White Paper **WP913001EN** Effective March 2016

COOPER POWER SERIES

Managing intelligent electronic devices

As part of their Smart Grid initiatives, utilities have been deploying large numbers of Intelligent Electronic Devices (IEDs) to implement advanced automation systems. However, they are discovering the high cost of maintaining these devices. Originally considered as essentially capital intensive, projects in the electrical sector have seen increasing operational costs as utilities are faced with devices that require complex commissioning as well as regular firmware updates and security patches.

In the same manner, as operators of large vehicle fleets have implemented "Fleet Management" programs supported by advanced software, utilities must now look for automated solutions to manage their IED fleets in order to tackle the ever increasing operational expenses.

In this paper, we will discuss some of the basic functions required for managing large fleets of IEDs, the solutions that have been developed to help utilities meet North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) cybersecurity requirements, and how these solutions can also be applied to help utilities manage the IEDs being deployed in distribution automation systems.

Contents

Powering Business Worldwide

Adapting to today's technology

Power distribution systems, which are essentially static, are increasingly becoming "active" and perform advanced coordinated real-time functions such as Fault Location Isolation and Service Restoration (FLISR), real-time power network status reporting, VAR Management and Voltage Optimization and Control.

While this technological evolution leads to valuable benefits, it also brings important new operational challenges. Advanced automation systems are built out of large numbers of programmable electronic devices, coming from a variety of vendors. All of these devices are expected to interoperate and exchange data in a secure and reliable manner.

However, there has been a significant change in paradigm. Traditional OT (Operational Technology) systems were designed to be long lasting and made of simple technology, using simple protocols, with little or no security. Once operational, they were not expected to change.

On the contrary, modern automation systems are increasingly inheriting some of the characteristics of IT (Information Technology) systems:

- The systems are becoming much more dynamic with a much shorter life expectancy
- The devices are more complex and the firmware must be updated regularly in order to address:
  - security vulnerabilities
  - programming errors
  - simply to add new functions
- Devices need to be replaced as their components rapidly become obsolete and are no longer manufactured
- Each new generation of devices seems to implement new technologies and protocols

Change has thus become a fundamental characteristic of modern automation systems and must now be taken into account.

The true benefits of modern automation systems will only be achieved if the cost of managing devices can be brought under control.

Managing the device lifecycle

Large organizations have developed a significant body of knowledge, standards, and best practices in the management of large numbers of networked devices used for their business operations. Implementing and maintaining large business networks requires a team of IT specialists that use specialized asset management tools such as Network Management Systems to assist in their tasks. In many cases, all the networking technology and tools will be selected from a single vendor to ensure seamless integration and complete control of the device lifecycle, from the initial commissioning to its secure disposal. Modern devices can often obtain their configuration settings automatically from the Network Management System and become operational as soon as they are plugged in.

This approach is very different from the evolutionary path that automation systems have been following. Communications, interoperability, and security have generally been secondary considerations as engineers selected "best of breed" devices, from a variety of vendors, according to their functional capabilities. Commissioning a device requires numerous manual operations, often using a proprietary software tool connected to a serial maintenance port. Up until now, this was not an issue since the automation system was often deployed as part of a larger project, with very little changes expected or planned once it is commissioned.

But, the reality of new devices is such that these systems are no longer static and need to be maintained, devices updated, or simply replaced. As utilities extend their communication networks to integrate ever-increasing numbers of devices in new applications, it will no longer be cost-effective to manage the system manually and some form of automatic configuration is inevitable.

While vendors of networking devices and proponents of the Internet of Things (IoT) have been promoting a vision of plug-and-play devices and zero-touch deployment, the whole process of commissioning electrical controls such as protection relays, voltage regulators, recloser controls, and capacitor bank controls, from a variety of vendors, is much more complex and will remain so for the foreseeable future.

While there are efforts to extend standards such as DNP3 and IEC 61850 to include device properties and configuration settings, these have not yet been widely adopted by the industry. The task of managing devices used in automation systems thus requires specialized knowledge and experience that can only be expected from vendors in the electrical sector. Fortunately, as we will see in the next section, such applications are already available.

Managing devices inside the fence

The electrical substation is the host of a large number of IEDs, from a variety of vendors, used for protection, metering, monitoring, and communications. Utilities that operate transmission substations were the first to implement automated device management systems, originally to reduce operational costs, but also to help meet compliance requirements.

One of the first applications to be automated was the retrieval of power system event and fault data from Digital Fault Recorders (DFR), in order to meet NERC PRC reliability requirements. Many utilities thus chose to connect their substations and deploy automated event retrieval software to eliminate the high cost of having skilled technical personnel drive to the substation simply to manually retrieve event data.

Automated event retrieval was thus the first application of Eaton's IED Manager Suite (IMS) software, allowing utilities to:

- Handle faults in a timely manner
- Reduce operational costs
- Reduce the average duration of interruptions (SAIDI), a key performance metric used to set rates

Deploying TCP/IP networks to the substations and installing advanced data concentrators had the additional benefit of providing the capability to manage devices remotely, further reducing operational costs. However, providing remote access to devices also opened a potential security issue which was rapidly addressed by NERC.

Utilities that operate transmission substations have to comply with the NERC CIP standards and have to put policies and procedures in place to ensure the security of the devices used to implement critical functions in the Bulk Electric System (BES).

Complying with the NERC CIP standards involves much more than complying with technical requirements. Utilities have to providing evidence that their operational processes comply with the requirements. Managing lists of devices, firmware versions, users, access permissions, and passwords update history are all operations that can be much better handled by a device management software than manually through the use of spreadsheets.

For many utilities, the business case for automating device management has thus been the ability to reduce operational costs through secure remote access in addition to implementing tools to automate NERC CIP compliance. Device management software, such as Eaton's IMS, provides the "intermediate device" functionality required to meet the NERC CIP standards for remote access as well as the additional functions required to help utilities achieve compliance, such as:

- Centralised user management
- Integration with Microsoft Active Directory
- Security event logging and monitoring
- Hiding device passwords through automatic login

While most large utilities have deployed some type of asset management software at the enterprise level, these systems are typically static and the information must be entered manually. IT Network Management Software, also typically used by large utilities, has generally been unsuccessful in handling IEDs because of the lack of standard protocols to interrogate substation devices and programmatically extract information such as firmware versions, serial numbers, and device settings.

Device management software designed for the electrical sector, such as Eaton's IED Manager Suite, implement device drivers for all common devices used in the electrical sector and support the functions required for managing the device's lifecycle for CIP compliance.

For instance, the CIP-007-5 standard requires that utilities evaluate and deploy firmware updates and security patches in a timely manner, and be able to provide evidence to that effect.

Eaton's IMS Configuration Manager module:

- Retrieves device settings, firmware versions, and serial numbers, on demand, or on a scheduled basis
- Provides the capability to set a baseline version
- Detect changes and automatically notify system operators
- Generates all applicable compliance and operational reports

The IMS Password Module also helps in meeting password management requirements by providing the capability to automatically update devices with complex passwords in addition to maintaining a history of all passwords changes for a device.

Utilities that have deployed device management software to provide secure remote access and automate many of the most labor-intensive aspects of CIP are now reporting additional unexpected benefits. Because substation devices can be accessed securely, departmental silos are breaking up, leveraging the communications infrastructure to provide access to multiple departments that require substation data for a variety of applications such as power quality or device condition monitoring. The time and effort required during the investigation of outages and power restoration is reduced through improved access to devices and the capability to remotely change settings during emergencies and weather events.

Device management systems are thus providing proven benefits for the operators of transmission substations. In the next section we will discuss how the experience gained through the use of these systems can be applied to operators of large fleets of distribution automation devices.

Managing devices outside the fence

As we have discussed, the high cost of compliance to NERC standards provides a clear-cut business case for implementing automated management of substation devices. What is the business case for devices used as part of distribution automation systems?

While the transmission substation can be characterized by the large variety of different devices installed in a single location, distribution automation is characterized by the large number of identical devices deployed throughout a large geographical area. The operational challenges will thus be very different.

Experience gained while working with utilities that are deploying large fleets of distribution automation devices has provided us with a better understanding of the areas where operational costs are the most significant. Distribution automation devices are geographically dispersed, therefore remote management becomes a cost effective alternative to an expensive truck roll. Bulk settings and firmware updates are the most common operations that can be performed remotely.

As utilities deploy their distribution automation systems, they gain a better understanding of the operation of their electrical network and will often need to change device operational settings from the original values. While some setpoints are mapped to DNP3 data points, not every setting is available through SCADA or DMS, and some changes need to be performed using the device configuration tool. Providing remote maintenance access to the device will obviously be less costly than driving to the site. Furthermore, this is an obvious application for a device management application such as Eaton's IMS Update Manager that can automatically perform a requested update on a large number of devices in parallel, instead of having qualified technical personnel remotely log in to individual devices to change settings. With thousands of devices to update, these operations rapidly become tedious, error prone, and very time consuming.

As mentioned previously, firmware updates are the new reality in power system automation. As devices become more complex and perform more functions, they expose more programming errors and security vulnerabilities. While updating device settings is generally a short and straightforward operation, firmware updates require the transfer of larger data files and take much longer to perform with the communication speed provided by most distribution automation communication networks. Having qualified technical personnel sit in front of a maintenance tool watching a progress bar slowly creep forward is simply not a cost effective operation.

As a ballpark figure, imagine an operation that requires at least 30 minutes performed, on a thousand devices, at an hourly cost in the range of $100 per hour to appreciate the potential cost savings of having the operation performed automatically, with no operator intervention.

Firmware and setting updates are applications where the reality of distribution automation is very different than the realities of substation automation. Because of the criticality of substation devices, utilities generally prefer to be on site to perform operations such as firmware updates. Eaton has thus developed the IMS Update Manager module primarily to meet the requirements of distribution devices that are typically less critical and where it is simply not cost effective to perform updates manually.

Automating the process of keeping track of device configuration settings also makes sense from the perspective of operational best practices, even if it is not a compliance requirement. Therefore, Eaton's IMS Configuration Manager module can be a valuable engineering tool as it stores all device settings in a readily accessible database and can be used to ensure that devices are configured as expected.

Finally, most utilities will not consider managing device passwords as a very high priority for distribution devices. However, this will change in the future as it is expected that cybersecurity requirements will certainly extend to the distribution network.

Summary

The following table summarizes the business case for IED fleet management for transmission substations as well as for distribution networks.

Function	Substation automation	Distribution automation
Secure remote access • Centralized user management • Two-factor authentication • Access logs and reports • Hide device passwords through automatic login • Encrypted communications (IMS Passthrough Manager)	Required by NERC CIP Network routers and switches do not provide "intermediate device" functionality requested by NERC CIP	Not currently a requirement. Since most device have very little security and often share the same password, a secure remote access solution provides a means to control and manage remote access as a best practice.
Configuration management • Retrieve device configuration settings automatically • Store settings in a database • Detect changes and notify administrators • Maintain a baseline and keep track of device configuration history and firmware version and updates (IMS Configuration Manager)	Required by NERC CIP System operators must be able to provide reports demonstrating that firmware updates have been performed when required. System operators must define baseline settings, perform security testing, and be able to demonstrate that the system has not deviated from its baseline since it was tested. Can be done manually, but it is tedious.	Having a centralized database of all device settings is a valuable engineering tool for diagnosing issues and ensuring that devices are configured as expected.
Password management • Automatically generate complex passwords and update devices • Centralized management of device passwords (IMS Password Manager)	Required by NERC CIP Device passwords must be updated on a regular basis and evidence provided to that effect. Can be done manually, but is tedious and error prone.	Not currently a common practice. Most devices are still deployed with the default password, or with the same password for all devices, which may be a cybersecurity issue.
Event retrieval • Automatically retrieve fault data and oscillography from DFRs and protective relays • Store data in a centralized database and provide web access to protection engineers (IMS Event Manager)	Required by NERC PRC reliability standards. Can be done manually, but is tedious.	Not applicable.
Firmware and settings updates • Push settings to devices • Push new firmware versions to devices (IMS Update Manager)	Required by NERC CIP System operators must evaluate the applicability of firmware updates provided by vendors and apply them if deemed necessary. However, this operation is very difficult to automate due to the large variety of devices from multiple vendors. In addition, for many devices, firmware updates require a direct connection to the maintenance port.	Modern devices support "over the air" or remote updates. However, performing these operations manually is time consuming and tedious. With the large number of geographically dispersed devices, automating settings and firmware updates can significantly reduce operational costs.

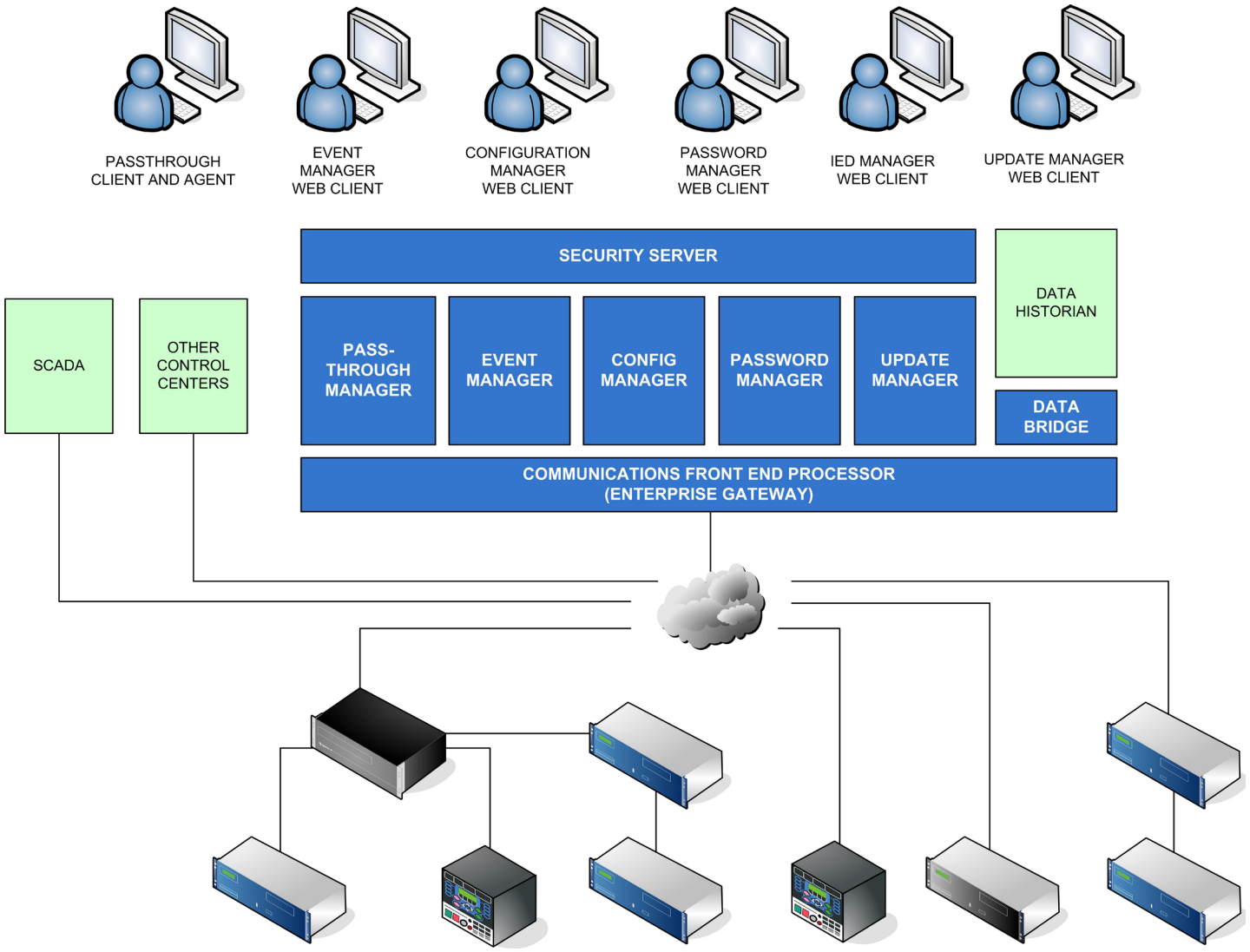

Figure 1. Eaton's IED manager suite modules

Conclusion

As we have seen, the business case for fleet management software for substation automation is very different than that for distribution automation.

The main drivers for automating at the substation level have been cybersecurity and compliance with the NERC CIP standards. To help utilities automate this aspect of their operations, Eaton has developed the IED Manager Suite software applications.

For the distribution network, the main drivers are the very large number of devices and their geographic dispersion. Eaton's IMS Update Manager will thus be a valuable tool to automate the process of updating device settings and firmwares, while the IMS Configuration Manager will help keep track of device configurations.

In both types of applications, utilities will benefit from the asset management capabilities and comprehensive reporting provided by Eaton's IED Manager Suite software.

Eaton
1000 Eaton Boulevard
Cleveland, OH 44122
United States
Eaton.com

Printed in USA
Publication No. WP913001EN
March 2016

Powering Business Worldwide