MANAGING THE BUILDING BLOCKS OF THE ACTIVE DISTRIBUTION SYSTEM

Jacques BENOIT
Eaton's Cooper Power Systems – Canada
jacquesbenoit@eaton.com

ABSTRACT

Visionary initiatives such as the Smart Grid and Active Distribution Systems promise to help us meet many of the energy and environmental challenges of the 21st century. Unthinkable just a decade ago, these initiatives have been made possible by the rapid technological evolution that has brought us low-cost communications, networking, and computing devices. However, all of these programmable devices, provided by a variety of vendors, are expected to interoperate and exchange data in a secure and reliable manner. While there exist standards to define how to exchange data, there is very little guidance available on managing the system as a whole, or the individual devices of which it is constituted.

In this paper the author will first review the device management requirements set forth in various standards and guidelines such as ANSI/ISA 62443 and NERC CIP, and discuss how configuration management is essential to the secure and reliable operation of automation systems. The paper will then discuss the challenges of managing devices from multiple sources and describe some of the efforts under way to meet these challenges.

INTRODUCTION

The evolving technological landscape made possible by relatively low-cost communications and ever more "intelligent" microprocessor-based devices has brought about a profound change in the nature of distribution systems. These systems, which were essentially static, can now perform advanced coordinated real-time functions. Enterprise-level or distributed systems can provide advanced functions such as Fault Location Isolation and Service Restoration (FLISR), monitoring systems can provide real-time network modelling software with data that can be used to perform VAR Management and Voltage Optimization and Control.

While this technological evolution will bring with it valuable benefits, it will also bring important new operational challenges. There are two types of building blocks used to put together the active distribution system: communication devices used to build the infrastructure and Intelligent Electronic Devices (IEDs) used to manage the electrical apparatus and implement the advanced functions. All of these programmable devices, provided by a variety of vendors, will be expected to interoperate and exchange data in a secure and reliable manner. The sum of all these interconnected intelligent systems will constitute one of the most complex engineering works ever implemented.

To make matters even more difficult, the rate at which technology is evolving brings with it another important paradigm shift. Traditional OT (Operational Technology) systems were designed to be long lasting and made of simple technology using very simple protocols. Once put into operation, they were not expected to change. On the other hand, modern automation systems have inherited some of the characteristics of IT (Information Technology) systems, being much more dynamic and having much shorter life expectancy. There are many reasons for this. The devices are more complex and the firmware needs to be updated regularly in order to address security vulnerabilities, programming errors, or simply to add new functions. Devices need to be replaced as their components rapidly become obsolete and can no longer be manufactured. Each new generation of device seems to implement new protocols and comply with new standards. Change has thus become a fundamental characteristic of modern automation systems and must now be taken into account.

System operators are not well equipped to face the technical and organizational-level challenges of managing change. While there exist standards to define how to exchange data, there is very little guidance available on managing the system as a whole, or the individual devices of which it is constituted. The traditional tools and practices of the IT industry are not directly applicable to OT. Stopping systems on a monthly basis to push software updates, a common practice in IT, is inconceivable in OT systems where high availability is the norm. New tools, processes, and standards will need to be developed to manage these devices. These tools will implement functions such as keeping track of device settings and installed firmware versions, updating firmware, managing passwords, encryption keys, and digital certificates for the large variety of devices that will form the active distribution system.

SYSTEM MANAGEMENT REQUIREMENTS

Interestingly, the best guidance on system management can often be found in security standards. This should not come as a surprise as from an engineering perspective, security should be considered as a property of a system, in the same manner as reliability and safety. To quote the authors of the IEC 62351 standards (IEC 62351-7 p. 7), *"Although some definitions of "security" just include the protection of systems against the deliberate attacks of terrorists or cyber hackers, often more damage is done by carelessness, equipment failures and*

natural disasters than by those deliberate attacks."

The International Society of Automation (ISA) has been developing a family of security standards for the process control industry. Valuable system management guidance can be found in ANSI/ISA-62443-2-1 (99.02.01)-2009 which defines basic requirements for ensuring the reliable operation of systems, including configuration management.

With the same objectives of ensuring the reliable operation of the Bulk Electric System, the North American Electric Reliability Corporation (NERC) has recently released version 5 of the Critical Infrastructure Protection (CIP) standards. All the configuration management requirements have now been grouped in the new CIP-010-1 standard.

The standard recognizes that systems change. They thus require that system operators validate the security and reliability of the original design as well as any change to the system.

The CIP-010-1 standard sets forth the following requirements:

- Develop a baseline configuration
- Authorize and document changes that deviate from the existing baseline configuration.
- Prior to a change, determine if the change could impact the required cyber security controls.
- Following the change, verify that the cyber security controls were not adversely affected.
- Monitor for changes to the baseline configuration. Document and investigate detected unauthorized changes.

Obviously, meeting these requirements will require some form of automated system management process. In the following sections we will define what type of data we will need to manage, the processes that will need to be implemented, and the applicable standards, if any.

MANAGING THE SYSTEM CONFIGURATION

The configuration of a system is essentially defined as the totality of all the data, parameters and settings that are necessary to implement the system in an operational state. The goal of the configuration management standards and guidelines is to ensure that once the system is operational and has been tested as being secure, any change is documented and tested to preserve the integrity and security of the system through a formal auditable process. Additionally, any change should be detected automatically and addressed.

The following are some of the elements that need to be taken into account:

- Network topology and device configuration settings: device inventory, IP addresses, routes, servers, etc.
- Network security: X.509 certificates and encryption keys, etc.
- Application specific device settings: protective relays, voltage regulators, capacitor bank controllers, communications devices, etc.
- Firmware versions
- User authentication: device local accounts, etc.
- User authorization: user permissions, groups, local device permissions, etc.
- Monitoring: device and communications status, device event logs, etc.

Let us now discuss the challenges of managing this type of information.

SETTING UP THE NETWORK

One of the key enabling factors of modern automation systems has been the introduction of a communications infrastructure based on the TCP/IP networking model. Vendors of networking technology have thus rapidly positioned themselves to offer their networking expertise in building the Smart Grid. The breadth of standards and the best practices developed in IT systems can certainly provide numerous benefits to designers of automation systems. However, IT and OT systems are different in many ways.

Large organizations have developed a significant body of knowledge and best practices in the deployment of large numbers of networked devices. Most of us take for granted the operation of these systems. One can plug an enterprise-issued laptop computer in a connector in any enterprise location and it will automatically acquire all of its network configuration and have access to email and printers. Unplug the computer from the wall connector and it may even automatically connect to the wireless network. This functionality is based on a sophisticated infrastructure with servers that implement standards-based networking services. When a computer is connected to the network, it will request its network settings from a DHCP server. It may also be authenticated by an X.509 certificate that was issued by a certificate server. Once part of the network, it may refer to an internal DNS server to obtain the addresses of the services that it requires such as printers, file servers, and email servers. Implementing and maintaining such a network requires a team of IT specialists that use specialized tools such as Network Management Systems to assist in their tasks. In many cases, all the networking technology and tools will have been selected from a single vendor to ensure seamless integration.

This approach is very different from the evolutionary path that automation devices have been following. Legacy devices used in utility automation systems had limited communications capabilities based on serial communications and point-to-point communications. Gradually, vendors started adding networking

capabilities to their devices. Communications settings such as IP addresses are generally static and set manually through a front panel user interface, or through a configuration application connected to a serial maintenance port. The allocation of IP addresses has generally been under the responsibility of the engineers designing the automation system. This has not been an issue since the automation system was most probably planned out using traditional engineering drawings, with direct wired connections logically replaced by network connections.

As utilities extend their communications networks to integrate ever increasing numbers of devices in new applications, it will no longer be cost-effective to manage the network manually and some form of automatic configuration is inevitable. Network vendors have been promoting a standards-based vision of plug-and-play devices and zero-touch deployment. With these technologies, a technician simply connects a field device and it configures itself automatically. While it may be possible to automatically configure network devices from a single vendor, the whole process of commissioning electrical controls such as voltage regulators, recloser controls, and capacitor bank controls, will always remain application specific. We cannot expect network vendors to support these devices. New applications will need to be developed to configure the complete device, not just the network part. This will require more sophisticated devices and the processing power required to implement such solutions will have to be taken into account. Typical distribution automation devices need to be very low cost because of the large numbers being deployed.

AUTOMATING DEVICE CONFIGURATION MANAGEMENT

As we mentioned in the previous section, the TCP/IP suite defines a large number of standards that can be used to automate some aspects of configuring a device's network connection. However, this is not sufficient to fully commission a device. It will also be necessary to provision the device with local security accounts, up-to-date firmware, and application specific parameters and settings. While there is still no well-defined standard for managing a device configuration, a working group has been exploring some promising solutions. The NETCONF Working Group recently posted an Internet Engineering Task Force (IETF) draft that describes a zero touch provisioning approach for devices. The goal of NETCONF zero touch is to reduce the cost of deployment by reducing the technical expertise required to put a device in service.

NETCONF is a network management protocol that was developed by vendors of networking devices. It provides a transactional method for reading and writing a device's configuration settings in the form of XML data over a secure transport mechanism. When a NETCONF zero touch device boots from its factory configuration, it tries to locate an associated "ConfigLet" that it will use to establish a secure connection to a configuration server that will then provide it with its settings. This approach could be used to make any type of device self-configuring.

READING AND WRITING DEVICE CONFIGURATIONS

As we previously established while defining the requirements, the configuration management system must be able to establish a baseline configuration, track changes to the configuration, and automatically detect any discrepancy between the operational configuration of a device and its baseline settings.

What may seem a simple operation becomes quite challenging considering that typical devices lack the basic functions necessary to programmatically manage their settings. For instance, very few devices provide the capability of reading their settings as a single object or file that can be stored, processed, and displayed. Many vendors have used an interactive command-line approach where settings can be changed one at a time, or printed out per groups, using a terminal application connected to a maintenance port. Special device-specific scripting or programming is required to retrieve the device settings. Alternatively, some vendors have developed configuration tools that read and write values using a protocol such as MODBUS, DNP3, or a proprietary approach. These approaches can make it even more difficult to retrieve settings as the proprietary interfaces are rarely documented.

Some information can be retrieved from the IEC 61850 Substation Configuration Language (SCL) file and its subsets. These files are used to represent a device's properties, including its network connection and topology. However, the goal of the standard is to define the logical role played by the device in the substation and not to define its configuration settings. The device's application specific settings will thus not be found in these files.

To the author's knowledge, the NETCONF standard, which we described in the previous section, seems to remain the most promising approach to providing a standard format for exchanging configuration settings between a device and a configuration management system. In the meantime, vendors of configuration management applications will remain challenged in supporting devices from multiple vendors.

AUTHENTICATION AND AUTHORIZATION

Authentication and authorization are key operational functionalities that should also be considered as elements of the device configuration. One of the most frequent security vulnerabilities is the availability of factory user accounts. Unless these default accounts are disabled or their passwords changed, they provide a very effective backdoor through which a user can

disrupt the reliable operation of a system, even without malicious intent.

IT systems use dedicated servers to authenticate users and grant access permissions. Systems such as Microsoft Active Directory, RADIUS servers, and the LDAP protocol are all part of the IT authentication strategy. These all share the same basic approach: users that need to connect to a computer provide their credentials to the computer which then queries the authentication server about the users' access permissions. If the authentication server is unreachable, the computer will use permissions that it has cached from a previous session. While this approach is a valid strategy for IT systems based on high-availability LAN networks, it is not as well suited for OT systems. Field devices may use very slow networks making the authentication round trip too slow or impractical. Also, a solution will need to be provided for local access to the device for maintenance or when the network is unavailable.

If field devices implement local access passwords, it will then be necessary to provide each device with a unique password and implement a password management solution. This is another aspect of device management that is challenged by the lack of standards. The most promising approach to managing local access to devices may well be the use of X.509 certificates. As part of the requirements we have briefly mentioned the need for secure communications. While it may not always be necessary to encrypt communications, it will be necessary to at least provide authentication mechanisms to ensure the authenticity of the application issuing control functions and the devices participating in the network. Technologies such as IPsec VPNs, TLS secures communications, and even DNP3 Secure Authentication, all use X.509 certificates to ensure the authenticity of end points. An X.509 certificate can also be used to authenticate a field technician and would alleviate the need for device level accounts and passwords.

MONITORING DEVICES

An Active Distribution System will be very complex engineering systems composed of thousands of devices working together. A fundamental requirement is thus to ensure that all parts are working correctly, or at least provide system operators with a correct image of the availability of its individual components. Once again we can refer to IT systems for guidance. Network Management Systems typically use SNMP to monitor the correct operation of network components such as switches and routers. The IEC 62351-7 standard has defined Management Information Bases (MIB) that can be used to report the state of a device or system. Besides the usual communications status, the standard also defines values to be used to monitor the integrity and security of the system by reporting attacks and physical breaches.

Another mechanism widely used in IT to monitor correct system operation is the syslog protocol. This provides a standard means for a computer or device to publish its logs to a centralized log collector where it can then be processed by a Security Information and Event Management (SIEM) system to produce reports and raise alarms on abnormal conditions.

Again, the challenge will be to implement these functionalities in low cost devices that use low speed networks or report-by-exception communications.

CONCLUSION

In this paper we have discussed the fundamental requirements for managing the devices used to implement the Smart Grid and Active Distribution Systems. We have identified a number of standards that are currently used to meet these requirements in IT systems and have discussed their applicability to OT systems.

The main roadblock that we can envision is the complexity of implementing these technologies at the individual device level. Vendors of networking devices have invested considerable efforts in developing solutions to implement large scale systems composed of numerous connected devices. Their efforts have provided us with advanced communications technology, standards and best practices. On the other hand, vendors of devices used to automate the electrical network have focused their efforts at the application level. The design goal has been to provide electrical functionality at a very low cost. Networking and management capabilities have generally been very low priority functions.

Building an Active Distribution System will thus be a challenging undertaking. The level of sophistication of solutions in the IT space have created very high expectations that will be difficult to meet with today's low-cost field devices. Until appropriate standards and practices are established, device management systems will remain difficult to implement and will have to take into account a large variety of vendor-specific approaches.

REFERENCES

[1] International Electrotechnical Commission, 2010, *IEC/TS 62351-7. Power systems management and associated information exchange – Data and communications security – Part 7: Network and system management (NSM) data object models.*

[2] International Society of Automation, 2009, *ANSI/ISA-62443-2-1 (99.02.01)-2009 Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program.*

[3] Jacques Benoit, 2012, "Defining Cyber Security

Requirements for Distribution Automation", *Proceedings Western Power Delivery and Automation Conference*

[4] K. Watsen, S. Hanna, J. Clarke, M. Abrahamsson, 2014, "Zero Touch Provisioning for NETCONF Call Home (ZeroTouch)", Internet Engineering Task Force, Draft.

[5] North American Electric Reliability Corporation, 2013, *CIP-010-1. Cyber Security — Configuration Change Management and Vulnerability Assessments.*