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

CIGRE US National Committee
2021 Grid of the Future Symposium

All in this Together: Integrating Data across Disciplines and Functions

A.C. WEST
SUBNET Solutions Pty Ltd
Australia

SUMMARY

The integration of new technologies is an on-going element of Grid Modernization. New technologies receive intense focus, sometimes at the expense of emphasis or awareness in other areas.

Grid automation is an inherently complex task, bringing together many specializations. Utilities have evolved internal organizational structures that recognize and support the multi-disciplinary approach needed for successful automation implementation. IEC 61850 and disruptive Internet of Things (IoT) technologies present new paradigms that can challenge these traditional structures: Adoption of such technologies may best be supported by refactoring traditional workflows. In such restructuring, emphasis is often placed on addressing new requirements and integrating new methods of engineering systems. In doing so, it is easy to overlook on-going needs of existing systems and functions or to neglect to take the opportunity to review whole-of-life information management of the system. For some systems, additional design effort can yield dividends in additional functionality or reduced operational expense.

Many functions interact with grid automation systems: Planning, architecture/design, configuration, commissioning, testing, operation, protection, maintenance, asset management, etc., with overarching requirements such as cybersecurity and corporate policy objectives.

An integrated, holistic approach to data access for operational and corporate purposes that integrates strong cybersecurity and role-based access for each user can enable operational efficiencies and lead to greater system resilience.

This paper serves to remind the reader to implement a multi-disciplinary approach to consider all information uses associated with a system, not only to manage the design, test and commissioning process; but also, to facilitate on-going system operation and support of information for non-operational functions.

KEYWORDS

Cybersecurity, grid automation, grid modernization.

Andrew.West@SUBNET.com

Introduction

The evolution of the grid, the development and inclusion of new control devices and the foreseeable integration of IoT devices each expand the amount and diversity of information used in grid management.

Recent introductions such as IEC 61850 and Phasor Measurement Units are examples of new technologies which provide new operational data, but which also depend on specific functionalities of the associated communications and configuration management systems.

New sources of data can enable new applications such as system stability analysis from phasor measurements or allow new business practices such as performing maintenance based on asset monitoring instead of on a periodic basis.

Business drivers

Many utilities have organizational structures that have separate responsible entities for functions such as power system planning, control system design, protection, communication, system engineering (configuration, testing and maintenance), operations, asset management, disturbance analysis, etc. These separate areas of responsibility and their operating procedures have evolved with the evolution of the grid. IEC 61850 integrates aspects of several of these areas of responsibility. Some utilities have found that adoption of these new technologies can stimulate or even mandate organizational restructuring in order to coordinate the engineering and operation of the new systems. Sometimes new multi-disciplinary teams need to be formed, bringing expertise from separate areas together.

The adoption of new technologies and standards typically provides value in terms of offering additional functionality coupled with manageable additional engineering to achieve that functionality. The adoption of new technologies does not replace the need to properly engineer system design, however, they may provide tools to simplify that task or parts of it. The framework provided by complex standards provide for consistent and interoperable interpretations of data, commands and configuration information. Without such common frameworks, the implementation of complex functions would require additional engineering and expense.

Electric utility automation systems are typically an integration of multiple subsystems (e.g. substation automation, SCADA, asset management, distribution automation, etc.). Traditionally, each of these systems have been managed by a separate responsible entity. While they each may have been operated more-or-less independently, there are synergies between them that make information sharing between systems beneficial. In many cases, specific integrations are performed to allow data sharing between subsystems in order to provide functional benefits to the utility. It is extremely unusual that all subsystems are updated at the same time, therefore the interaction between those subsystems needs to be considered whenever upgrading one of them.

Design considerations

When integrating new technology or new functionality, the impacts of that technology or functionality on other aspects of the utility business need to be considered, so as to ensure that all services and support needed by the new technology (e.g. communication system updates, additional staff training, etc.) are also incorporated as part of the project.

Further benefit may also be derived if it is feasible to also integrate the new technology with other stakeholder use cases. For example: The provision of enhanced communication services may permit access to additional data for other purposes such as asset health monitoring, remote device access for engineering and maintenance, etc. If the needs of all utility divisions are considered as part of any project, the overall capability and efficiency of the utility may be enhanced by using the opportunity to also integrate support for the various data use cases of each group of users. At a minimum, any new

automation project should consider on-going system operation and management needs as part of the design process. This may consider aspects such as

- on-going self-monitoring and testing
- access for maintenance functions
- data retrieval for fault analysis
- support for automatic or remotely-operated testing
- cybersecurity objectives and/or compliance

Architectural considerations

The provision of data for a diversity of applications moves the utility from a traditional model where communication access to the automation system is only provided for operational purposes (usually to a SCADA Control Centre) to a model where multiple users are provided access to a much wider range of data. In this migration, the system becomes exposed to a wider range of people and the need to manage and control that access also changes. The utility's cybersecurity policies may need review to ensure that they are applicable to the various kinds of access and new policies and procedures may need to be implemented. In most cases, this needs involvement of the utility IT group, the operational system design team, the maintenance engineering team and other stakeholders. Each category of user may need specific access to different kinds of data that become available from the automation system, and should be protected from inadvertently (or deliberately) accessing or changing information that they do not require or do not have a need to manage. In general, a system that supports role-based-access will typically be needed to meet cybersecurity policy objectives.

The need to ensure isolation of the automation system equipment from the corporate IT network (and, beyond that, the public internet), while also allowing controlled access to data from various users will typically lead to a review of the communication system architecture requirements. Guidance on this is available from various sources, e.g.: NIST SP-800-82 [1]. When controlling access into an operational automation device network, it is usually appropriate to use architectures that conform to a "Zones and Conduits" model as described in IEC 62443 [2] where data between a less trusted network (the "Enterprise Zone") and a more trusted network (the automation system zones) is only permitted through controlled paths (the conduits) and is monitored and managed to ensure that only permitted traffic passes between zones. Each utility should make its own determination regarding such architectural analysis and how its cybersecurity policies can be implemented while also providing the functionality required to perform the required functions. In general, zones are firewalled from each other and care should be taken to avoid simply opening "holes" through the firewall for automation system traffic: More sophisticated architectures with demilitarized zones and jump servers are typically required that do not permit direct access from one zone to another.

When the various kinds of substation and distribution devices are included, together with the various communication systems used to access those sites and the integration with data collected for various operational and non-operational purpose is directed to the users who have responsibility for that information, an architecture might result such as that shown in Figure 1. Different kinds of data will typically use different protocols: Operational data might use IEEE 1815 (DNP3) or IEC 61850; fault records might be collected as COMTRADE files; maintenance engineering will usually use a proprietary vendor protocol. The integrated system is responsible for ensuring that each user is provided access to the information required to perform their role and to isolate that data from any impact caused by other users or functions.

Cybersecurity regulations for electric utilities vary from jurisdiction to jurisdiction. In North America, the NERC CIP standards dictate particular requirements for the automation system and policies and procedures for staff. The European NIS Directive identifies a different approach that a utility may be required to adopt and focus more on monitoring of the control system to enterprise interface for malicious activity. There is merit in each approach and they may be considered to complement each other. Implementing a utility's own internal cybersecurity policies may require compliance to local

regulations as well as and additional cybersecurity controls. Cybersecurity can require system-level design and implementation considerations. This itself can require a multi-disciplinary approach.

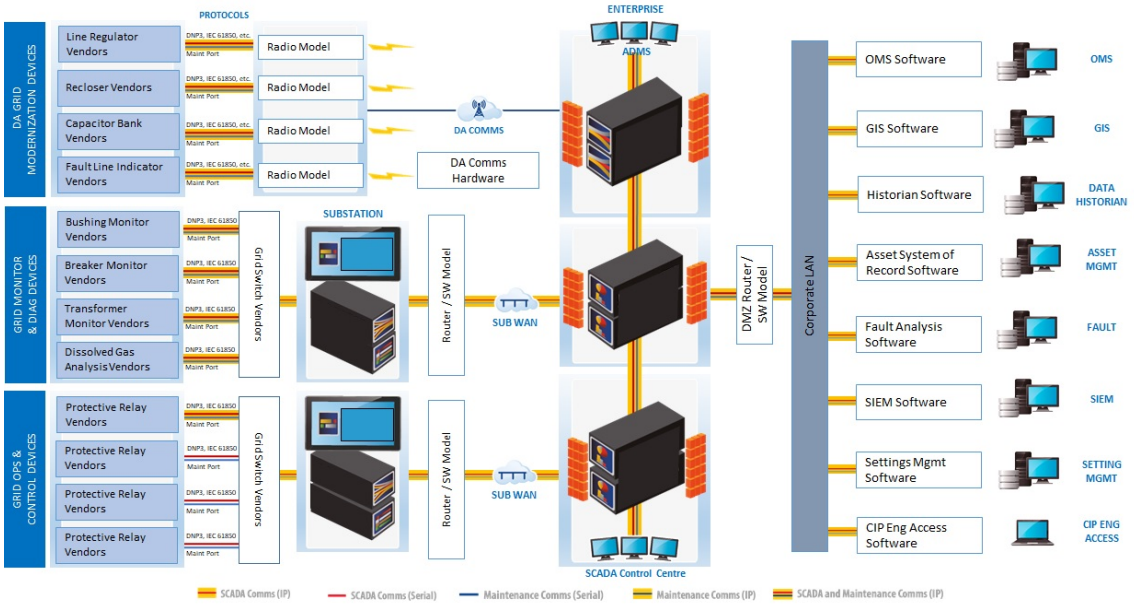

Figure 1. Typical utility automation system communication architecture

Standards

IEC 61850 is now seen to provide functional benefits and is expanding its reach to wider segments of the electric utility space, but it still does not address all functional requirements.

- IEC 61850 within Substation Automation Systems has demonstrated an ability to support complex system architectures and a wide range of substation automation functions. The concept of a single configuration definition (using System Configuration Language: SCL) for the whole substation has benefits for engineering, on-going management and documentation. SCL can be extended to include "private" data covering non-IEC 61850 equipment in the substation. For systems above a certain level of complexity, this can be more cost effective than traditional methodologies.
- IEC 61850 design fits well with the needs of substation automation, especially the object modelling and introduction of additional protocols:
  - GOOSE messaging for fast, reliable coordination of protection signals between relays
  - Sampled Values (SV) for the sharing of CT and PT data across communication networks rather than by directly wiring these signals to each relay
- IEC 61850 now defines "Technical Reports" (akin to "Application Notes" or guidelines for the implementation of specific functionality) covering a wide range of utility functions, but the list of these functions is not exhaustive.

IEC 61850 has changed how some functions are performed. Signals that might previously appeared as discrete wired terminals on a relay (where they can be independently monitored or isolated from other devices for test purposes by lifting links) now appear as data on the network. This requires alteration of design, test and maintenance practices and corresponding training in the new techniques.

- Maintenance operations such as isolating operator controls need to be considered as part of system design and may require specific programming of tools to automate these functions rather than just listing a set of steps on a manual checklist. In many cases, maintenance procedures should be considered as part of the system design process: The ability to

monitor and manipulate automation system signals for test and maintenance purposes will sometimes depend on that access being specifically identified as a functional requirement during system design. This may be an iterative process as the additional maintenance requirements are identified during system design.

- New maintenance tools become possible to inject test signals (both GOOSE and SV) to verify automation functions. IEC 61850 defines methods to allow test signals and operational signals to coexist on a network, permitting various forms of in-service testing with minimal system disruption. Remote testing becomes possible if appropriate test equipment is included as part of the deployed installation.

A caveat: While specified in the standard, test functionality is not uniformly implemented. During system design, the actual behavior of devices in the various data simulation and test modes must be verified to ensure that actual operation is as expected. Failure to do this correctly can compromise personnel safety!

Various functions remain out-of-scope for IEC 61850. For example: A protection relay may have settings and settings groups that can be modified remotely, but not protected by the same kind of cybersecurity authorization requirements (e.g. username, password) as would be required through a typical vendor's maintenance tool. At present the only aspect of device management defined within IEC 61850 is an ability to update IED firmware and configurations [3]. Device management and engineering access to devices remains largely proprietary in nature.

Access to the data within IEDs may be made for many purposes. Different users have differing data access needs to perform their responsibilities. Work is underway to define how an IED using IEC 61850 might impose role-based-access restrictions to different data for different users, but this remains a work in progress and includes considerable complexity. For non-IEC 61850 access, each different device may impose whatever restrictions or controls the manufacturer implements through their maintenance tools. In addition to this, the utility may determine that addition cybersecurity access controls are required over and above those available natively in the product tools. Enforcing the utility's cybersecurity policies might require additional procedures (workflows, training, etc.) or additional technical measures to manage data access, create auditable logs, verify device operation, etc.

Other considerations

Following is a list of some factors that may affect design choices and therefore should be considered during grid automation system projects:

- Consider all applications or users that require access to information from the system. Also consider potential future applications that might require such access and how such future access might be provided.
- Consider the functional requirements of subsystems:
    - Are there reasons why a particular technology may be mandatory or preferred for some purpose?
    - Do subsystems need to share information with other subsystems? If so, how is this done (technology, protocols, etc.) and how is it secured (verified, authorized, monitored, etc.)?
    - Are there commercial considerations that might influence or override functional requirements?
- Can various users / applications be given access to the same data? How is this controlled (authorized, verified, logged for auditing, etc.)? Do users need to be assigned to groups where access permissions are defined for the group, or are users individually assigned permissions?
- Does information need to be protected (e.g. from accidental or unauthorized alteration)? If so, from whom and how?

- Can information available within a subsystem be mapped or translated into a suitable format for use within another subsystem without loss of relevant data (e.g. without loss of timestamp or without loss of semantics)? If such lossless transformation is not possible, what limitations arise from this?
- How will maintenance actions be performed (e.g. isolation of automation functions when workers are present)?
- What kinds of remote monitoring or control are allowed for operational purposes?
- What kinds of remote monitoring or control are allowed for maintenance purposes? What kinds of changes are permitted remotely? Has this policy been reviewed to consider travel and contact restrictions such as may have been in force during the COVID-19 pandemic?
- Is similar access required to all devices, irrespective of manufacturer, age, protocol, etc., or are individual access methods for each device type appropriate? Do some devices need common access and some need individual access? This may require consideration of operational and maintenance functions, training requirements, etc.

Conclusion

Utility automation systems consist of many differing subsystems. There are typically a range of equipment types, functions performed, data available and communication protocols supported by that equipment. There are many users who have a legitimate need to access some subset of information available in the various subsystems and may have differing needs for the timeliness of that access (from immediate update of operational SCADA data to historical archive data retrieval). An integrated automation system should give all users timely access to all information they need to perform their tasks, irrespective of the actual source of that information. All access should be secured appropriately to allow authorized access and prevent unauthorized access or alteration. Each user should have such access with the minimum of impediment caused by cybersecurity functions that control the access. The process should be sufficiently intuitive as not to require extensive training.

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.

Utilities perform many functions internally, with staff having a range of skills and expertise. The automation systems they use must support those functions. A fully-integrated automation system provides the synergy of information needed to support the multi-skilled, multi-discipline workforce and enable the multiple functions that they perform for grid reliability.

BIBLIOGRAPHY

[1] 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.

[2] International Electrotechnical Commission: IEC TS 62443-1-1:2009 Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models, IEC, Geneva, 2009.

[3] International Electrotechnical Commission: IEC TR 61850-90-16:2021 Communication networks and systems in power utility automations - Part 90-16: Requirements of system management for Smart Energy Automation, IEC, Geneva, 2021.