception, are only capable of identifying the existing IED firmware version number. There is a lot more that needs to be done in this area as this is an important function for security and reliability. Generally, the hybrid or centralized systems are better suited to managing many device firmware files.

- The evaluated systems do a reasonable job of managing passwords based on the criteria for this report however based on a broader set of requirements, there is a lot more work to be done. Future requirements should include support for local and remote updates, automatic system wide password updates, support for multiple passwords and levels per device, alerts when certain passwords are used such as default passwords and password checkout (each time a device is accessed). Operations during emergencies is an aspect that must be considered as well.

Table 11-1
Summary of Assessments

Evaluation Category	Overall Assessment
Architecture Aspects	Fully supported
Communications	Partially supported
Asset Discovery	Partially supported
Asset Inventory	Partially supported
Configuration Management	Fully supported
Firmware Management	Minimally supported
Password Management	Partially supported

Summary Statement

Referring to Table 11-1 above, we can conclude that the supplier offerings for RDM partially support the evaluation categories that we addressed. While there has definitely been some good progress made by a few suppliers, much work remains to be done to reach the definition of an ideal RDM; to fully manage, update, secure, monitor and analyze all the remote IEDs of all types at all locations.

Next Steps:

Refer to the future research recommendations in Section 12.

12
FUTURE RESEARCH

As a result of the work in developing this report, it has become apparent that it would be beneficial to continue the research in the RDM area as follows:

1. Develop an updated detailed set of utility requirements for RDM.
2. Conduct a deeper investigation (and possible coordination with EPRI Cyber Security) into the cyber security aspects of RDM which includes a secure remote access capability.
3. Investigate expanded use of communications standards in lieu of vendor specific protocols.
4. Explore in greater detail, RDM capabilities in asset discovery and asset inventory.
5. Examine potential for new configuration and firmware management functions.
6. Assess the industry progress with password management and related functions.
7. Investigate the benefits and challenges associated with the integration RDM and other systems.
8. Develop an updated assessment of the state of the industry.
9. Consider investigating work-flow aspects related to RDM deployments.

13
REFERENCES

1. Guidance for Secure Interactive Remote Access, NERC, July 2011
2. Security architecture principles for digital systems in Electric Power Utilities, Cigre Report 615, April 2015
3. The IEC 61850 Smart Grid Device Management System to improve the Asset Management, Thierry Coste, EDF, PACWorld, September 2017
4. *Substation Security and Remote Access Implementation Strategies*, EPRI, Palo Alto, CA: 2014. 1024424
5. Vendor documentation (where publicly available)

Export Control Restrictions

Access to and use of this EPRI product is granted with the specific understanding and requirement that responsibility for ensuring full compliance with all applicable U.S. and foreign export laws and regulations is being undertaken by you and your company. This includes an obligation to ensure that any individual receiving access hereunder who is not a U.S. citizen or U.S. permanent resident is permitted access under applicable U.S. and foreign export laws and regulations.

In the event you are uncertain whether you or your company may lawfully obtain access to this EPRI product, you acknowledge that it is your obligation to consult with your company's legal counsel to determine whether this access is lawful. Although EPRI may make available on a case by case basis an informal assessment of the applicable U.S. export classification for specific EPRI products, you and your company acknowledge that this assessment is solely for informational purposes and not for reliance purposes.

Your obligations regarding U.S. export control requirements apply during and after you and your company's engagement with EPRI. To be clear, the obligations continue after your retirement or other departure from your company, and include any knowledge retained after gaining access to EPRI products.

You and your company understand and acknowledge your obligations to make a prompt report to EPRI and the appropriate authorities regarding any access to or use of this EPRI product hereunder that may be in violation of applicable U.S. or foreign export laws or regulations.

The Electric Power Research Institute, Inc. (EPRI, www.epri.com) conducts research and development relating to the generation, delivery and use of electricity for the benefit of the public. An independent, nonprofit organization, EPRI brings together its scientists and engineers as well as experts from academia and industry to help address challenges in electricity, including reliability, efficiency, affordability, health, safety and the environment. EPRI members represent 90% of the electric utility revenue in the United States with international participation in 35 countries. EPRI's principal offices and laboratories are located in Palo Alto, Calif.; Charlotte, N.C.; Knoxville, Tenn.; and Lenox, Mass.

Together…Shaping the Future of Electricity

3002012588

Electric Power Research Institute
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 • USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com