21, rue d'Artois, F-75008 PARIS
http : //www.cigre.org

CIGRE US National Committee
2022 Grid of the Future Symposium

Grid Automation System Device Management and Cybersecurity

A.H. HAMDON, A.C. WEST
SUBNET Solutions, Inc.
Canada

SUMMARY

Power grid automation systems typically integrate a diverse range of different makes and models of devices, each of which has been designed to perform some task effectively or economically.

Many of these automation devices provide real-time data (usually via standard protocols) for the operation of the system, typically via a SCADA, EMS or ADMS system. In addition to the operational data, devices typically host other data such as asset management data; engineering management data; configuration data; fault records; etc. This data is often accessed in proprietary formats, and this is especially true for engineering access and configuration data.

Staff who access the non-operational data are typically required to learn the use of each device vendor's tools and to know device passwords and information such as network addresses and access paths to connect to the devices and access data.

Regulations and good cybersecurity practice require that all data access to all devices is managed in a secure manner to ensure the integrity of information and to prevent access or manipulation of data and devices by personnel not authorized to perform those tasks.

This paper describes requirements and a design philosophy for an integrated device management process to provide each user with access to all data in all different kinds of devices through a single interface, while controlling what each user is permitted to access (attribute-based access control), hiding device details that the user does not need to manage and preventing inadvertent (or deliberate) device operation or data alteration by staff who do not have authority to perform those tasks. The integrated system can provide a single interface for management of additional cybersecurity functionality such as automated device password management, automation of periodic or automatic data collection processes (e.g. automatic retrieval of fault records or asset data from devices). The system can also automatically verify the status and versions of firmware and configurations in use, ensuring that only approved

Hamdon@SUBNET.com

code and configurations are operating. Unauthorized changes can be identified, alerted and automatically reverted to approved versions, if desired. All access, user actions, automated tasks (such as background version checking) and changes to the system are tracked in audit logs that assist verification of system integrity and cybersecurity.

Centralized device management opens scope for integration of additional features such as version management of software, configurations and device documentation. It facilitates new operational workflows for the creation, approval, deployment and automatic verification of configurations. Centralized access management to all devices through a single interface lowers training requirements for most users. Centralized user access management and device password management simplifies the process of granting role-based access to users. Fine-grained attribute-based access controls permit tight control of user permissions, going beyond coarser management of permitting who can connect to what devices. By enabling secure access to multiple sets of data for multiple purposes, new corporate applications can be envisaged, allowing system operation with improved efficiently and reliability.

KEYWORDS

Cybersecurity, Device management, Attribute-based access control.

1. Control System Overview

Modern grid automation systems provide a wide range of functions and integrate many subsystems that were initially developed independently.

Some aspects of the automation system involve operational (SCADA) data that is transmitted in near-real-time to control room operators, allowing them to manage the system. This operational data typically uses standard SCADA and automation protocols such as IEC 6070-5-101/-104 or IEEE 1815 (DNP3). Data within modern substations is often communicated using the models and protocols specified in IEC 61850. The adoption of these standards generally simplifies integration of equipment from different vendors and allows the end-user a wide selection of equipment types that may be integrated into the control system.

In addition to operational data, many control systems also include equipment that may produce or make use of non-operational data such as maintenance diagnostics; asset management information; fault records; historian information; configuration data; settings, etc.

As regulations and other business drivers evolve over time, systems are revised with new functions being added and new devices integrated into the system to support those functions. Examples may include changing priority of timely service restoration after a fault due to changing regulatory penalties or the introduction of condition monitoring as part of a change to reduce costs by migrating from periodic maintenance to condition-based maintenance. In the majority of systems, the diversity of functions and equipment types continues to grow over the life of the system and new stakeholders come into contact with the system.

There are now many applications or functions in use in the power grid, such as SCADA (real-time operations); EMS / DMS / ADMS; System monitoring and diagnostics; Protection and fault analysis; Asset management; Historian; System engineering and maintenance; Configuration management; Planning / system design, etc. New applications such as integration of renewables, DERMS and Phasor Measurement Unit data continue to expand the range of functionality included. Some of these applications are managed individually and have evolved processes and protocols in isolation. This independent evolution means that the various subsystems often do not make allowance for integrating data or functionality with other subsystems.

In some cases, the non-operational data is collected through the same SCADA mechanisms as the real-time operational data and is then distributed from the SCADA control centre to other corporate applications. In other cases, non-operational data is collected during site visits by maintenance staff or through alternate paths such as direct connection to corporate applications.

It is increasingly common to interconnect substation and distribution automation equipment to a wide-area network that allows communication between the field devices and the SCADA control room and also to various corporate applications. A typical arrangement of such communication may appear as shown in Figure 1, which shows automation devices in substations or distributed across the distribution network; devices serving other functions such as condition monitoring; the real-time operational control rooms for SCADA and ADMS and interconnection to the corporate network and applications such as Outage Management Systems, Graphical Information Systems, Historians, Asset Management Systems, Fault Analysis Systems, Settings Management Systems, Engineering Systems, Cybersecurity Monitoring Systems, etc. Many utilities have or plan to have these functions and subsystems integrated in order to improve workforce productivity or system reliability.

While the sharing of operational data is now well standardized, one of the issues that remains difficult to address for the integration of other data is the diversity of protocols and interfaces that are used. There is standardization in some areas, such as the widespread use of COMTRADE format for

protection fault records. But, in most other cases, protocols and interfaces are largely proprietary, and this is especially true for device-level engineering access and configuration management.

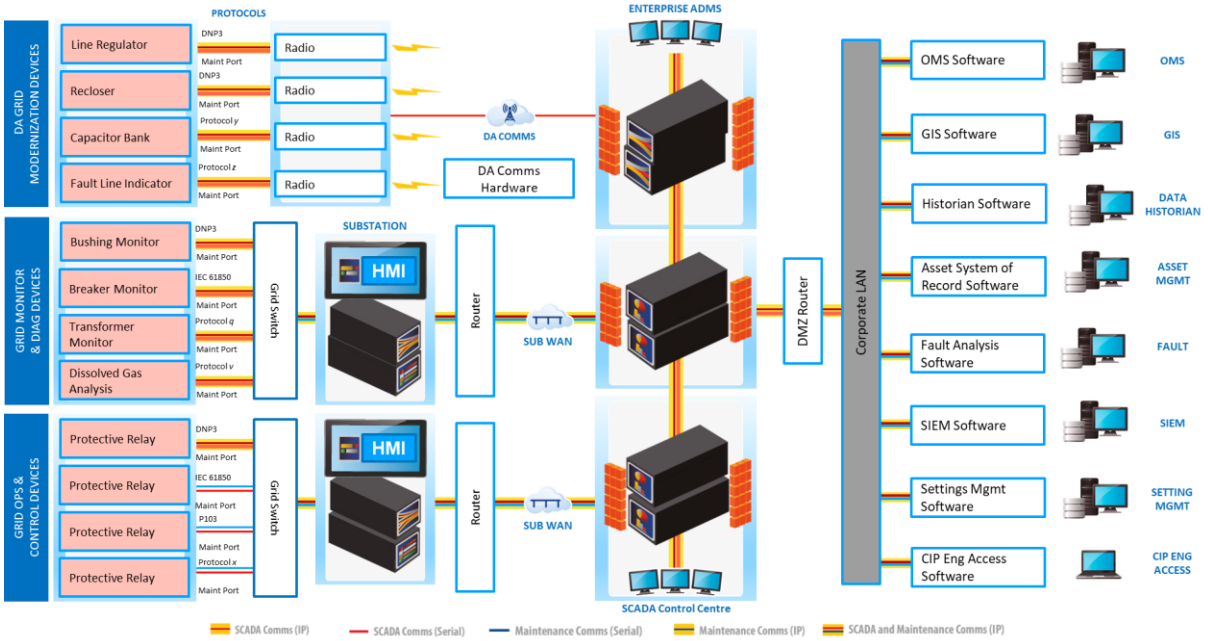

Figure 1-Typical Electric Utility Communication Architecture

2. Cybersecurity

When interconnecting systems in this manner, due consideration needs to be given to cybersecurity and the management of access to all devices by each application and each user. In some jurisdictions, cybersecurity requirements are regulated. Even where this is not mandated, prudent consideration of risk mitigation should lead to adoption of good cybersecurity design practices.

Multiple applications may make use of data from a device and each application may have legitimate business need to access data that might have previously been considered to "belong" to other subsystems. It is no longer sufficient to restrict data access on a simple role basis such as requiring that an asset monitoring application can only access dedicated asset monitoring equipment. Instead, a more refined methodology such as attribute-based-access-control (ABAC) may be employed, which controls not only which applications or users can access which devices or subsystems; but also manages what specific data within those devices or systems may be viewed and what may be modified. For example: A maintenance technician may be permitted to view and modify the configuration settings in a protection relay, but should not be able to operate the relay to trip a circuit breaker.

Such restrictions could be established by policies, procedures and training, but these may be overcome inadvertently by human error or by malicious action. A more secure approach is to enforce the policy by technical means that does not permit an unauthorized user to view or modify any aspect of a device that is not within their job role. In a similar way, technical controls can be put in place to shield the user from needing knowledge about the system or devices that they do not require in order to perform their job. An example of this might be to hide equipment IP addresses and access credential information such as passwords. A user who is authorized to interact with a device could be automatically logged into the device when needed without having to enter addressing information or passwords.

A well-engineered cybersecurity system can simplify the user's work by relieving them of the need to manage a wide range of vendor applications needed to access the same kind of information from different device types and to manage login details ad credentials for a large number of devices. Simplifying the worker's task encourages them to work within the guidelines imposed by the system.

Recent grid-specific cyber-attacks such as the Industroyer malware from December 2016 reported by Cherepanov [1] demonstrate that attackers are sophisticated and have deep domain knowledge of the electricity grid and the automation equipment used to operate it. A comparable level of sophistication is now required by utilities to help safeguard their assets. A zero-trust architectural model may be one approach that should be considered: Verify and authenticate all connections and users at all levels of the system. Useful guidance and communication architecture examples are provided in NIST Special Publication 800-82 [2].

3. Control System Planning

System expansion is often triggered by operational needs. Some stakeholders who could make use of the data available in a device might only become aware of the existence of equipment after it is commissioned. Retrospectively providing data access to the device for those users will typically be more expensive and less functional that would be the case if their needs were considered prior to installation.

Integration of data from multiple devices and systems for multiple users needs careful consideration. There are many stakeholders who could use system data if it can be made available to them in a secure manner. If the needs of all stakeholders can be considered early in system design, this may lead to improved utilization of data and new efficiencies at a lower cost than adding access to new applications later in the system life.

Throughout the planning and architectural design phases, close cooperation with the corporate IT department can help in the planning of a secure network architecture. Cybersecurity policies appropriate to the operational environment need to be developed and implemented. This will include suitable training for all users and regular review. All procedures, especially incident response and disaster recovery procedures should also be rehearsed and periodic exercises used to reinforce readiness. Exercising disaster recovery plans also verifies that the plans are current and that technical resources such as backups are viable. It is better to find this out in a drill than in response to an actual incident.

Any project to extend the automation system should be taken as an opportunity to review all uses of data available in the new extensions and all requirements to access the new extensions for engineering management of those extensions. Modern utility automation equipment has a wide range of data available, extending beyond that traditionally used for operational purposes. Providing appropriately secured access to that information can enhance the capability and efficiency of the utility divisions that make use of that information. Throughout this process, the cybersecurity aspects of access management need to be included in all considerations.

A data management platform to provide these services needs to understand both the operational and non-operational interfaces used by a wide range of devices, to provide that data to authorized users and to enforce appropriate attribute-based access controls that ensure easy access for authorized users while preserving the integrity of data and keeping confidential information that users do not require, especially access login and addressing information.

CONCLUSION

Modern electric grid control systems bring together a diverse range of equipment and integrate data from multiple sources. Many different applications can be enhanced if they can access data from a wide subset of the intelligent control devices in the network.

Integration of real-time operational data is simplified by the wide adoption of standard protocols. Integration of many other kinds of data, especially access for remote engineering and maintenance of devices, remains largely proprietary.

Across all data access, it is necessary to implement strong attribute-based access controls to ensure that the right data can be accessed by the right users and applications and to protect the system from increasingly-sophisticated cyber threats.

BIBLIOGRAPHY

[1] Anton Cherepanov, WIN32/Industroyer A new threat for industrial control systems [ESET, 2017, http://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf]

[2] National Institute of Standards and Technology: Special Publication (NIST SP) - 800-82 Rev 2 Guide to Industrial Control Systems (ICS) Security, [NIST, Gaithersburg, USA, 2015]