

# industry reports

79

## Impact of IEC 61850 on Protection and Automation



B5 is one of 16 Study committees of CIGRE. Its scope is to facilitate and promote the progress of protection and automation.

IEC 61850, THE STANDARD FOR COMMUNICATION IN SUBSTATIONS was published three years ago and is already widely used in Substation Automation projects. The goal of the standard is interoperability between devices from different manufacturers. It supports the interconnection of all applications in the substation automation (SA) system from the station level with its HMI and remote control gateway to the protection and control IEDs in the bays (station bus), and from these IEDs down to the switchgear (process bus). It supports also the use of unconventional current and voltage sensors. It may replace all signal wires by serial communication links. The standard goes beyond the definition of communication since it provides additional important features like the domain specific Data Model and the Substation Configuration description Language (SCL). Therefore questions came from the users: What is the impact of IEC 61850 on protection and automation? How introduce IEC 61850 based substation automations system to exploit all benefits but to minimize the risk of this step? The CIGRE Study Committee B5 had formed the WG 5.11 which created a brochure covering all these topics and, as common, a summary in Electra - both published in fall 2007. This CIGRE brochure cannot replace the more than 1000 pages of the standard but is intended as a practical guideline for utilities. This article cannot replace the 110 pages of the CIGRE brochure



by Klaus-Peter Brand

but explain shortly some findings and highlight its helpful role for utilities.

The chapters in the brochure were written by different authors from utilities and providers. The brochure was compiled by the members of working group 5.11 and crosschecked by the representatives of CIGRE SC B5 36 member countries world-wide. The idea is that each chapter is readable by itself depending on the background and the aim of the reader. Therefore, there is some overlap between the chapter content.

Benefits and justification

Chapter 2 summarizes the features of IEC 61850 and points to the benefits. The combination of all its discussed features makes the standard unique. The homogeneous and comprehensive abstract data model including all services for the communication in substations is formulated very near to the user's (substation engineer) terminology and independent from any implementation which is left as task for the manufacturers. The mapping of this model to main stream communication means i.e. MMS, TCP/IP and Ethernet makes the standard future proof. The inclusion of the sampled values service allows exploiting the benefits of new non-conventional instrument transformers like Rogowski coils, capacitive dividers, and electro-optical sensors for

current and voltages, as well as using the common conventional transformer-type ones. The SCL of IEC 61850 provides a comprehensive description of the complete SA system. It was defined to be used by all tools - also from different manufacturers - for configuration, engineering, testing, and maintenance i.e. in any phase of the life-cycle starting from any single compliant product and ending with the maintenance phase of the customer specific SA project (Figure 3). In chapter 3 it is shown how these benefits correlate to operative and cost benefits for the utility justifying the introduction and use of IEC 61850. Examples are the use of SCL and mainstream communication technology, but also the options to replace copper wires by serial fiber optic links transporting GOOSE messages or to use any kind of today's and tomorrow's current and voltage sensors. Last not least, interoperability is not only provided between devices of different suppliers but also between different generations of products.

Concepts and migration

SA systems realized according to IEC 61850 up to now are more or less one-to-one copies of existing ones replacing only the proprietary communication by IEC 61850. This step is already beneficial since it excludes communication from competitor comparison

The switchgear and SA system should be considered as a whole.

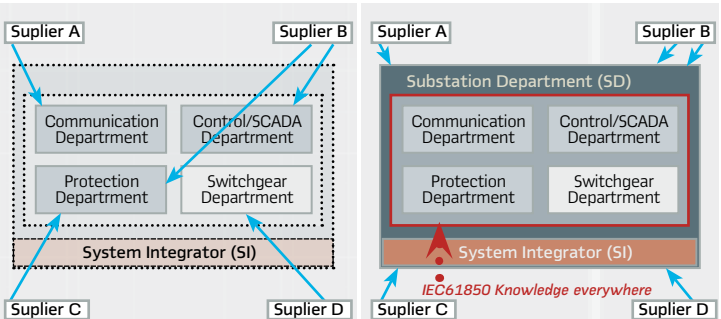
and facilitates the integration of a third party main 2 protection as needed for transmission lines. At the beginning of chapter 6 it is recommended to reconsider the system concepts to exploit the benefits of IEC 61850 as much as possible. This is especially important for migration strategies (chapter 4). There are no general strategies because any migration depends on the actual state and the intended goal for the SA system.

Specification of IEC 61850 based Systems

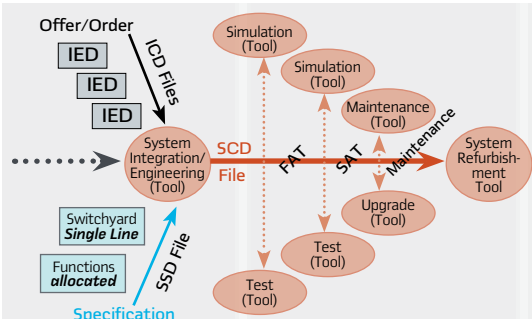
The most sensitive phase for SA systems is the specification phase because corrections later in the implementation phase may either be not possible or very costly. Guidelines for specification are given in chapter 6 by description and as checklist. The description of the site and the already existing or newly ordered switchgear is essential. The starting point is the single line diagram of the substation and the allocated SA functions as usual. The communication design based on Ethernet is more flexible and scalable than the previous proprietary ones. Active elements like switches support

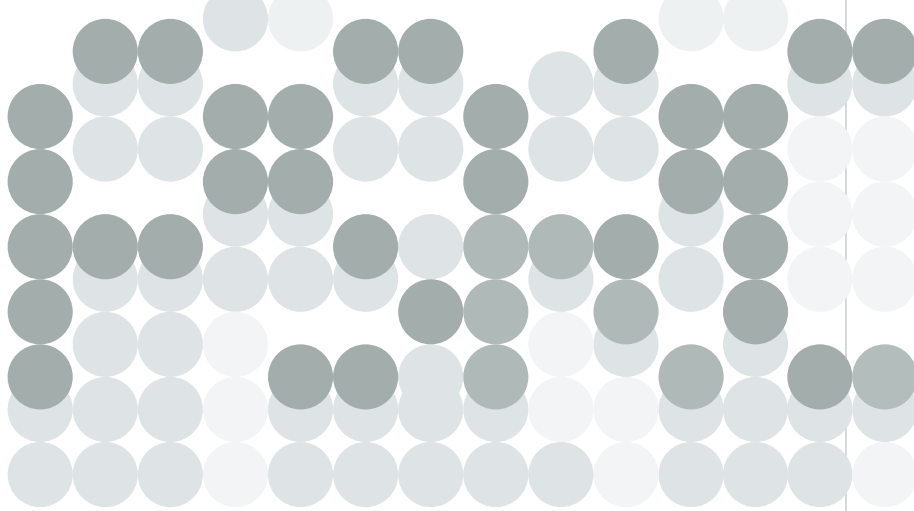
The brochure discusses a lot of questions utilities have before and when introducing IEC 61850

1 Current Responsibility of departments in utilities 2 IEC 61850-Holistic responsibility for substations



3 SCD - Thread through the life cycle of SA and substation





this flexibility. To get an optimized SA architecture, requirements for both availability and performance have to be stated. If there are no restrictions in the specification, GOOSE messages may replace all wiring between IEDs. At least for new substation the use of unconventional instrument transformers providing samples via the process bus may be considered. However, these advanced features are not a must for using IEC 61850 but an option for the future. The responsibility that the system composed of interoperable devices from different suppliers is running as specified has to be taken by the System Integrator and fixed in the specification. This role needs appropriate tools, test equipment and trained staff. Besides the SA system itself the most important item to be delivered is a single SCL-based Substation Configuration Description (SCD) file - a very cost effective basis for all testing and maintenance tools and, therefore, for any future upgrades also.

#### Responsibility in utilities

The project execution (chapter 7) is normal besides the fact that in the engineering process the SCD for the complete system has to be created and reused for system tools. In addition to the specification, the procurement process (chapter 5) and the life-cycle management (chapter 8) are within the responsibility of the utility. The utilities should invest in the knowledge about the standard to understand what they may request and what they will get. The integration of the different functions in the substation to one system may strongly impact the structure of utility organization (see Figures 1 & 2).

#### References

The introduction of IEC 61850 and its impact on protection and automation within substations

■ *Cigre Brochure 326* (produced by SC B5 WG B5.11), 2007, price 75/150 €, [www.cigre.org](http://www.cigre.org)

■ *Summary in Electra N°233*, August 2007, 21-29 ■

## Cyber Security Issues for Protective Relays



The Power System Relaying Committee is in the Power Engineering Society of IEEE.

by Solveig Ward, RFL, USA

IN A MAJOR MOVE TOWARD ensuring the reliability of the electric grid, the Federal Energy Regulatory Commission (FERC) approved eight cyber security and critical infrastructure protection (CIP) standards proposed by NERC, CIP 002-1 to 009-1. The standards will require bulk power system users, owners, and operators in the U.S. to identify and document cyber risks and vulnerabilities, establish controls to secure critical cyber assets from physical and cyber sabotage, report security incidents, and establish plans for recovery in the event of an emergency.

Substantial compliance is required by 06/2008 and full compliance by 12/2008. Utilities that do not meet audit requirements will face stiff penalties for non-compliance when audits begin in 2009.

Because of the importance of this subject the IEEE Power Systems Relaying Committee Working Group CI studied the issues of cyber security related to different aspects of power system protection and produced a report "Cyber Security Issues for Protective Relays" that is available to the community.

Cyber security is the term

commonly used with respect to the area of computers. Computers, or microprocessor-based devices with computing capability, are now commonly used for control and automation functions in addition to traditional data archival and processing.

Technological misuse and abuse has become a serious concern in all areas where computers are used and networked. The electric industry has embarked on the process to secure control systems. This requires risk assessment and review to determine what is vulnerable to cyber attacks. All assets should be analyzed in regards to the need for security.

Protection and securing of networked communications, intelligent equipment, and the data and information vital to the operation of the future energy system is one of the key drivers behind developing an industry level architecture. Cyber security faces substantial challenges, both institutional and technical, from the following major trends:

■ Need for greater levels of integration with a variety of business entities

#### Biography

Solveig M. Ward received M.S.E.E. from the Royal Institute of Technology, Sweden in 1977. She joined ABB Relays, where she has held many positions in Marketing, Application, and Product Management. After transferring to ABB in the US 1992, she was involved in numerical distance protection application design, and was Product Manager for current differential and phase comparison relays. She is a member of IEEE, holds one patent and has authored several technical papers. In June 2002, Solveig joined RFL Electronics Inc. as Director of Product Marketing.



by Solveig Ward, RFL, USA

- Increased use of open systems-based infrastructures
  - The need for integration of existing or “legacy” systems with future systems
  - Growing sophistication and complexity of integrated distributed computing systems
  - Growing sophistication and threats from hostile communities
- The report analyzes relay communications and the requirements covered in the different NERC standards. Two main groups of protection related communications applications are identified:

■ between protection IEDs and different substation and remote client applications

■ between protection IEDs with a substation or in different substations.

The requirements for the different cases are discussed in the report, followed by analysis of the impact of the communications media used on the security of the system.

In evaluating the security threat to substation equipment the report concludes that numerous people have physical contact with various devices within the substation. These individuals include employees, contractors, vendors, manufacturers, etc. Of particular concern is the fact that the typical substation environment can

provide a means to compromise the power system with a low probability of being detected or apprehended.

Threats may be caused by actions of authorized persons as well as malicious actions of authorized and unauthorized persons. Some of the threat sources to consider include:

■ Employees with criminal intent to profit or to damage others by the misappropriation of utility resources

■ Disgruntled employees or ex-employees who cause damage to satisfy a grudge

■ Hobbyist intruders who gain pleasure from unauthorized access to utility information systems

■ Criminal activity by both individuals and organizations directed against the utility, its employees, customers, suppliers, or others

■ Terrorists

■ Competing organizations searching for proprietary information of the utility, its suppliers, or customers

■ Unscrupulous participants in the markets for electric power or derivatives

■ Software providers who, in attempting to protect their intellectual property rights, create vulnerabilities or threaten to disable the software in contractual disputes

Communication protocols are one of the most critical parts of power system operations.

The International Electrotechnical Commission (IEC) Technical Council (TC) 57 Power Systems Management and Associated Information Exchange is responsible for developing international standards for power system data communications protocols. The international standards account for much of the data communications protocols in newly implemented and upgraded power industry SCADA systems, substation automation, and protection equipment.

## The report analyzes relay communications and security issues

By 1997, IEC TC57 recognized that security would be necessary for these protocols. It therefore established a working group to study the issues relating to security. The work by IEC TD57, WG 15 is to be published by the IEC as IEC 62351, Parts 1-7. The IEEE PSRC report concludes with the following Recommendations :

■ Security must be planned and designed into systems from the start. Planning for security, in advance of deployment, will provide a more complete and cost effective solution. Advance planning will ensure that security services are supportable.

■ Establish a security policy tailored to the needs of protective relay systems and the access needs of protective relay engineers

■ Assess existing communications channels for vulnerabilities to intrusion

■ Implement and enforce policies re computer usage, remote access control, with frequent auditing of systems and policies. Emphasize that security is not a part time ad hoc function.

■ Where appropriate, add policies, procedures and hardware to vulnerable communications channels and access ports.

■ Where appropriate, implement authentication and/or encryption techniques based on individual risk assessments

■ Monitor logs and traffic.

■ Maintain and monitor a list of authorized personnel who have password or authenticated access.

■ Comply with industry and government regulations.

■ Maintain a backup of vital information.

■ Prepare a recovery procedure in the event of an attack ■

### 1 Electronic Security Perimeter

