427

The Impact of Implementing Cyber Security Requirements using IEC 61850

Working Group
B5.38

August 2010

The Impact of Implementing Cyber Security Requirements using IEC 61850

Working Group B5.38

August 2010

Members

Dennis HOLSTEIN (US) Convenor, TW CEASE (US) Editor,
Stephen THOMPSON (UK) Secretary/Editor, Alex APOSTOLOV (US), Charles NEWTON (US),
Txetxu ARZUAGA (ES), Markus BRAENDLE (CH), Erik SAN TELMO QUECEDO (ES),
Janne STARCK (FI), Luc HOSSENLOPP (FR), Jo STEWART-RATTRAY (AU),
Keith STOUFFER (US), Marc LACROIX (CA), Haiju LI (UK), Albertino MENESES (PT)

Corresponding Members

Iony PATRIOTA de SIQUEIRA (BR), Ubiratan CARMO (BR), Richard SCHIMMEL (NL),
Darren WEBB (UK), Adam MIDDLETON (UK), Rodney HUGHES (AU),
Jian-cheng TAN (CA)

ISBN: 978-85873-115-2

Table of contents

Table of figures

Table of tables

1 Introduction

The International Electrotechnical Commission (IEC) has published IEC 61850 [1]. This open system standard is gathering significant worldwide momentum to become the dominant basis of protection and automation systems not only within substations, but also between substations, between substations and control centers, and between substations and other remote locations.

One feature of IEC 61850 is its strong emphasis on interoperability between intelligent electronic devices (IEDs) manufactured by different vendors. Another strong feature is the open publication of the IED data dictionary and communication services supported for most protection and automation functions. Lastly, IEC 61850 includes the specifications for peer-to-peer operation over high-speed communication channels using the Internet Protocol (IP) as shown in Figure 1.

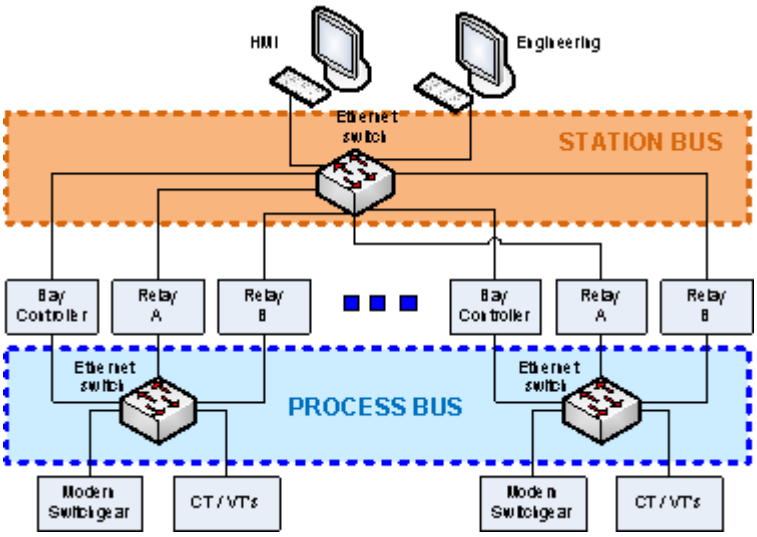


Figure 1 IEC 61850 Architecture

Interoperability, open publication of the data dictionary and communication services, and IP-based communications (both within the substation and external to the substation) inherently means that what was once a physically isolated domain of protection and automation related information and functionality within the substation, is now connected to, and hence accessible via, the general corporate communications system and potentially the World Wide Web. This raises significant cyber security[1] concerns; thus, the need to introduce requirements for prevention against unauthorized cyber-based access to and use of IEDs.

[1] Cyber security: measures taken to protect computers and computer networks from accidental or malicious harm. The security of a system is only as strong as its weakest link. When a fault is identified

Most cyber-based vulnerabilities addressed in this brochure are endemic to IP networked systems in general; for this reason one should not infer that IEC 61850 systems are more or less secure per se. The question addressed here is what is the quality and impacts of cyber-security solutions offered by others to mitigate the risk of a successful attack that applies to IEC 61850 system protection and automation reliability.

The cyber attack may be only one component of the attack; another component may be a physical attack that is coordinated with the cyber attack.

IEC 61850 itself is concerned with the processes to enable the provision of the required functionalities within a power system. Whilst by its nature it relies on a communication system defined in accordance with the ISO/OSI models it is far from prescriptive regarding the design, capability and security aspects of the communications system. Such matters should best be addressed by the Information Technology, Telecommunications and LAN/WAN technology professionals. The primary interest of CIGRE Study Committee B5 however is to provide guidance to the protection and automation community on those measures that can be included in the communications systems in order to establish and maintain a reliable, risk managed mission critical protection and automation system.

To some degree it should also be emphasized that any security measure can ultimately be broken with a combination of persistence, the right tools and inside knowledge. The objective of security measures in general is therefore to minimize the likelihood of simple attacks, increase the time it may take to complete an attack such that detection is more likely and minimize the area that an attack may exploit.

If cyber security requirements can be implemented for IEC 61850 based systems without significantly impacting the performance and cost of these systems the advantages to electric utility protection and automation are significant. It is important to understand the background for the need to examine the impact of implementing cyber security.

- IEC 61850 is a well-defined standard for the definition of protection and automation functions and the associated communication process, but currently it does not include cyber security specifications needed to control access to and use privileges of IEC 61850 data objects.
- Several CIGRE study committees, IEEE committees, IEC technical committees, ISA, United Telecom Council, ENTLEC and others are actively involved in evaluating requirements for cyber security. In most cases, the focus of the work in these forums is based on an IT perspective and addresses a wide range of communication systems. More work is needed to understand the impact of cyber security from a protection and automation perspective as an input to the work by these other groups.
- The vulnerabilities of unauthorized access to control data and unauthorized privileges to modify that data are well understood in terms of local continuity of operations.

---

and corrected, the system tends to be stronger. This state is often transient, as other faults are eventually detected and exploited.

- The impact of implementing cyber security requirements using IEC 61850 systems is not well understood by the users, which is one of the responsibilities of CIGRE Study Committee B5. For this reason, it commissioned a working group (B5.38) to perform a study to survey the threats and attack scenarios applicable to protection and automation systems, and to assess existing recommendations that offer operationally efficient and cost effective cyber security solutions.

This technical brochure reports the findings and supporting data of the work performed by CIGRE B5.38 describing the survey of threats and attack scenarios applicable to protection and automation systems. Of most interest are those threats and attack scenarios that are based on a comprehensive understanding of protection and automation system operations.

A second survey of the applications and technology was performed to identify existing IEC 61850 cyber protection methods (e.g., passwords) that provide some level of protection against unauthorized access to and use of settings. Assessments of these methods were used to identify and characterize the vulnerability and potential impact on system reliability and performance if access and use privileges are compromised. Results of these assessments are grouped into three categories.

- IED technical support performed remotely or locally by utility personnel or support vendors.
- Automation functions between IEDs that do not include human-in-the-loop control or oversight.
- EMS/SCADA and other functions that use data from, or remotely control, IEC 61850 field devices.

From a protection and automation point of view, WG B5.38 used the seven foundational requirements[2] to assess the cyber security solutions for IEC 61850 systems offered by existing or emerging standards and recommendations.

> **AC: Access Control** - "Control access to selected devices, information or both to protect against unauthorized interrogation of the device or information."
>
> **UC: Use Control** –"Control use of selected devices, information or both to protect against unauthorized operation of the device or use of information."
>
> **DI: Data Integrity** - "Ensure the integrity of data on selected communication channels to protect against unauthorized changes."

[2] Representatives from several utilities first developed six foundational requirements in the Process Control Systems Forum (PCSF). These requirements plus a seventh established by ISA were published in the ISA 99.01.01 standard [13], which was vetted and approved using ISA balloting procedure. The same requirements are in IEC 62443 [12] currently being balloted using IEC procedures.

DC: Data Confidentiality – "Ensure the confidentiality of data on selected communication channels to protect against eavesdropping."

RDF: Restrict Data Flow – "Restrict the flow of data on communication channels to protect against the publication of information to unauthorized sources."

TRE: Timely Response to Event – "Respond to security violations by notifying the proper authority, reporting needed forensic evidence of the violation, and automatically taking timely corrective action in mission critical or safety critical situations."

NRA: Network Resource Availability - "Ensure the availability of all network resources to protect against denial of service attacks."

Table 1 describes the common template used by WG B5.38 to perform assessments and evaluations of cyber security consideration of threats and attack scenarios, and solutions offered by various organizations that apply to IEC 61850. The Performance Metric relates to the potential security latency that could impact protection response time. Metrics covering hardware or software impact relate to a requirement for embedding security functionality in an IEC 61850 IED.

Table 1 Common template used for assessments and evaluations

Assessment Metric Category	Foundational Requirement						
	AC	UC	DI	DC	RDF	TRE	NRA
Performance							
IED H/W impact							
IED S/W impact							
Client-Server mixed mode							
Cost effective security management							
End-point security							
Security certification							

Protection and automation engineers place particular emphasis on the term "selected" in the AC, UC, DI and DC foundational requirements because security mechanisms embedded in new

IEC 61850 IEDs must be gracefully integrated into existing infrastructures and operate with IEDs that do not have embedded security mechanisms. They also stressed the need for a cost effective security management system to handle digital certificates, revocation lists, public keys, etc.

Security professionals are very worried about the insider threat because the insider knows in considerable detail not only how the protection and automation system works but also the most vulnerable points of access to enable attack vectors. Strongly coupled with insider threats is end-point security, which is a highly probable means of propagating an attack throughout the system.

Interoperability is an issue that must be addressed when adding security functionality. This is currently not addressed by existing standards.

When cryptographic mechanisms are required, IED manufacturers and system integrators must provide validated certification by a recognized accreditation authority (such as CMVP validation authorities for FIPS 140-2[2]) for their products and services[3]. This may add significant cost over the life cycle of the IEDs and the system.

Through common membership between WG B5.38 and the organizations offering these recommendations, the findings in this report represent a reasonable level of harmonization. These assessments and harmonization efforts produced two important contributions, which are described in this technical brochure.

- Mandatory and optional design requirements and security levels needed to protect access to and use of IEC 61850 data objects so as to mitigate the risk of compromising critical mission functions were identified.
- Mechanisms needed to adequately implement protected access to and use of IEC 61850 data objects offered by emerging standards or recommendations were identified.

1.1 Scope

Study Committee B5 is responsible for studying principles, design, application and management of power system protection, substation control, automation, monitoring and recording. Working Group B5.38 was commissioned to evaluate the impact of implementing cyber security requirements related to the use of IEC 61850, which were recommended by various study groups and standards organizations as of 2008.

The scope of the working group was limited to applications such as retrieving and changing settings, operator use and automatic control. It did not address the underlying protection and automation functions, although any security measure should not limit the ability to perform

[3] Note: Other certification authorities may be available in the future to certify non-FIPS products; e.g., ISA 99 products.

these functions. The scope did include the impact on those systems that interface to IEC 61850 field devices if cyber security requirements are implemented.

Furthermore, the scope did not include assessments of important security considerations such as those required in, or derived from, NERC's Critical Infrastructure Protection Standards (NERC, January 2008[3], and as revised May 2009) for physical security, video monitoring systems, security reporting and response planning, etc. These subjects are treated by others [4] too numerous to list in this technical brochure. WG B5.38's evaluation of the NERC CIP standards is described in Appendix D of this technical brochure.

Although there are many very good technical documents describing risk assessment methods, WG B5.38 decided to use the reports from CIGRE WG D2.22 because of its clarity and excellent descriptive examples. Several reports are listed in their recent progress report [4]. Special attention should be given to the risk assessment paper [5]. This paper is well aligned with the roadmaps developed by the EU [6] and the United States [7].

Two roadmap reports were found to be exceptional for WG B5.38's work.

> A report from the US DOE "Roadmap to secure control systems in the energy sector [7]" was of great use. In this report, the executive summary introduction states "Control systems form the central nervous system of the North American energy infrastructure. They encompass vast networks of interconnected electronic devices that are essential in monitoring and controlling the production and distribution of energy in the electric grid and the oil and gas infrastructure. The ability of these cyber systems to provide automated control over a large, dispersed network of assets and components has helped to create the highly reliable and flexible energy infrastructure we have today. However, this span of control requires control systems to communicate with thousands of nodes and numerous information systems—thus exposing energy systems and other dependent infrastructures to potential harm from malevolent cyber attack or accidents."
>
> A report from the European Commission "ICT Vulnerabilities of Power Systems: A Roadmap for Future Research" [6] also deserves attention. The GRID consortium prepared this report. GRID is a Coordination Action funded under the Trust and Security objective of the IST Programme of the 6th Framework to achieve consensus at the European level on the key issues involved by power systems vulnerabilities, in view of the challenges driven by the transformation of the European power infrastructure and ICT integration. GRID has assessed the needs of the EU power sector on these issues, so as to establish a Roadmap for collaborative research in this area. Partners in GRID are mostly European research institutes and organizations from the energy and ICT communities. The GRID stakeholder board involves prominent transmission system operators in the EU, energy authorities and the main power system manufacturers across Europe.

Protection engineers generally understand the need for cyber security. The IEEE Power System Relaying Committee (PSRC) has published a report on "Cyber Security Issues for Protective

Relays [8]. This report covers issues concerning the security of electronic communication paths to protective relays. WG B5.38 used this report to focus attention on cyber security as it relates directly to protection and automation. WG B5.38 evaluations of this contribution are described in Appendix D of this technical brochure.

IEC TC 57 WG 15 has prepared a technical specification, IEC 62351-6[9], of security solutions for IEC 61850. Because IEC 62351-6 includes by normative reference IEC 62351-3 [10] and IEC 62351-4 [11], all three documents are applicable to IEC 61850. These documents are under active consideration by IEC TC57 WG 10 to determine which recommended solutions will be incorporated into IEC 61850. WG B5.38 used the same documents to evaluate their recommendations against the seven foundational requirements.

IEC TC 65 WG 10 prepared a draft Publicly Available Specification (PAS) "PAS 62443: Security for Industrial Process Measurement and Control – Network and System Security [12]. Although PAS 62443 focuses its attention on process control systems rather than substation protection and automation systems, its treatment of the seven foundational requirements discussed above provides some very practical recommendations to provide defense-in-depth (DiD) against cyber threats and attack scenarios.

The same subject addressed by PAS 62443 is treated by ISA in their multi-series publication ISA "Security for Industrial and Automation Control Systems." ISA and IEC TC65 have agreed to parallel balloting in both bodies and publish all ISA99 documents as IEC numbered documents. WG B5.38 used ISA's treatment of security levels, establishing a security program and detailed requirements in their assessment of optional security solutions. Currently, the ISA series is numbered as follows:

ISA-99.01.01-2007: Terminology, Concepts and Models [13]

ISA-TR99.01.02: Master Glossary of Terms and Abbreviations [14]

ISA-99.01.03: Security for Industrial Automation and Control Systems: System Security Requirements and Security Assurance Levels [15]

ISA-99.02.01-2009: Establishing a System Security Program [16]

ISA-99.02.02: Operating a System Security Program [17]

ISA-TR99.02.03: Patch Management in the Industrial Automation and Control Systems Environment [18]

ISA-TR99.03.01: Security Technologies for Industrial Automation and Control Systems [19]

ISA-99.03.02: Technical Security for Industrial Automation and Control Systems: Target Security Assurance Levels for Zones and Conduits [20]

ISA-99.03.03: Security for Industrial Automation and Control Systems: System Security Compliance Metrics [21]

ISA-99.03.04: Technical Security for Industrial Automation and Control Systems: Product Development Requirements [22]

ISA-99.04.01: Technical Security for Industrial Automation and Control Systems: Embedded Devices [23]

ISA-99.04.02: Technical Security for Industrial Automation and Control Systems: Host Devices [24]

ISA-99.04.03: Technical Security for Industrial Automation and Control Systems: Network Devices [25]

ISA-99.04.04: Technical Security for Industrial Automation and Control Systems: Applications, Data and Functions [26]

1.2 Purpose

This technical brochure discusses the impact of implementing cyber security requirements using IEC 61850 on protection and automation operations, although individual functions of modern intelligent electronic devices (IEDs) are not discussed. The overall aspects of how to implement and manage secure access and use of the protection and automation functions are not part of the scope, but rather are a consequence of the introduction of the security measures. The focus is on impact, not implementation.

The purpose of this technical brochure is to provide a guide for utility responsible users (e.g., design managers, asset managers) on the impact of cyber security solutions for protection and automation systems using IEC 61850.

Unless otherwise stated, the definitions provided in the IEEE 100 dictionary [27] are used in this technical brochure.

2 Summary of findings and recommendations

This technical brochure has considered the various experience gained by utilities, study committees and standards making organization over the past several years, which have defined the cyber security risk mitigation for utility operations. It is recognized that because of known IP-based communication network vulnerabilities, availability, secure access and confidentiality are the three primary concerns of the electric power operators. There have been a number of levels and complexities of such mitigation techniques and technologies employed to date and several new ones that are already being deployed.

This work cannot hope to define "the right" technology to use to meet a utility's operational objective. It can serve as a guideline for protection and automation engineers to determine the range of solutions available and the issues that need to be considered in their final choice. The following findings and recommendations were considered the most important and deserve to be addressed in more depth by future CIGRE working groups.

1. The survey of current and planned use of substation security measures shows which security technology investments have priority from a utility point of view. Physical security continues to top the list, but cyber security is beginning to receive significant attention.
2. Many of the security issues addressed by WG B5.38 are not unique to IEC 61850. A future working group should examine the general security questions that are common to all open and proprietary protection and automation systems.
3. It is clear that no one document addresses all seven foundational requirements with sufficient detail to implement effective cyber security. More disturbing is the overlap between documents, where the same issues are addressed but the recommendations differ, and in some cases conflict. A utility should not simply require compliance with a specific document but should tailor their requirements to ensure that proposed solutions directly address their risk mitigation objectives.
4. IEC 61850 requires human interaction with the IEDs, subsystems, and system at all stages of their life cycle. A utility would be wise to include effective identity management requirements in their procurement specifications by specifying compliance with FIPS 201 [28].
5. NIST 800-53 provides the guidance to establish system level target security levels based on a utility's risk assessment and consequence analysis[4] [29]. That's the good news. The bad news is that allocating security level to the component or subsystem level is not straightforward. More work is needed to establish a verifiable mathematical model of the process and address two outstanding issues: 1) how to include the coupling or interdependence between components, and 2) how to include time and event driven changes in component security levels.
6. The statements of "research needs" in the ICT GRID [6] and the US DOE [7] roadmaps provide excellent guidance for future research. Although both roadmaps have the same objectives, their milestone dates to reach these objectives are slightly different. Their emphasis on control architectures and technologies is a very strong motivation to implement the security requirements of IEC 62351 in IEC 61850 as soon as possible.
7. Protection and automation engineers need to be concerned with the security of engineering tools used to configure IEDs and to manage mission critical settings. No standard explicitly address the security requirements imposed on IEC 61850 tools. Of particular concern are the security vulnerabilities introduced when attaching a field technician's notebook or other device (e.g., portable media) to the substation LAN. For this reason, strong security for both local as well as remote access and use

[4] Risk assessment is not based on the probability or likelihood that a threat will occur. Rather, the risk assessment is based on the consequence resulting from a cyber security exploit.

control is most important and should be addressed by IEC TC65WG15 in 62351-8 [30].

8. No standard or guideline provides sufficient technical detail to effectively address patch management in a timely manner. Although this is a general security problem, more research is needed to develop a concrete specification for patch management of IEC 61850 operating systems, protocol stacks and applications.
9. No standard or guideline provides sufficient technical detail to effectively address the TRE foundational requirements. Intrusion detection and reporting systems are currently designed to look for known scripts, but are woefully lacking in their ability to learn from attack patterns in a timely manner. More research is needed to develop derived requirements for IEC 61850 to ensure that cyber security events are reported to the proper authority in a timely manner.
10. No standard or guideline provides sufficient technical detail to effectively address the RDF foundational requirement. As reported in the Newton-Evans survey (J.1), use of firewalls to restrict data flows is receiving much attention. More research is needed to develop derived requirements for IEC 61850 to ensure the correct configuration of stateful firewalls.
11. IEC TC57WG10 should include strong cyber security compliance statements in the next revision of IEC 61850. For example, security requirements should specify security assurance levels for access and use control for any named data object. For this purpose, good security metrics using the Jaquith criteria must be established [31]. A comprehensive discussion of security metrics is offered by INL [32] and The Center for Internet Security[33].
12. As evident from the specifications reviewed[5] by WG B5.38, performance metrics to measure the impact of adding security are not clearly understood. Mission critical functions require timely delivery of information to the receiving IED. For this reason latency or throughput must include a measurement of end-to-end degradation of message delivery, not just time over the wire (network). Because IEC 61850 IEDs have not yet been designed to include security requirements adding a security signature to GOOSE / Sample Value messages is not feasible without changing the IED hardware. The primary functional requirement for the hardware acceleration is to satisfy the substation automation performance requirements for message delivery. A comprehensive report to understand cryptographic performance is described by Freescale [34].
13. The United States Congress is seriously considering comprehensive legislation to address unacceptable vulnerability to massive cyber crime, global cyber espionage and cyber attacks that could cripple critical infrastructures [35]. Within this act, the legislation would require the National Institute of Standards and Technology to establish measurable and auditable standards that would be applicable both to government and private sector. Furthermore, the legislation would require an

[5] No specification reviewed supported their claim with quantitative measurements of performance. Security mitigation recommendations were based on analytic analysis and consensus of their experts. ISA99WG04 intends to include text describing the rationale, hopefully quantitative, that supports each of their security mitigation recommendations.

Advisor to work with the US Secretary of State to develop international standards and techniques for improving cyber security.

3 ISA 99 and NIST vet the foundational requirements

ISA 99 codified the seven foundational requirements as a normative specification, ISA-S99.01.01 [13]. In ISA-99.01.03 [15], ISA and NIST performed an extensive evaluation of the foundational requirements by correlating them with the requirements in NIST 800-53 [29]. ISA99WG04TG03 extended the work in ISA-99.01.03 to establish the target security assurance levels for zones and conduits in ISA-99.03.02 [20]. In addition to relating the security assurance levels to zones and conduits, ISA-99.03.02 established the basis for compensating security mechanisms and removed the ambiguity of assigning security assurance levels based on the rules in ISA-99.01.03.

There are 17 requirements families in 800-53. Six families are covered in the management and operational aspects of ISA-99.02.01 [16]and ISA-99.02.02 [17] of the standard. ISA WG04TG02 analysis showed that except for Awareness and Training, Certification, Accreditation, and Security Assessments, Planning, Personnel Security, Risk Assessment, and System and Services Acquisition all 158 pages of the 800-53 requirements and supporting rationale were mapped to the seven foundational requirements. In addition, the mapping shows how the NIST 800-53 requirements, rationale/supplemental guidance, requirement enhancements and system-level security assurance levels can be stated.

CIGRE WG B5.38 used ISA-99.01.03 and ISA-99.03.02 to support their evaluation of security technologies and solutions offered by others that are applicable to IEC 61850 protection and control systems.

By substituting the IEC 61850 term Substation Automation System (SAS) for ISA 99 term Industrial Automation Control System (IACS), an example of this mapping and its relevance to this technical brochure is shown below.

FR 1: Access Control (AC)

800-53 AC-3: Access Enforcement (AE)

Requirement: The SAS shall enforce assigned authorizations for controlling access to the system in accordance with applicable policy.

Rationale/Supplemental Guidance: Access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) are employed by organizations to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the SAS. In addition to controlling access at the system level, access enforcement mechanisms are employed at the application level, when necessary, to provide increased information security for the organization. Consideration is given to the implementation of a controlled, audited and manual override of automated mechanisms in event of

emergencies or other serious events. The organization ensures that access enforcement mechanisms do not adversely impact the operation performance of the SAS.

Requirement Enhancement (RE-1): The automated control shall restrict access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel.

Enhancement Rationale/Supplemental Guidance: Explicitly authorized personnel should include, for example, SAS operators, security administrators, system and communication network administrators, and other privileged users. Privileged users are individuals who have access to system control, monitoring, or administration functions (e.g., systems administrators, SAS security officers, maintainers, system programmers).

Requirement Enhancement (RE-2): The SAS shall require dual authorization based on approved organizational procedures, to privileged functions that have impacts on facility, human and environmental safety.

> **RE-2 Security Strength 0:** No explicit security strength is mandated.
>
> **RE-2 Security Strength 1:** Organization with functional responsibility shall sign-off on access privileges.
>
> **RE-2 Security Strength 2:** Senior management with oversight responsibility of the functional organization responsible shall sign-off on access privileges.

Enhancement Rationale/Supplemental Guidance: The organization does not employ dual-approved mechanisms when an immediate response is necessary to ensure human and environmental safety.

System Security Assurance Levels:

> **SAL_{target}=1:** FR-1, 800-53 AC-3
> **SAL_{target}=2:** FR-1, 800-53 AC-3, RE-1 and RE-2 with security strength 0
> **SAL_{target}=3:** FR-1, 800-53 AC-3, RE-1 and RE-2 with security strength 1
> **SAL_{target}=4:** FR-1, 800-53 AC-3, RE-1 and RE-2 with security strength 2

The value of mapping the NIST 800-53 requirements to seven foundational requirements is clear. The good news is that guidance and rationale provides a very strong basis for developing the derived requirements for a particular SAS system. The bad news is that there seems to be very little empirical justification for the assignment of security assurance level – more research is needed in this area.

4 What was learned from the survey of existing threats and attack scenarios

Francis Cleveland in her paper "IEC TC57 Security Standards for Power System's Information Infrastructure – Beyond Simple Encryption" [36]has written a reasonably comprehensive description of security requirements, threats and possible attacks that are of concern to the protection and automation engineer. CIGRE B5.38 used a somewhat modified version of Cleveland's description – see Figure 2. Threats are shown in the middle row of boxes and are

mapped to the requirements for confidentiality, integrity, availability, and non-repudiation. Listening, modification, denial of service, and after-the-fact attacks are mapped directly to a specific requirement, where as Interactions and Planted in System attacks are mapped to all requirements.

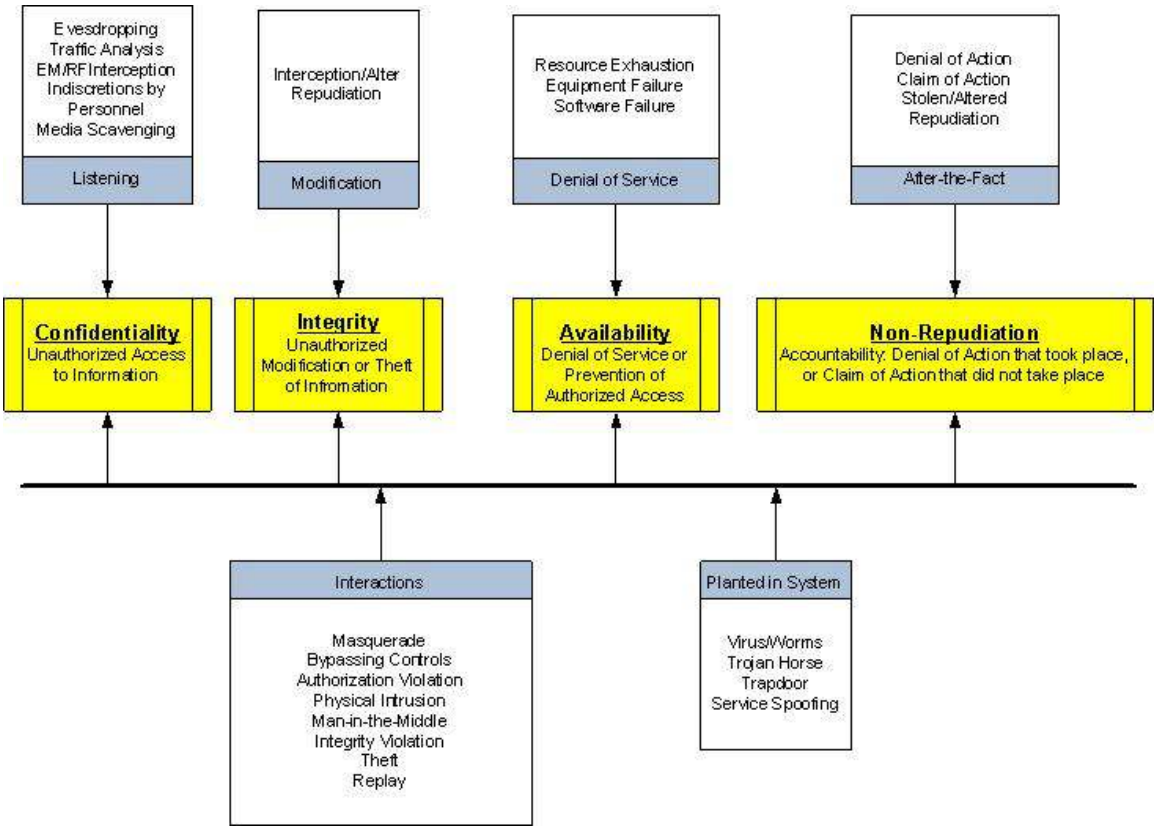


Figure 2 Security requirements, threats and attacks

5 What was learned from the survey of cyber security solutions

Reading any standard is an art form, and certainly IEC 62351 and IEC 61850 are no exception to this observation. IEC 62351 is particularly difficult because it blends several technologies such as ASN.1, cryptography and IP-based communications to define the standard. For this reason, the power system engineer and IT professional reading this brochure are first advised to read an excellent white paper by Francis Cleveland, "IEC TC57 Security Standards for Power System's Information Infrastructure – Beyond Simple Encryption" [36]. Given this background, one is ready to proceed to the assessment of impacts addressed by several documents.

5.1 First, an assessment of the contributions considered by WG B5.38

Using the seven foundational requirements and the assessment criteria, WG B5.38 performed an assessment of the quality of security solutions offered in the open literature. Although many

contributions addressed the foundational requirements, the detailed specifications varied significantly.

As with all analysis, the context of the problem space must be clearly understood in terms of the operating environment. Within a single substation, IEC 61850 IEDs exchange messages over the high-speed Ethernet station bus using a modified Manufacturing Messaging Specification (MMS) communication protocol. Messaging between substations and between substations and a control center or engineering center also use a modified MMS protocol or a non-IEC 61850 protocol such as the Distributed Network Protocol (DNP) to seamlessly interface to external applications. These two environments were grouped together for WG B5.38's assessment.

Sample values from measurement units in the substation yard are streamed over a process bus using a highly efficient communication protocol. Operating and performance constraints severely limit cyber security mitigation strategies for the process bus. For this reason, WG B5.38 separated the messaging approaches for their security assessment from the previous group.

5.1.1 Messaging within an IEC 61850 substation over the substation bus and external interfaces

Using the seven foundational requirements and the assessment criteria, WG B5.38 performed an assessment of the quality of security solutions offered in the open literature. Although many contributions addressed the foundational requirements, the detailed specifications varied significantly.

- Only ISA seems to have the initiative to develop substantial enabling detail. This work-in-progress is in its infancy and the system level requirements won't be balloted until late 2009 at the earliest. Component level requirements won't be balloted until 2011 at the earliest.

- IEC 62351 offers the best security solutions for access control, data integrity and data confidentiality, but currently falls short in other areas. A new work item has been approved to address the requirements for Role Based Access Control [30]. WG B5.38's expectation is that IEC 62351-8 will include strong requirements for use control.

Table 2 shows the quality of the solution offered using the following indicators:

PD: substantial security policy detail,

SD: substantial enabling technical detail,

VW: enabling detail is very weak

NA: not addressed.

Color-coding is added for emphasis.

Table 2 An assessment of contributed security solutions for station bus and external messaging

Document	Reference	AC	UC	DI	DC	RDF	TRE	NRA
IEC 62351 -3	[10]	TLS[6] & Certificates with strong requirement statements	VW	TLS using MAC[7] with strong requirement statements	TLS using Encryption with strong requirement statements	NA	VW	NA
IEC 62351 -4[8]	[11]	TLS & Certificates with enabling detail	VW	TLS using MAC with enabling detail	TLS using Encryption with enabling detail	NA	VW	NA
IEC 62351 -6[9] (station bus & external interfaces)	[9]	TLS & Certificates with enabling detail	VW	Digital signature using SHA256 and RSA	TLS, AES & SHA for 61850-8-1 only	NA	VW	NA
IEC 62351 -8	[30]	RBAC[10] requirements		Unknown (work-in-progress)				
CIGRE D2.22 reports	[4]	Risk-assessment methods and models address all foundational requirements						
EU ICT GRID & US DOE roadmaps	[6]& [7]	Identified research needed to address all foundational requirements						
PSRC Report	[8]	SD	PD	PD	PD	PD	NA	NA
Newton-Evans Report	[37]	Worldwide survey of Investor Owned Utilities rank ordered solutions to reduce cyber vulnerabilities						
IEC PAS 62443	[12]	Publicly Available Specification describes policy-based rationale for recommended cyber solutions						
ISA-99.01.01	[13]	Formally defined foundational requirements						
ISA-99.02.01 ISA-99.02.02	[16] [17]	SD	VW	VW	VW	VW	NA	NA

6 TLS: Transport Layer Security (see IETF RF 2246)
7 MAC: Message Authentication Code
8 Note: IEC 62351-4 includes by normative reference all the specifications in IEC 62351-3 and provides significant enabling details.
9 Note: IEC 62351-6 includes by normative reference all the specification in IEC 62351-3 and IEC 62351-4 and provides significant enabling details.
10 RBAC: Role Based Access Control

Document	Reference	AC	UC	DI	DC	RDF	TRE	NRA
ISA-99.01.03	[15]	System security requirements and security assurance levels to be addressed in detail (work-in-progress).						
ISA-99.03.02	[20]	System target security assurance levels for zones and conduits to be addressed in detail (work-in-progress). One area of particular interest are the requirements for compensating security mechanisms.						
ISA-99.03.03	[21]	System security compliance metrics to be addressed in detail (work-in-progress). One area of particular interest is the metrics related to the impact of unknown vulnerabilities on cyber security assurance.						
ISA-99.03.04	[22]	Product development security requirements to be addressed in detail (work-in-progress)						
ISA-99.04.01	[23]	Embedded device security requirements to be addressed in detail (work-in-progress)						
ISA-99.04.02	[24]	Host device security requirements to be addressed in detail (work-in-progress)						
ISA-99.04.03	[25]	Network device security requirements to be addressed in detail (work-in-progress)						
ISA-99.04.04	[26]	Applications, data and functions security requirements to be addressed in detail (work-in-progress)						

5.1.2 Messaging within an IEC 61850 substation over the process bus

WG B5.38 concluded that only IEC 62351, ISA-99.03.04 and ISA-99.04.0x contributions offer security requirements for messaging within an IEC 61850 substation over the process bus: IEC 62351-6 and ISA 99.04.0x, where x=[1,4]. As stated earlier, ISA 99.04's technical requirements is in its infancy and won't be balloted until 2011 at the earliest.

Continuing with the same coloring scheme and notation, Table 3 shows the quality of security solutions offered. IEC 62351-6 does not address AC, UC, DC, RDF and NRA requirements for the process bus, and ISA-99.04.0x intends to address all requirements for a functionally equivalent process bus. IEC 62351-6 provides significant enabling detail to prevent tampering and replay – thus it is colored green. Furthermore, SMV logs should provide the basis for timely reporting of events – thus it is colored yellow.

Table 3 Assessment of contributed security solutions for the IEC 61850 process bus

Document	Reference	AC	UC	DI	DC	RDF	TRE	NRA
IEC 62351 -6 (process bus)	[9]	NA	NA	MAC with enabling detail to prevent tampering and replay	NA	NA	SMV logs	NA
ISA-99.04.01	[23]	Embedded devices to be addressed in detail (work-in-progress)						
ISA-99.04.02	[24]	Host devices to be addressed in detail (work-in-progress)						
ISA-99.04.03	[25]	Network devices to be addressed in detail (work-in-progress)						
ISA-99.04.04	[26]	Applications, data and functions to be addressed in detail (work-in-progress)						

The reader is advised that an expansion of the assessment of IEC 62351-6 for the process bus is discussed in Chapter 5.2.2 of this report.

5.2 Assessment of impacts addressed by IEC 62351

The stage is set – only IEC 62351 and the ISA 99 technical requirements offer details of cost-effective cyber security solutions. Since the ISA 99 technical requirements are in their infancy, WG B5.38 focused its attention on IEC 62351. It is important to clearly state that several conclusions of this assessment resulted from issues that are currently not within the scope of TC57WG15. Thus, WG B5.38 assessment is not intended, nor should it be interpreted as a criticism of their work, but rather a call-to-action to consider expanding their scope of work.

Again, WG B5.38 separated the assessment into two groups: Station bus and external messaging, and process bus messaging.

5.2.1 IEC 62351 impact on messaging over the substation bus and external interfaces

IEC 62351 states that IEC 61850-8-1 profile utilizing TCP/IP and ISO 9506 (MMS) shall support TLS (Transport Layer Security). In addition to the cipher suites specified in IEC 62351-4 (that are to be used for communication between the control center and substation), within the substation TLS_DH_RSA_WITH_AES_128_SHA is recommended[11].

There are other traffic types on the station bus; i.e., IEC 61850-8-1 GOOSE and IEC 61850-8-1 GSE Management. IEC 62351 states that the same security requirements applicable to IEC

[11] See Rescorla [39] for a comprehensive explanation of cipher suites.

61850-9-2 Sampled Values (see 5.2.2) shall be considered. The impact of implementing IEC 62351 on GOOSE and Sampled Measurement Values (SMV) traffic is discussed later.

Finally, IEC 62351-6 specifies for the SNTP (as defined in RFC 2030) the use of authentication algorithms. The SNTP sync message includes a field, called Authenticator, which is optional, that includes the Message Authentication Code (MAC) information defined in Appendix C of RFC 1305.

Table 4 shows WG B5.38's assessment of IEC 62351 impacts for station bus and external messaging. Following the table is an expanded discussion of the consequences and implications of these impacts.

Table 4 Impact of implementing IEC 62351 for station bus and external messaging

Metric	AC	UC	DI	DC	RDF	TRE	NRA
Performance	For AC & UC, TLS using MAC implementation should not have a significant impact. For DI, the impact is unclear and maybe sensitive to hardware implementation.			• TLS impact is not clear because it may be sensitive to hardware implementation. • Encryption is not recommended for station bus GOOSE; i.e., within the substation. • Encryption is recommended for messaging to external substation interfaces	NC	NC	NC
IED H/W impact	May require increased CPU power and isolated security mechanisms				NC	NC	NC
IED S/W impact	• Protocol stack modification is required to support TLS • Application software modification is required to support embedded security functions				NC	NC	NC
Role Based Access Control (Part 8)	Work-in-Progress			Unknown (work-in-progress)			
Interoperability	• Selected cryptographic algorithms should minimize degradation in interoperability • Stress the importance to allow IEC 62351 conformant products to interoperate with non-conformant products						
Client-Server mixed mode	Migration strategy to implement security is not effectively addressed by IEC 62351 because it was out of scope.						
Cost effective security management	Life-cycle cost, a major concern for utility executives, is not effectively addressed by IEC 62351.						

Metric	AC	UC	DI	DC	RDF	TRE	NRA
End-point security	IEC 61850 end-point security against the insider threat is not effectively addressed by IEC 62351 because it was out of scope.						
Security certification	Formal security certification requirements are not effectively addressed by IEC 62351 because it was out of scope. This could add significant cost to 61850 IEDs.						

5.2.1.1 Why the yellow rankings

IEC 62351 provides strong access control, data integrity and data confidentiality without impacting IED hardware and software functionality. However, the "yellow" ranking is based on the uncertainty in measuring the impact on GOOSE message delivery and processing.

IEC 62351-6 uses "TLS_DH_RSA_WITH_AES_128_SHA" encryption to provide data confidentiality (DC) of information exchanged between IEDs. This cipher suite is in addition to those specified in 62351-4 in order to allow less CPU utilization when the communication environment is within a substation. For data exchanged in a relatively secure environment, within a single substation, this is probably a reasonable approach. However, data that is exchanged between IEDs in the substation and IEDs or controllers external to the substation, which is the objective of IEC 61850, should be protected against interception and interrogation by an adversary. IEC 62351-4 includes specific or normative references, recommendations for the use of encryption between substation IEDs and IEDs or controllers external to the substation.

5.2.1.2 Why the red rankings

End-point security against the insider threat is not addressed in IEC 62351. As a rule of thumb, about 20% of those working for the utility as employees or contractors are prone to be compromised. Some of these people will have access to IEC 61850 IEDs and in accordance with the GRID report [6] strong access control needs end-point security[12]. IEC 62351 should include specific, or by normative reference, recommendations on how the digital certificates used to control access are to be managed.

The need to add encryption for data exchanged between IEDs in the substation and IEDs or controls external to the substation is clear. If encryption is added, then security certification must be addressed. Issues related to providing tamper resistant or tamper proof protection of embedded encryption mechanisms is not addressed in IEC 62351. Other studies have shown that this requirement could be implemented by appropriate red-black separation, secure operating system, or secure daughter boards. However, these implementation schemes and certification probably add significant development and life-cycle maintenance cost to the IEDs. IEC 62351 should include specific, or by normative reference, recommendations on the requirements for security certification.

[12] An excellent paper "An Access Control Protocol for Embedded Devices" is recommended [44].

5.2.1.3 Security issues that need to be addressed

In summary, WG B5.38's assessment of implementing IEC 62351 for substation bus and external interface messaging raises several security issues.

- If "performance" is a concern, IEC 62351 does not address the issues; in fact IEC 62351-3 includes the note "The actual performance characteristics of an implementation claiming conformance to this standard is out-of-scope of this standard." Without performance metrics or performance criteria it is difficult to determine how best to implement these requirements.
- Furthermore, performance impact is unclear because it depends on hardware implementation, which may be memory and processing intensive.
- Implementing security may have significant life cycle cost impacts due to the extraordinary complexity of the IEC 62351 security management schemes for digital certificates, multiple certificate authorities and revocation lists.

Additional work by TC57WG15 or by TC57WG10 is needed in several technical areas:

- Develop cost effective specifications for UC, RDF, TRE and NRA.
- Develop cost effective specifications for client-server mixed mode to support a graceful migration strategy for security deployment and security management.
- Given the utility's emphasis on patch management and enhanced virus protection, end-point security should be effectively addressed.
- Security certification of IEC 61850 IEDs should be effectively addressed because of potentially high costs associated with secure key storage, secure boundary requirements for cryptographic functions, and red-black separation for high-security applications.

5.2.2 IEC 62351 impact on messaging over the substation process bus

Only IEC 62351-6, which incorporates IEC 62351-3 and IEC 62351-4, includes security requirements for substation process bus – specifically SMV security. Table 5 summarizes WG B5.38's assessment of impact to implement IEC 62351-6 on IEC 61850 process bus messaging.

Table 5 Impact of implementing IEC 62351 on process bus messaging

Metric	AC	UC	DI	DC	RDF	TRE	NRA
Performance	NA	NA	For DI, the impact is unclear and maybe sensitive to hardware implementation.	NA	NA	NA	NA
IED H/W impact	NA	NA	May require increased CPU power and isolated security mechanisms.	NA	NA	NA	NA
IED S/W impact	NA	NA	Isolating security mechanisms from SMV functional mechanisms maybe sensitive to software implementation.	NA	NA	NA	NA
Role Based Access Control (Part 8)	Unknown (work-in-progress)						
Interoperability	Requirements specified for SMV processing should enable interoperability between solutions offered by different manufacturers.						
Client-Server mixed mode	Migration strategy for SMV processing to implement security is not in the current scope of work, thus it is not effectively addressed by IEC 62351.						
Cost effective security management	Life-cycle cost associated with maintenance of digitial signatures, a major concern for utility executives, is not in the current scope of work, thus it is not effectively addressed by IEC 62351.						
End-point security	IEC 61850 end-point security against the insider threat is not in the current scope of work, thus it is not effectively addressed by IEC 62351.						
Security certification	Formal security certification requirements are not in the current scope of work, thus they are not effectively addressed by IEC 62351. This could add significant cost to 61850 IEDs.						

5.2.2.1 Data integrity is the focus of attention for IEC 62351-6 GOOSE & SMV security

It is important to note that the developers of IEC 62351-6 focused their attention on preventing replay by requiring message authentication security extensions to prevent tampering. Client processing of the SMV message improves security by discarding SMV messages whose time stamp exceeds a two-minute skew. The client should record and track the received sample count (smpCnt) for the publishing IED. If a lesser value for sequence number (sqNum) is received, and there has been no rollover, the message should be discarded[13].

Lastly for DI, generating the SHA256 hash and signing the value of the hash achieves strong authentication.

[13] This most likely will be a compliance issue (compliant to IEC 62351) and will be the responsibility of the vendor to prove this compliance, probably via an independent assessment agency.

IEC 62351 provides strong access control, data integrity and data confidentiality without impacting IED hardware and software functionality. However, the “yellow” ranking is based on the uncertainty in measuring the impact on SMV message delivery and processing.

5.2.2.2 Digital signature using message digest function

WG B5.38 used seven foundational requirements (AC, UC, DI, DC, RDF TRE and NRA) to assess the cyber security solutions for IEC 61850 systems. As evident from the survey (see J.1) and IEC 62351, Protection and automation engineers seem most interested in the first four requirements. Furthermore, all requirements are not needed in all situations and those applicable should be qualified (or tailored) to minimize functional performance degradation. For example, confidentiality (DC) of protection trip messages within the substation is generally not required, but integrity (DI) is generally required.

The substation automation system should ensure that the status change message “GOOSE” issued by logical node PDIS that is received by logical node XCBR has not been altered. Thus, from a cyber security point of view, DI is required. IEC 62351 provides the necessary integrity using a digital signature as specified by RFC 2313[38]. Keep in mind that the length of a GOOSE message depends on the choice of a data set and applying a cryptographic algorithm could significantly increase the computational requirements for the IEDs containing the two logical nodes.

Figure 3 illustrates one approach to use the hash algorithm to securely sign a GOOSE message. Other approaches are equally effective. First, MD5[39] is used to calculate 128 bit hash for the plain text GOOSE message. Using the private key Da, the RSA algorithm is used to create the digital signature and sign the GOOSE message[14]. Note that MD5 is applied only over the hash, not the full message. This ensures integrity, but not confidentiality. The good news is that processing resources needed is minimal because the length of the hash is only 128 bits.

[14] IED vendors provide the software capability to perform these functions inside the IED. A system integrator will enable the scheme and provide other optional data that the IED requires.

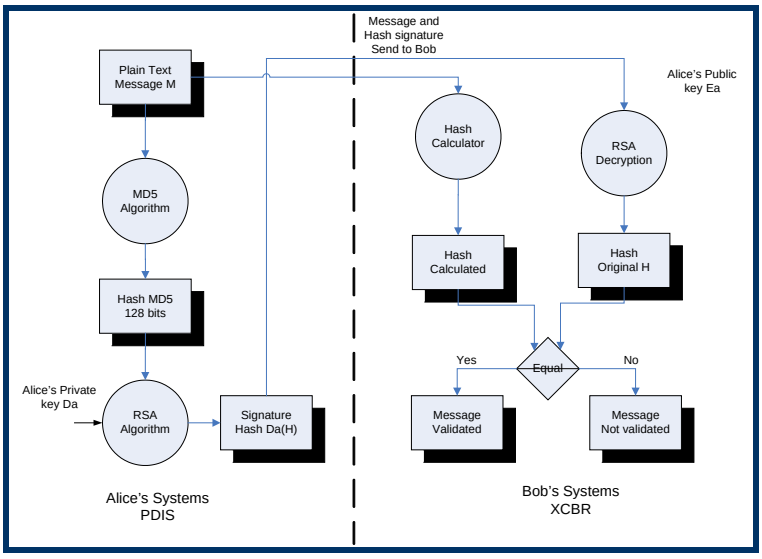


Figure 3 Digital signatures using the hash algorithm

The GOOSE message together with the hash and digital signature (called the message digest) is sent from the IED containing PDIS to the IED containing XCBR. The receiving IED recalculates the hash over the message received. Using the public key[15] Ea for RSA decryption the original hash is calculated[39]. If the two match, the GOOSE message is authenticated. If the two do not match the GOOSE message is not authenticated.

5.2.2.3 An underlying assumption of IEC 62351-6 regarding SMV security

WG B5.38 noted in IEC 62351-6, Clause 4.1 that SMVs (and GOOSE for that matter) are supposed to be restricted to a logical substation LAN (for SMV, the process bus) that provides confidentiality for information exchanges. When combined with the functional performance requirements, the developers of IEC 62351-6 concluded that encryption is not recommended. For messaging that is not performance constrained, encryption is recommended. The developers of IEC 62351-6 further noted that actual performance characteristics of an implementation-claiming conformance to IEC 62351-6 are out-of-scope. Thus, with the exception of confidentiality IEC 62351-6 sets forth a mechanism that allows coexistence of secure and non-secure Protocol Data Units (PDUs).

WG B5.38 concluded that SMVs are inherently restricted to a logical substation LAN (for this case, the process bus) which provides some security in terms of security of information in transit. However, process bus end-device security and the security of data at rest (IED configuration settings for the measurement units sending SMVs) is another matter, which is not adequately addressed in IEC 62351-6. Data at rest is being addressed by ISA99 in their standard ISA-99.04.04 [26].

[15] Public key cryptography is a fundamental and widely used technology around the world, and is the approach which underlies such Internet standards as Transport Layer Security (TLS) (successor to SSL)

6 All IEC 61850 tools need to be secure

WG B5.38 was quite surprised by the lack of attention given to the need for security assurance in the tools used to configure, test and monitor automation systems in general, and IEC 61850 systems in particular. Because of this lack of attention, this chapter includes an expanded discussion of what is needed for tool security. Only with this background was it possible to assess the impact of cyber security on the tools used in an IEC 61850 automation and protection system.

The first task was to establish five groups of tools, which could be used to summarize the impacts in the context of the seven foundational requirements. One advantage of this grouping is their direct relationship to the life cycle operation of IEC 61850 systems.

Configuration tools: These tools perform configuration of the system, whether of the whole system, an individual IED or certain components of the system. Typical configuration tools are the System Configurator and the IED Configurator.

Testing tools: These tools provide facilities to perform tests, such as simulation of conditions, and injection of signals. In an IEC 61850 system the types of tools in this category are the Station Bus Simulator and the Process Bus Simulator.

Data collection tools: These tools perform data collection operations on the network. Also, they provide permanent or temporary, local or remote, data collection for automatic recovering of internal fault records, status and measurements, reports and other data available from IEDs as well as raw data collection for packet analysis. Typical tools are Protocol Analyzers and Data Gathering.

Security tools: Tools used to configure and test the cyber security features implemented in the system. Although important, they are not specifically affecting, or affected by, IEC 61850 per se.

Commissioning tools: These tools are generally combinations of features of other tools, such as configuration and testing tools, and as such any impact on IEC 61850 systems is already considered.

It is important to note that WG B5.38 only considered tools related to IEC 61850. Although tools such as protocol analyzers are capable of wider application, it is not WG B5's intention to present an analysis of communication system tools. And, it is only the impact on IEC 61850 security that is of interest. Other impacts that may arise are not discussed in this technical brochure.

Figure 4 shows the various tool 'in situ' for a typical IEC 61850 network. Note, although the diagram shows each tool running on a separate computer, it is possible to have more than one tool running on a single computer, or even all the tools running on a single computer.

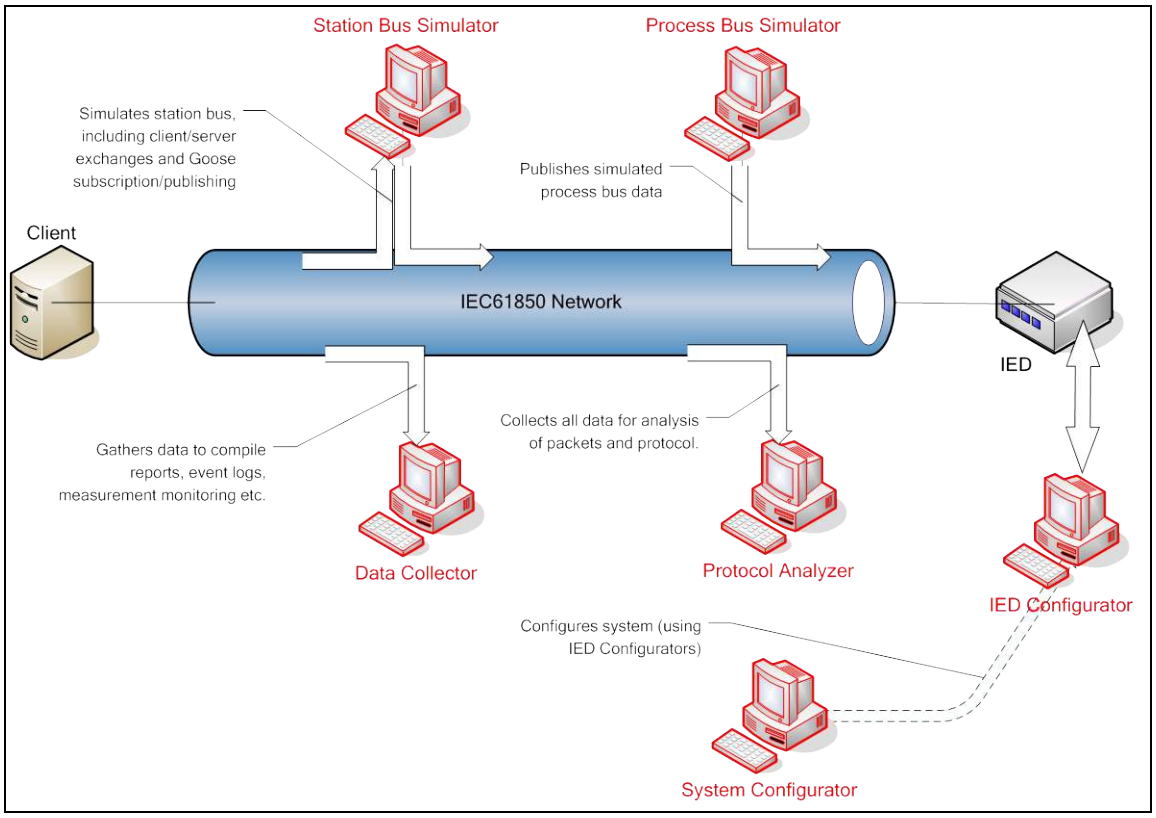


Figure 4 IEC 61850 Tool Usage

6.1 Determining category-of-impact (CoI) on IEC 61850 systems is a subtle exercise

When considering any sort of impact it should be noted that there are different categories, depending on the affect of the cyber security features implemented. The various categories of impact on a tool can be classified into three main areas.

> **Functional Impact:** The behavior, configuration, usability, application and effectiveness of the tool are compromised.
>
> **Management Impact:** Licensing, patches, updates, distribution, IP, documentation and other areas not forming part of the actual functionality of the tool are affected.
>
> **Enhancement Impact:** Tool needs new features in order to configure, manage, control, test, encode, decode and interface to systems.

Consider the impact of adding encryption. More than likely this will render most test tools totally unusable and the tools will need enhancement in order to function in the system. But should this be designated as a Functional Impact (the functionality of the tool is compromised) or an Enhancement Impact (the tool needs enhancement in order to work again)?

In determining the impact category for a tool, the main consideration is to answer the following question: does the tool continue to perform its existing functions after introduction of cyber security, or does it require new features to handle the additional requirements of the cyber security mechanisms?

- In the case of adding encryption to a test tool, such as a network-monitoring tool, it will probably fail to perform its existing functions. This will be categorized as a Functional Impact even though the tool will need enhancements to be able to function again.
- A configuration tool's functionality may not be affected by encryption, so there is no functional impact. But it may need additional functionality to allow it to configure the encryption itself. This will be an Enhancement Impact category.
- A tool may be categorized with both Functional Impact and Enhancement Impact. This would be the case where the tool's existing functions are compromised and also new functions are required to handle the cyber-security feature.
- A tool will be categorized with Management Impact if some aspect of the tool that is non-functional is impacted. A good example would be encryption key management that a tool may need to have in order to communicate with the other IEC 61850 components in the system. The management of the encryption keys for the tool would be a new factor in its life cycle.

Before leaving this topic, it is important to note that the impact costs (cost of tool modifications and adjustments to resolve any impacts) are not considered as an 'impact' in themselves – they are essentially a consequence of resolving the issues that arise from the actual impact category and will vary considerably.

6.2 Levels of functional impact

When considering functional impact it is useful to consider the level of impact that tool's functionality may incur. Some tools may not be affected at all, whilst others may have major functional impact that could render the tool unusable. WG B5.38 used for analysis the simple numeric scale shown in Table 6.

Table 6 Levels of functional impact

Level	Impact	Affect on tool functionality
1	Minor	Majority of functions still available
2	Major	Majority of functions unavailable
3	Critical	Total loss of functionality

6.3 Relating impact to foundational requirements

The seven foundational requirements give rise to a variety of mechanisms, functions and techniques – collectively described as 'Effects.' Some Effects, such as data encryption will have

impact on one or more tools. Table 7 lists the various Effects that will impact tools that arise from each of the foundational requirements. Certain terms are used to describe Effects:

Authentication: determining the identity of a user

Authorization: determining the level of control of a user

Interrogation: the act of reading and extracting data or configuration from an IED

Usage: the act of configuring and/or controlling an IED

Configuration file: data used to configure an IED or system for IEC 61850

Communication packet: a TCP/IP station bus packet

IEC 61850 interface: primary device interface through which IEC 61850 traffic flows

Table 7 Relationship between foundational requirements and 'Effect'

Foundational Requirement	Effect
AC: Access Control	Authentication management for IED interrogation
	Authorization management for IED interrogation
	Authentication management for configuration interrogation
	Authorization management for configuration interrogation
	Knowledge of authentication & authorization access scheme
UC: Use Control	Authentication management for IED usage
	Authorization management for IED usage
	Authentication management for configuration usage
	Authorization management for configuration usage
	Knowledge of authentication and authorization usage scheme
DI: Data Integrity	Detection of configuration information corruption
	Detection of IEC 61850 interface integrity failure
	IEC 61850 interface integrity management
DC: Data Confidentiality	IEC 61850 Configuration file encryption
	IEC 61850 Configuration file decryption
	IEC 61850 Communication packet encryption
	IEC 61850 Communication packet decryption
RDF: Restrict Data Flow	IEC 61850 Interface filter definitions
TRE: Timely Response to Event	Capture of tool software violations
	Capture and notification of corrupt information data
	Identification & information capture of unexpected scenarios
	Audit logging
	Intrusion detection
	Backup & recovery policy
NRA: Network Resource	None

Foundational Requirement	Effect
Availability	

6.4 Using an impact designator for tool impact assessment

The impact designator indicates the impact categories that will affect the tool. Where a functional impact is identified, the functional impact level is also identified. The Impact Designator codes are defined in Table 8.

Table 8 Impact designator for tool assessment

Impact Category	Impact Designator
Management Impact	M
Enhancement Impact	E
Functional Impact	F

Where a function impact is identified, its impact level (see 6.2) is also indicated in Table 9. Table 9 lists the various effects (see 6.3) against different types of test tools (see introduction to Chapter 6) and specifies for each an Impact Designator. For example, if a tool incurs management impact and also a functional impact at level 2, the impact designator will be MF2. Where there is no functional impact, because the Effect does not apply to that tool, then 'not applicable (n/a)' is the designator.

The reasons why certain designators have been applied to certain tools in Table 9 (see cross-reference in parenthesis) are explained in Table 10. The reasons are often not obvious although many are completely apparent. The general rule used by WG B5.38 is to designate the likely impact. But, some of the impacts designated in the table, especially those related to functional impact, are dependent on a certain tool's method of operation, and not all tools in that category will be impacted the same way. For this reason, WG B5.38 recommends that the reader regard the designations as a worse case.

Table 9 Tool impact assessment

FR	***Effect***	***Configuration Tools***		***Testing Tools***		***Data collection Tools***	
		System Config.	***IED Config.***	***Station Bus Simulator***	***Process Bus Simulator***	***Protocol Analyzer***	***Data Gatherer***
AC	Authentication management for IED interrogation	EF2 (DJ 1)	EF2 (DJ 1)	F1 (DJ 2)	n/a	n/a	n/a
	Authorization management for IED interrogation	EF2 (DJ 1)	EF2 (DJ 1)	F1 (DJ 2)	n/a	n/a	n/a

FR	*Effect*	*Configuration Tools*		*Testing Tools*		*Data collection Tools*	
		System Config.	*IED Config.*	*Station Bus Simulator*	*Process Bus Simulator*	*Protocol Analyzer*	*Data Gatherer*
	Authentication management for configuration interrogation	EF2 (DJ 1)	EF2 (DJ 1)	F1 (DJ 2)	n/a	n/a	n/a
	Authorization management for configuration interrogation	EF2 (DJ 1)	EF2 (DJ 1)	F1 (DJ 2)	n/a	n/a	n/a
	Knowledge of authentication & authorization access scheme	EF2 (DJ 1)	EF2 (DJ 1)	F1 (DJ 2)	n/a	n/a	MF1 (DJ 3)
UC	Authentication management for IED usage	EF2 (DJ 1)	EF2 (DJ 1)	F1 (DJ 2)	n/a	n/a	n/a
	Authorization management for IED usage	EF2 (DJ 1)	EF2 (DJ 1)	F1 (DJ 2)	n/a	n/a	n/a
	Authentication management for configuration usage	EF2 (DJ 1)	EF2 (DJ 1)	F1 (DJ 2)	n/a	n/a	n/a
	Authorization management for configuration usage	EF2 (DJ 1)	EF2 (DJ 1)	F1 (DJ 2)	n/a	n/a	n/a
	Knowledge of authentication & authorization usage scheme	EF2 (DJ 1)	EF2 (DJ 1)	F1 (DJ 2)	n/a	n/a	MF1 (DJ 3)
DI	Detection of configuration information corruption	E (DJ 4)	E (DJ 4)	n/a	n/a	n/a	E (DJ 4)
	Configuration file encryption	F3 (DJ 5)	F3 (DJ 5)	n/a	n/a	n/a	n/a
DC	Configuration file decryption	F3 (DJ 6)	F3 (DJ 6)	F3 (DJ 6)	F2 (DJ 7)	n/a	F2 (DJ 7)
	Communication packet encryption	F3 (DJ 12)	F3 (DJ 12)	F3 (DJ 12)	F2 (DJ 13)	n/a	n/a
	Communication packet encryption	n/a	n/a	F3 (DJ 10)	F3 (DJ 10)	F3 (DJ 9)	F3 (DJ 9)

FR	*Effect*	*Configuration Tools*		*Testing Tools*		*Data collection Tools*	
		System Config.	***IED Config.***	***Station Bus Simulator***	***Process Bus Simulator***	***Protocol Analyzer***	***Data Gatherer***
	Communication packet decryption	n/a	n/a	F3 (DJ 10)	F3 (DJ 10)	F3 (DJ 9)	F3 (DJ 9)
	SCL file encryption	F3 (DJ 5)	F3 (DJ 5)	n/a	n/a	n/a	F2 (DJ 8
	SCL file decryption	F3 (DJ 6)	F3 (DJ 6)	F3 (DJ 6)	F3 (DJ 6)	n/a	n/a
RDF	Communication interface filter definitions	F1 (DJ 11)	F1 (DJ 11)	n/a	n/a	n/a	n/a
TRE	Capture tool software violations	n/a	n/a	E (DJ 12)	E (DJ 12)	E (DJ 12)	E (DJ 12)
	Capture & notification of corrupt information data	E (DJ 12)	E (DJ 12)	E (DJ 12)	E (DJ 12)	E (DJ 12)	E (DJ 12)
	Identification & information capture of unexpected scenarios	E (DJ 12)	E (DJ 12)	E (DJ 12)	E (DJ 12)	E (DJ 12)	E (DJ 12)
	Audit logging	E (DJ 12)	E (DJ 12)	E (DJ 12)	E (DJ 12)	E (DJ 12)	E (DJ 12)
	Intrusion detection	ME (DJ 13)	ME (DJ 13)	ME (DJ 13)	ME (DJ 13)	ME (DJ 13)	ME (DJ 13)
	Backup & recovery policy	ME (DJ 13)	ME (DJ 13)	ME (DJ 13)	ME (DJ 13)	ME (DJ 13)	ME (DJ 13)
NRA	None	None	None	None	None	None	None

Table 10 Designator justification

Item	Designator	FR	Tool Class	Explanation
DJ 1	EF2	AC UC	System Configuration IED Configuration	• (E) Configuration of access and user control features in an IED or in a system will need new functions added to a configuration tool. • (F2) Existing configuration functions may be impacted by the introduction of access or user control in the system and much of its functionality may become unavailable if the tool is not able to access the IED or system.
DJ 2	F1	AC UC	Station Bus Simulator	• (F1) Part of the station bus simulator functionality is dependent on being able to modify (write to) objects, which will be compromised by authentication and authorization requirements.
DJ 3	MF1	AC UC	Data Collection Tool	• (F1) Data Collection tools' functionality will be affected to a lesser extent, probably in aspects of the configuration of the tool. Data Collection itself will probably be unaffected.
DJ 4	E	DI	Configuration Tools Testing Tools Data Collection Tools	• (E) Tool needs additional functionality to provide this detection facility.
DJ 5	F3	DC	Configuration Tools	• (F3) Configuration tools will lose all of their functionality in systems where configuration files and SCL files from the configuration tools are required to be encrypted.
DJ 6	F3	DC	Configuration Tools Station Bus Simulator	• (F3) Configuration tools that are capable of reading configuration files (either their own or from other tools) and simulator tools will lose all of their functionality in systems where configuration and SCL files are required to be encrypted.
DJ 7	F2	DC	Process Bus Simulator Data Gathering Tools	• (F2) Tools that can process configuration files may lose some of their functionality in systems where configuration files are required to be encrypted. However, some of this functionality may still be available through manual configuration.
DJ 8	F2	DC	Data Collection Tools	• (F2) Data Collection tools that can process SCL files may lose some of their functionality in systems where SCL files are encrypted. However, some of this functionality may still be available through manual configuration.
DJ 9	F3	DC	Data Collection Tools	• (F3) Data Collection tools will lose all functionality when processing encrypted data streams.

Item	Designator	FR	Tool Class	Explanation
DJ 10	F3	DC	Simulation Tools	• (F3) Simulation tools will lose all functionality in systems requiring encrypted data streams
DJ 11	F1	RDF	Configuration Tools	• (F1) Configuration tools may suffer some loss of functionality, depending on their means of communication that could be affected by RDF.
DJ 12	E	TRE	All	• (E) Almost all tools will require enhancements to support the requirements of TRE. But there will be no impact on the tool's existing functionality.
DJ 13	ME	TRE	All	• (M) Management of all tools will be impacted by the requirements of a backup and restore policy. • (E) – See item DJ 12

6.5 Tools are also vulnerable to attack

In the great scheme of things a tool is just another application, whether it is for configuration, monitoring or testing. As such it should be resilient to cyber attack so that it is not compromised or used to provide a mechanism for cyber attackers to gain access to the network. Exploitation of vulnerabilities in a feature contained in an application is a common method used by adversaries. This implies that any tool must satisfy the same criteria as any other security-aware application, outlined as follows:

- A tool should be designed and implemented using cyber-security guidelines that help to avoid accidental creation of vulnerabilities within the tool. These guidelines will specify avoidance of certain design and implementation features that are known to contain or enable vulnerabilities.
- Tools must be capable of being updated with the latest security practices. This may mean that some tools may have to be able to be updated 'on-the-fly' if they are permanently active.
- Tools need to be resilient to passive functions, such as port scans which often are an overture to an actual attack, but are not themselves an attack.
- Tools testing should include cyber-security testing as well as any functional and other tests performed by the vendor or developer. Standards that define cyber-security testing, such as penetration testing, for the class of application to which the tool belongs should be adhered to as far as possible.

Software development is moving into a new phase of requirements. Consideration for aspects such as quality and reliability, which are the norm for properly managed development, together with safety which is fast becoming a de facto requirement in embedded systems, will now also start to include security as a further essential need. Standards, legislation, coding techniques and recognized good practices will all impact tool development and could have far-reaching consequences for tool vendors. All of which is outside the scope of this technical brochure. What is significant, however, is to recognize that when considering the development of a tool, or the purchase of tool from a 3rd party, the cyber-security aspects should play as important role as any other criteria.

6.6 Are there any standards that are applicable?

B5.38 surveyed the available standards to assess their applicability to this subject. All the standards checked, unsurprisingly, did not address impact, as they tend to concentrate on what must be achieved rather than how to get there.

- The NERC CIP standards address requirements for cyber-security at a fairly high level with no specific reference to tools.
- IEC 62351 does not mention tools – the subject is ignored.
- ISA 99 does address tools, significantly in some sections, but mainly in terms of requirements to manage cyber-security – see [16].

Where tools are covered, mainly in ISA 99, the focus is on tools required to manage the system or to test the cyber-security features. For example, Automatic Software Management (ASM) tools are extensively covered with emphasis placed on patches and update management.

Existing tools with suitable upgrades could conceivably address some aspects of functionality that these tools would perform. Systems may already have in place tools that perform an ASM function that just requires additional features to manage it in a secured environment, although it is unlikely that this tool is specific to IEC 61850.

It is a recognized fact that tools will be impacted by cyber-security requirements, and that new tools (or additional functionality added to existing tools) are a necessary consequence of that. But, in answer to the question “Are there any standards that are applicable?” the answer is NO, only ISA promises to address tool security.

6.7 Assessment of contributions which address tool security

Using impact designators and impact levels, Chapter 6.4 sets forth a well-structured methodology for the assessment of contributions, including tool security requirements. That’s the good news!

Now for the bad news: WG B5.38 could find no contribution in the open sources that address tool security requirements. One could argue that IEC 62351 does address the communication between tools and IEC 61850 IEDs, but this was clearly not the focus of IEC’s current work. ISA 99 intends to address tool security requirements, but this work is in its infancy.

WG B5.38 concluded that tool security is a serious challenge for other experts; e.g., IEEE, ISA, NIST and IEC. However, the end-game requires that IEC TC57WG 10 should address the issues outlined here to develop a cost-effective security solution for IEC 61850 systems.

7 The long pole in the tent – security management

WG B5.38 assessed the impact of security management from two points of view: the impact of management processes and the impact of management controls. Appendix J provides an informative view of security from a utility executive's view point of who is responsible for implementing security, remote and local access, and some research initiatives favored by utility management.

7.1 The impact on management processes is generally high

Security management is the set of processes for identification of an organization's information assets, and the implementation of policies, standards and procedures to assure their secure use and preservation.

Utility executives have clearly stated their security concerns in response to a comprehensive Newton-Evans international survey [37]. The results of this survey are described in Appendix J.1. Influencing management requirements is the NERC Critical Infrastructure Protection (CIP) standard [3][16]. A comprehensive discussion of the CIP requirements and the implication of impacts on IEC 61850 system deployment are discussed in Appendix D.

The United States Congress is seriously considering comprehensive legislation to address unacceptable vulnerability to massive cyber crime, global cyber espionage and cyber attacks that could cripple critical infrastructures [35]. Within this act, the legislation would require the National Institute of Standards and Technology to establish measurable and auditable standards that would be applicable both to government and private sector. Furthermore, the legislation would require an Advisor to work with the US Secretary of State to develop international standards and techniques for improving cyber security. This legislation is certainly consistent with the findings of WG B5.38 as described in this technical brochure.

IEC 61850 architectures pose some unique security management challenges for policy management, risk management, monitoring and auditing, and incident response. IEC 61850 networks and systems should address the following management issues.

- Protection from unauthorized access by persons, acts, or influences; creating, deleting, and controlling security services and mechanisms; distributing security-relevant information or cryptographic keying material; and authorizing subscriber access, rights and privileges.
- Establishing a set of processes used to ensure timely reporting of security-relevant events, assessing substation risk exposure and identifying which mission critical assets to secure; defining methods and tools to reduce risk to and acceptable level; and designing plans for mitigating security risks to ensure reliable power system operation

[16] In response to FERC Order 706, NERC Cyber Security Standards is undergoing revisions. The intent is to strengthen the CIP requirements by consideration of the NST risk management frameworks, ISA 99 standards and other standards.

by providing a fast, structured and deterministic response to security incidents. ISA99 is addressing these requirements in their standards and technical reports. The challenge is to differentiate between a cybersecurity induced event and a normal operational event.

- Establish, maintain and measure the effectiveness of security awareness including personal responsibility. ISA99 is developing a standard for system security compliance metrics[21] based on the Jacquith criteria[31]. These quantitative metrics should identify the measurements needed to monitor and manage the effectiveness of security deployed in IEC 61850 systems.

Although out of scope for this technical brochure, CIGRE SC B5 should consider writing a Protection Engineer's user guide, which includes recommendations for security language to be included in a procurement specification and request for proposal.

7.2 The impact on management controls varies

The management process may use several management controls and tools, depending on the organization's security solution. These controls are classified as administrative, physical or technical, which may be applicable to IEC 61850 installations and operations. Some examples are:

- Configuration management and patch management to minimize administrative risks.
- Video supervision, locked doors and restricted locations to minimize physical risks.
- Firewalls, virus-scanning software, password control to minimize technical risks.

Table 11 shows WG B5.38's qualitative assessment of the impact of the implementation of the foundational requirements on management processes. One word of caution: the devil is in the details. Holstein and others have shown that excessive management security controls can be counter-productive, resulting in less security not more [40].

Table 11 Impact on management controls

Management Control	AC	UC	DI	DC	RDF	TRE	NRA
Administrative control	Medium	Medium	Medium	High	High	High	Medium
Physical control	Low	Low	Low	Low	Low	High	Low
Technical control	High	High	High	High	Medium	Medium	High

More bad news: Again, WG B5.38 could find no contribution in the open sources that address security management requirements. One could argue that TC57WG15 (IEC 62351) does address security management of IEC 61850 IEDs, but this was clearly not the focus of IEC's current work.

ISA 99.00.04 (part 4) intends to address security management requirements, but this work is in its infancy based on the framework developed in ISA 99.02.01 [16] and ISA 99.02.02 [17].

WG B5.38 again concluded that this is a serious challenge for other experts; e.g., IEEE, ISA, NIST and IEC. However, the end-game requires that IEC TC57WG 10 should address the issues outlined here to develop a cost-effective security solution for IEC 61850 systems.

A Bibliography

[1] IEC TC57WG10, "IEC 61850: Communication Networks and Systems in Substation," Standard IEC 61850, 2003/2004.

[2] NIST, "FIPS PUB 140-2 Security Requirements for Cryptographic Modules," Standard [Same as ISO 19790], 2001.

[3] NERC, "Critical Infrastructure Protection (CIP) Standard - CIP 002-009," Standard CIP 002-009, January 2008.

[4] CIGRE WGD2.22, "CIGRE WG D2-213: Treatment of Information Security for Electric Power Utilities," Progress Report from CIGRE WG D2.22 D2-213, January 2008.

[5] G. Dondossola, "Risk Assessment of Information and Communication Systems - Analysis of some practices and methods in the Electric Power Industry," 2008, On behalf of CIGRE D3.22.

[6] GRID Consortium, "ICT Vulnerabilities of Power Systems: A roadmap for Future Research," December 2007.

[7] US DoE, "Roadmap to Secure Control Systems in the Energy Sector," January 2006.

[8] IEEE PES/PSRC, "Cyber Security Issues for Protective Relays," Technical Report, July 8, 2007.

[9] IEC TC57WG15, "IEC 62351-6: Power systems management and associated information exchange: Data and Communication Security - Security for IEC 61850," Standard IEC 62351-6, January 2007.

[10] IEC TC57WG15, "IEC 62351-3: Power systems management and associated information exchange: Data and Communication Security - Profiles including TCP/IP," Technical Specification IEC 62351-3, January 2007.

[11] IEC TC57WG15, "IEC 62351-4: Power systems management and associated information exhange: Data and Communication Security - Profiles including MMS," Standard IEC 62351-4, January 2007.

[12] IEC TC65WG10, "IEC 62443: Security for Industrial Process Measurement and Control – Network and System Security," Public Available Specification IEC 62443, 2008.

[13] ISA99WG01, "ISA-99.01.01: Security for Industrial and Automation Control Systems - Terminology, Concepts and Models," Standard ISA-99.01.01, 2007.

[14] ISA99, "ISA-TR99.01.02: Master Glossary of Terms and Abbreviations," Draft Technical Report ISA-TR99.01.02, Work in Progress.

[15] ISA99WG04TG02, "ISA-99.01.03: System Security Requirements and Security Assurance Levels," Standard ISA-TR99-01-03, 2009 (Work-in-Progress).

[16] ISA99WG02, "ISA-99.02.01: Security for Industrial and Automation Control Systems - Establishing an Industrial Automation and Control Systems Security Program," Standard ISA-99.02.01, 2009.

[17] ISA99WG03, "ISA-99.02.02: Security for Industrial and Automation Control Systems - Operating an Industrial Automation and Control Security Program," Draft Standard ISA 99.02.02, Work-in-Progress.

[18] ISA99WG0x, "ISA-TR99.02.03: Patch Management in the Industrial Automation and Control Systems Environment," Draft Technical Report ISA-TR99.02.03, Work in Progress.

[19] ISA99WG04, "ISA-TR99.03.01: Security Technologies for Industrial and Automation Control Systems," Draft Technical Report ISA-TR99.03.01, Work in Progress.

[20] ISA99WG04TG03, "ISA-99.03.02: Technical Security for Industrial Automation and Control Systems: Target Security Assurance Levels for Zones and Conduits," Draft Standard ISA-99.03.02, 2009 (Work in Progress).

[21] ISA99WG04TG05, "ISA-99.03.03: Security for Industrial and Automation Control Systems: System Security Compliance Metrics," Draft Standard ISA-99.03.03, 2010 (Work in Progress).

[22] ISA99WG04TG04a, "ISA-99.03.04: Technical Security for Industrial Automation and Control Systems: Product Development Requirements," Draft Standard ISA-99.03.04, Work in Progress.

[23] ISA99WG04TG04b, "ISA-99.04.01: Technical Security for Industrial Automation and Control Systems: Embedded Devices," Draft Standard ISA-99.04.01, Work in Progress.

[24] ISA99WG04TG04c, "ISA-99.04.02: Technical Security for Industrial Automation and Control Systems: Host Devices," Draft Standard ISA-99.04.02, Work in Progress.

[25] ISA99WG04TG04d, "ISA-99.04.03: Technical Security for Industrial Automation and Control Systems: Network Devices," Draft Standard ISA-99.04.03, Work in Progress.

[26] ISA99WG04TG04e, "ISA-99.04.04: Technical Security for Industrial Automation and Control Systems: Applications, Data and Functions," Draft Standard ISA-99.04.04, Work in Progress.

[27] IEEE, *IEEE 100: The Authoritative Dictionary of IEEE Standard Terms*. Standards Information Network: IEEE Press, Seventh Edition - 2000, Note: Reference in braces [ ] refer to non-standard sources cited in IEEE 100.

[28] NIST, "FIPS 201: Personal Identification Verification (PIV) of Federal Employees and Contractors," Standard [Same as ISO 24727] FIPS 201-1, March 2006.

[29] NIST, "NIST SP 800-53: Recommended Security Controls for Federal Information Systems," Special Publication [Same as ISO 27002] NIST SP 800-53, February 2005.

[30] IEC TC57WG15, "IEC 62351-8: Role Based Access Control for Power Systems," NWIP.

[31] A. Jaquith, *Security Metrics - Replacing Fear, Uncertainty, and Doubt*. Boston, MA, USA: Pearson Education, Inc., 2007.

[32] M. McQueen, W. Boyer, S. McBride, M. Farrar, and Z. Tudor, "Measurable Control System Security throught Ideal Driven Technical Metrics," Conference Paper, 2008.

[33] Center for Internet Security, "The CIS Security Metrics," Consensus Metric Definitions V1.0.0, 11 May 2009.

[34] Freescale Semiconductor, "Understanding Cryptographic Performance," White Paper CRYPTOWP Rev .3, August 2008.

[35] Rockefeller&Snowe, "Cybersecurity Act of 2009," US Congressional Legislation, Work in Progress.

[36] F. Cleveland, "IEC TC57 Security Standards for Power System's Information Infrastructure - Beyond Simple Encryption," Xanthus Consulting International, October 2005.

[37] Newton-Evans, "Worldwide Market Trends on Adoption of Control Center Security Measures and Use Plans for IEC 61850 Implementation (2008-2010)," Technical Paper, May 2008.

[38] Internet Engineering Task Force, "RFC 2313 - PKCS #1: RSA Encryption Version 1.5," IEEE

Request for Comment RFC 2313, March 1998.

[39] E. Rescorla, *SSL and TLS: Designing and Building Secure Systems*. Addison-Wesley, 2001, ISBN 0-201-61598-3.

[40] D. K. Holstein, "A Systems Dynamics View of Security Assurance Issues," in *HICSS-42*, 2009.

[41] A. Carasik-Hemmi, *Best Damn Firewall Book Period*. Syngress Publishing, Inc, 2003.

[42] Pollet, Jonathan , "Who's Afraid of the Big Bad NERC," no. 3rd Quarter 2007, pp. 27-32, 3rd Quarter 2007.

[43] D. L. S. D. T. W. S. Robert J. Shimonski, *Best Damn Firewall Book Period*. Rockland MA 02370, United States: Syngress Publishing, Inc., 2003, ISBN: 1-931836-90-6.

[44] S. Tom and R. Wells, "Recommended Practice for Patch Management of Control Systems," Idaho National Laboratory Draft INL/EXT-08-14740, October 2008.

[45] IEC TC57WG15, "IEC 62351-7: Power systems management and associated information exchange: Data and Communication Security - Network and system management (NSM) data object models," Technical Specification IEC 62351-7, June 2007.

[46] M. Naedele, "An Access Control Protocol for Embedded Devices," in *1-4244-9701-0/06*, 2006.

B Definitions and acronyms

B.1 Definition of terms

Asset	A useful or valuable quality, person, or thing; an advantage or resource.
Audit	1. An independent examination of processes and data to assess compliance with specifications, standards, contractual agreements or other criteria. 2. An assessment of data logs and traces to determine that a cyber security intrusion has occurred.
Authentication	The process by which you prove that you are eligible to join a network. A challenge process to prove (validate) the identification provided; e.g., a fingerprint (identification) to access a computer via a biometric device (authentication). The biometric device authenticates the identity of the fingerprint.
Authenticator	An entity that controls the access gate
Authorization	Access privileges granted to an entity; conveys an "official" sanction to perform a security function or activity.
Authorizer	An entity that grants privileges
Availability	Ensuring timely and reliable access to and use of information
Blackout	An unplanned and uncontrolled interruption of a major part of the power system, leaving a large number of consumers without electricity. A "major" part of the power system includes at least a portion of the transmission network; i.e., an interruption in a large distribution network is not characterized as a blackout.
Confidentiality	Mechanisms that protect against the inadvertent or malicious disclosure of sensitive information
Control architecture	"Architecture" denotes the organizational dimension (hierarchical, functional and spatial) of the control system rather than the technological solutions (information and communication hardware, protocols, software) supporting it.
Control system	A device or set of devices to manage, command, direct or regulate the behavior of other devices or systems.
Criticality	The extent the failure of the considered function has the potential to lead to a major outage.
Cryptography	The study of making and breaking encryption algorithms
Cyber security	Measures taken to electronically and digitally protect computers and computer networks from accidental or malicious harm.
Data at Rest	Information stored in any repository including memory registers of an IED.
Demilitarized Zone (DMZ)	A computer host or small network inserted as a "neutral zone" between a private network and a public network[41].

End point security	An information security concept that basically means that each device (end-point) is responsible for its own security.
Entity	An individual (person), organization, device or process.
Hardware acceleration	The use of hardware to perform some function faster than is possible in software running on the general purpose CPU. Examples of hardware acceleration include instructions for complex operations in CPUs.
Hash function	Any well-defined procedure or mathematical function which converts a large, possibly variable-sized amount of data into a small datum, usually a single integer that may serve as an index into an array. The values returned by a hash function are called **hash values**, **hash codes**, **hash sums**, or simply **hashes**.
Incident response	The set of processes used to minimize the impact of security incidents on substation and power system operations.
ICT functions	Functions based on information and communication technology needed for power system observability and controllability. In the context of power systems, they encompass protection, monitoring, control operator decision support, system management and coordination.
Identification	The process of recognizing an entity (human or device). Identification could be a password, a token or a fingerprint.
Information assurance	See information security
Information security	Mechanisms that deal with several different “trust” aspects of information as it applies to all aspects of safeguarding or protecting information or data, in whatever form. Another common term is information assurance.
Integrity	The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner.
Message protection	A process to ensure that once you have joined the network, you can communicate without risk of interception, modification, or other security risks
Monitoring	The continuous observation of a device or system with respect to its state or any changes that may occur over time, using a measuring device of some sort.
Multicast (GOOSE)	A transmission mode in which a single message is sent to multiple network destinations (i.e., one-to-many). Note, from Wikipedia: IP Multicast is a method of forwarding IP datagrams to a group of interested receivers.
Non-repudiation	A service that is used to provide proof of the integrity and origin of data in such a way that the integrity and origin can be verified by a third party as having originated from a specific entity in possession of the private key of the originator.
Observability	Property of a system which implies that its initial state can be determined from input and output variables, which are observed within a finite time interval.

Password	A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.
Phishing	A form of criminal activity using social engineering techniques. It is characterized by attempts to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an apparently official electronic communication. Phishing is typically done using email or an instant message. The term *phishing* arises from the use of increasingly sophisticated lures to "fish" for users' financial information and passwords.
Policy management	The set of processes used to define and enforce an organizational strategy including organization standards, procedures and guidelines related to information security.
Privacy (Data privacy)	The evolving relationship between technology and the legal right to, or public expectation of privacy in, the collection and sharing of data about one's self. Privacy concerns exist wherever uniquely identifiable data relating to a person or persons are collected and stored, in digital form or otherwise. In some cases these concerns refer to how data is collected, stored, and associated. In other cases the issue is who is given access to information. Other issues includes whether an individual has any ownership rights to data about them, and/or the right to view, verify, and challenge that information. The service used to prevent the content of messages from being read by other than the intended recipients. {Note: in this context, this technical brochure uses the term "confidentiality" instead of privacy.
Proxy server	A process providing a cache of items available on other servers which are presumably slower or more expensive to access.
Protocol Data Unit (PDU)	**1.** Information that is delivered as a unit among peer entities of a network and that may contain control information, address information, or data. **2.** In layered systems, a unit of data that is specified in a protocol of a given layer and that consists of protocol-control information of the given layer and possibly user data of that layer.
Red-black separation concept	Refers to the careful segregation in cryptographic systems of signals that contain sensitive or classified plaintext information (**RED signals**) from those that carry encrypted information, or cipher text (**BLACK signals**).
Revocation	The process by which privileges and access rights are removed (cancelled or annulled)
Revoked	The state of being cancelled or annulled.
Risk management	Establishment and maintenance of security processes to mitigate the consequences of a vulnerability that can be exploited.
Security	See IEEE Dictionary definitions for software and computer resources, but for this technical brochure exclude the definition for the degree of certainty that a relay or relay system will not operate incorrectly. Note: in this technical brochure the term security should always be restricted to the context of cyber security.

	Cyber-security as defined by Webster Dictionary “measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack.”
Supplicant	An entity that wants to have access.
Threat	Any indication, circumstance or event with the potential to disrupt or destroy critical infrastructure or any element thereof, including accidents, natural hazards as well as deliberate attacks.
Trust	An attribute of an entity that is relied upon to a specified extent to exhibit an expected behavior
Trustworthiness	An attribute or trait of the system which causes it to be deserving of trust (see definition of trust) and confidence
Vulnerability	An expression of the system’s lack of ability or reduced ability to withstand an unwanted situation, limit the consequences, and to recover and stabilize after the occurrence of the situation, where an unwanted situation is a situation with real or potential death or injury of people or loss of economic value.
Wi-Fi	An industry standard for products based on IEEE 802.11 as defined by the Wi-Fi alliance – an industry consortium

B.2 Definition of acronyms

AC	Access Control
AES	Advanced Encryption System
ASM	Automatic Software Management
CERT	Computer Emergency Response Team
CC	Coordination Center [CERT-CC]
CMVP	Cryptographic Module Validation Program
CPNI	Centre for Protection of National Infrastructure [UK]
DC	Data Confidentiality
DI	Data Integrity
DMZ	Demilitarized Zone
DoS	Denial of Service
DiD	Defense in Depth
EPRI	Electric Power Research Institute
ES-ISAC	Electricity Sector –Information Sharing and Analysis Center
FERC	Federal Energy Regulatory Commission [US]
FIPS	Federal Information Processing Standards [US]

FIRST	Forum of Incident Response and Security Teams
HMI	Human Machine Interface
ICT	Information and Communication Technologies
IM	Identity Management
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
INL	Idaho National Laboratory
ISA	The International Society of Automation
IOU	Independent Operated Utility
ISO	International Organization for Standardization
IT	Information Technology
MAC	Message Authentication Code or Media Access Control
MD	Message Digest
MSMUG	Microsoft Manufacturing Users Group
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NRA	Network Resource Availability
PAS	Publicly Available Specification
PDU	Protocol Data Unit
PSRC	Power System Relaying Committee
RADIUS	Remote Authentication Dial-In Service
RBAC	Role Based Access Control
RFC	Request for Comment
RTU	Remote Terminal Unit
SCSM	Specific Communication Service Mapping
SMV	Sampled Measured Value
SSL	Secure Socket Layer
TISP	The Infrastructure Security Partnership
TLS	Transport Layer Security
TRE	Timely Response to Event
UC	Use Control

VLAN	Virtual Local Area network
VPN	Virtual Private network
VSL	Violation Severity Levels

C Who is the adversary

There are many threats and attack scenarios that have been suggested in the open literature. The problem is that no one has addressed a comprehensive distributed attack on the bulk power delivery system, which is needed for WG B5.38 analysis. So, rather than using one of the published scenarios, WG B5.38 members used their imagination to create a credible scenario that would highlight the cyber issues that are most related to protection and automation starting with the "insider threat." This was broadened to include the notion of an insider to include not only employees of the utilities, but IEC 61850 device and systems companies, system integrators, and consultants that support all aspects of protection and automation design, test and evaluation, commissioning, operations, and maintenance who may normally have legitimate need to access any part of the system.

To create the threat and attack scenario, WG B5.38 had to "think outside the proverbial box." One advantage was that the working group members knew in considerable detail the cyber vulnerabilities of IEC 61850 protection and automation systems. With this knowledge, we considered what was possible rather than what attacks had been reported in the open literature. A good analogy is the attack on Pearl Harbor by the Japanese in 1941. United States military leaders did not believe that a torpedo attack was possible because the harbor was too shallow for existing air delivered torpedoes. The Japanese military understood this limitation, and with a well-defined objective in mind, developed shallow running torpedoes. The attack was rehearsed until all elements of the attack were coordinated in both space and time. Keep this in mind – WG B5.38 used the same approach.

It is beyond the scope of this work to define the motive for the attack. Rather, we simply state that the sponsor of the attack is well financed and has sufficient patience to properly train and rehearse all attack elements over considerable time to ensure that all procedures are well defined. The attack scenario is designed to leverage cyber vulnerabilities of the substation systems, and is highly coordinated in both space and time to achieve the maximum effect such as a wide area blackout, physical damage to primary equipment, extreme financial liability and loss of confidence in the electric utility sector reliability. The cyber attack may be only one component of the attack; another component may be a physical attack that is coordinated with the cyber attack.

Agents[17] of the attack sponsor are carefully chosen. Again, it is beyond the scope of this work to discuss how the agents are selected and what motivation (e.g., financial, exposure of sexual

[17] The coordinated attack envisioned by this scenario will require many well trained people. Those who execute the attack are called "agents" of the sponsor of the attack. The sponsor may be a rogue

orientation, marital problems, etc) was used to compromise their integrity. However, this is a topic of considerable importance when defining a security program and for performing a comprehensive risk assessment that should be addressed by CIGRE SC D2.

For the purpose of this analysis, WG B5.38 defined the adversary as many people (not a single hacker) with a comprehensive knowledge of the mission critical protection and automation functions, which are the object of the attack. These protection and automation functions may be operated by one utility, or they may be operated by several utilities on a large segment of the electric grid.

A good model for the adversary to consider is the 13 August Northeast blackout in the United States. The operational situation that resulted in the blackout was the underlying fact that neither technical nor management staff knew about the problem in advance. Had they known, they had the tools and the means to prevent the blackout. The situation is analogous to the "fog of war" in the sense that because of system operating complexities, the response timeline, and the ability of the adversary to confuse the responders, a highly coordinated and well-practiced attack will produce the desired consequences.

D NERC CIP requirements may have sharp teeth

The North American Electric Reliability Corporation (NERC) has developed a series of Cyber Security Standards, called Critical Infrastructure Protection (CIP), which are numbered CIP 002 through CIP 009[18]. The intent of these standards is to ensure that all entities responsible for the reliability of the Bulk Electric Systems in North America identify and protect Critical Cyber Assets that control or could impact the reliability of the Bulk Electric Systems. The Federal Energy Regulatory Commission (FERC) initially approved these standards in January 2008 with the exception of CIP 006-1a, which was approved in February 2008. The standards were revised and approved in May 2009 as Revision 2. Utility executives have expressed some apprehension of standards without defining success metrics. Without these metrics what criteria will be used to levy the ominous $1M USD fines?

NERC is currently developing a document which addresses the proposed Violation Severity Levels (VSL) for the CIP series of standards.

While these standards are strictly speaking only applicable to North America, it is expected that some version of these standards will eventually be applied elsewhere.

---

organization, a nation state, or any individual with sufficient funds and patience to plan and coordinate the attack.

[18] The latest approved version of the NERC CIP standards can be obtained at http://www.nerc.com/~filez/standards/reliability_standards_regulatory_approved.html.

D.1 What NERC laid on the table that requires compliance

In order to discuss CIGRE B5.38's assessment of the impact of these standards on IEC 61850 systems, it is best to review the content and objectives of these standards. Keep in mind that NERC designed these standards to provide a cyber security framework to support reliable operation of the Bulk Electric System. As such, each standard should be read as part of a group of standards, and not treated individually.

The standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets need to manage its reliability, and the risks to which they are exposed. NERC recognized that business and operational demands for managing and maintaining system reliability increasingly rely on Cyber Assets supporting critical functions and processes. These functions and processes must communicate with each other, across functions and organizations, for services and data.

To add some perspective of these requirements, B5.38 began with a table developed by Jonathan Pollet that was published in the UTC Journal, 3rd Quarter 2007 [42]. WG B5.38 added some text (shown in italics) to the table to highlight specific considerations applicable to their assessment of the impact implementing NERC CIP standards using IEC 61850. In particular, B5.38 separated SCADA system operators, from protection and control engineers who reside in separate organizational units. Each organization unit should be an active member of the security team to ensure that compliance with the NERC CIP standards reflects their operational constraints, and minimizes mission critical performance impacts that could be introduced by a specific security solution.

As shown in Table 12 for each requirement group, Pollet identified five project work phases and owner (organizational department) responsible for the assessment. A short description of each project phase is shown in Table 12 for reader convenience. The work process flow and timetable for CIP compliance is discussed at length in the journal article.

Table 12 Break NERC compliance effort into manageable phases

CIP Standard	Requirement	Project Phase	Project Owner
002 Critical Cyber Asset Identification		Phase 1	IT Lead Working with SCADA system operators, and protection and control engineers.
	R1 Critical Asset Identification Method	NERC GAP analysis to determine critical assets & critical cyber assets. The critical assets are identified using a risk-based assessment and methodology similar to CIGRE WG D2.22 approach (CIGRE WGD2.22, January 2008).	
	R2 Critical Asset Identification		
	R3 Critical Cyber Asset Identification		
	R4 Annual Approval		
003 Security Management Controls		Phase 2	HR Lead

CIP Standard	Requirement	Project Phase	Project Owner
	R1 Cyber Security Policy(ies)	Compare existing corporate policies, procedures, and personnel training with NERC CIP Standard to ensure that minimum-security management controls are in place to protect Critical Cyber Assets.	Working with IT, SCADA system operators, and protection and control engineers. Note: It is important to consider all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors.
	R2 Leadership		
	R3 Exceptions		
	R4 Information Protection		
	R5 Access Control		
	R6 Change Control		
004 Personnel Training			
	R1 Awareness		
	R2 Training		
	R3 Personal Risk Assessment		
	R4 Access		
006 Physical Security		Phase 3	Physical Security Lead Working with IT SCADA system operators, and protection and control engineers. Note: To get FERC approval, CIP 006 was revised from the original to add an appendix discussion dial-up access to RTU, and when it is not necessary to have a "six-wall" border.
	R1 Physical Security Plan	Compare existing physical security measures at critical assets against NERC requirements.	
	R2 Physical Access Controls		
	R3 Monitoring Physical Access		
	R4 Logging Physical Access		
	R5 Access Log Retention		
	R6 Maintenance & Testing		
005 Electronic Security Perimeters		Phase 4	IT Lead Working with SCADA system operators, and protection and control engineers.
	R1 Electronic Security Perimeter	Conduct a vulnerability assessment of critical cyber assets to determine existing controls, vulnerabilities, minimal ports/services, and document patch management and remaining NERC CIP requirements.	
	R2 Electronic Access Controls		
	R3 Monitoring Electronic Access		
	R4 Cyber Vulnerability Assessment		
	R5 Documentation Review and Maintenance		
007 System Security Management			
	R1 Test Procedures		
	R2 Ports & Services		

CIP Standard	Requirement	Project Phase	Project Owner
	R3 Security Patch Management		
	R4 Malicious Software Protection		
	R5 Account Management		
	R6 Security Status Monitoring		
	R7 Disposal or Redeployment		
	R8 Cyber Vulnerability Assessment		
	R9 Documentation Review & Maintenance		
008 Incident Reporting & Response Planning		Phase 5	IT Lead Working with SCADA system operators, and protection and control engineers.
	R1 Cyber Security Incident Response Plan	Review existing cyber security plans for incident reporting and response planning. Make sure that plans can be exercised on a routine basis *and are consistent with existing continuity of business and disaster recovery plans*.	
	R2 Cyber Security Incident Documentation		
009 Recovery Plan for Critical Cyber Assets			
	R1 Recovery Plans		
	R2 Exercises		
	R3 Change Control		
	R4 Backup and Restore		
	R5 Testing Backup Media		

D.2 WG B5.38's assessment of NERC CIP impact on IEC 61850

The following is an assessment of how the NERC CIP standards apply to the foundational requirements. These descriptions give an indication of the requirements at this time. Since some of the NERC CIP standards are still under development some of these assessments are "best guess." Using the same notation described in 5.1.1, Table 13 shows the assessment of NERC CIP standards impact on IEC 61850.

Table 13 Assessment of impacts addressed by NERC CIP standards on IEC 61850

NERC CIP Standard	AC	UC	DI	DC	RDF	TRE	NRA
002 Critical Cyber Asset Identification					X	X	PD
003 Security Management Controls	PD	PD		PD	PD		
004 Personnel & Training	PD						
005 Electronic Security Perimeters	PD	PD	PD	PD	PD		PD

006 Physical Security	PD	PD	PD	PD			
007 System Security Management	PD	PD	PD	PD			
008 Incident Reporting & Response Planning						PD	
009 Recovery Plan for Critical Cyber Assets						PD	PD

NERC has 2 documents out for comment: 1) **Violation Risk Factor** that shows NERC's assessment of the risk factors for CIP-003-2 and CIP-006-2, and 2) **Violation Severity Levels** that delineate the various severity level violations. These levels are **Lower VSL**, **Moderate VSL**, **High VSL**, and **Severe VSL**. NERC has not documented what the fine or other remedial action will be implemented per violation.

D.3 UK's Centre for Protection of National Infrastructure

There is currently no organization in the UK that mandates cyber-security legislation in power distribution control systems. Certification appears to be a matter of utility or vendor preference, although several companies provide validation and certification services, and it is assumed that utilities would expect to see some level of cyber-security validation certification from a prospective vendor.

But this does not mean that the government in the UK is blind to the risks and dangers of unsecured control systems. A new body, the Centre for Protection of National Infrastructure (CPNI), was created on 1 November 2007 from a merger of two other bodies that were responsible for security advice and co-ordination. The principle aim of the CPNI is to provide advice, guidelines and information for businesses and organizations involved in running and maintaining the national infrastructure. This encompasses a wide range of national infrastructure areas ranging from emergency services, health and transport to energy, finance and food and addresses many security threats including bombs and other physical threats.

Of course cyber-security is what this Technical Brochure is interested in and the CPNI has much to say about this subject. It has published a series of guidelines and recommendations for process control and SCADA security that, whilst not explicitly concerned with power distribution and protection, does cover many of the areas discussed in this technical brochure such as architecture and responses to incidents. The CPNI also has guidelines on general network security that covers many of the remaining areas of interest in this document.

Whilst the role of the CPNI is presently advisory, it is accountable to the Director General of the Security Service (MI5) and operates under the Security Service Act 1989, and so it does not need much imagination to consider that in the future many of its recommendations may become mandatory as the threats against national security become ever more pervasive and

determined. However, whether recommendation or mandatory requirement, it is certain that the cyber-security pronouncements of the CPNI are every bit as essential as the ones from North American organizations like NERC and ISA.

E IEEE PSRC provides significant insight into mission critical cyber vulnerabilities

In Appendix C, WG B5.38 established the adversary. IEEE PSRC protection engineers provided significant insight into critical cyber vulnerabilities that WG B5.38 used as a framework for achieving the objective of the attack scenario. PSRC in their report [8] summarized the following issues. These issues formed a significant basis for analysis by WG B5.38.

The need for remote access: Utility personnel require remote access to the protection, control, and monitoring devices located in substations scattered throughout the system. This access is required to: continuously assess the health of the system; recognize developing problems that may adversely affect the ability of the system to remain operational; identify the location of faults and failures to facilitate the dispatch of repair crews; analyze the operation of protective devices to ensure correctness and maintain coordination to prevent cascading outages; identify possible improvements to protective schemes; verify the accuracy of system models to facilitate planning studies.

Level of access required: The level of access required depends on job function. System control operators need to know what happened and where (breaker status changes, system element loading, relay target data and fault locations, intrusion alarms, etc.) Protection engineers typically need to read the stored data (relay, fault recorder, and disturbance monitor event records and setting records) in order to analyze system disturbances, support operations personnel, coordinate protection schemes, and ensure compliance with NERC standards. Protection engineers can also make settings changes as required due to changes in system configuration. Field relay technicians need read/write access to all levels of the devices in order to apply the settings determined by the protection engineers and set up the devices for proper operation and communication with those that need access.

Relays are critical to the power system: The settings in a relay determine the response (or non-response) of the device and incorrect settings may have serious effect on the power system operation. Typically, relay settings are allowed to be changed by Protection Personnel only, but the multi-function nature of microprocessor relays have extended use of protection devices to other groups as well. A modern relay may replace a traditional RTU and provide metering data and control functions for opening and closing breakers and other switches. A relay may also be connected to a substation computer that performs automation and control functions. The multi-function nature of the relay device may generate the need to extend 'setting-change-privileges' to others than protection engineers that creates an added challenge for the protection engineer to track, document and verify relay settings.

IEC 61850, like other protocols, introduces special re-commissioning requirements: Utilities may have processes in place that dictate if any relay setting has changed, including the communication security settings, the relay must be re-commissioned. Changing the settings could adversely impact the protective functions of the relay. Where relay passwords must be changed, requiring re-commissioning of all relays can quickly become impractical because there may be hundreds or thousands of passwords to change. Clearly, this is not necessary because it does not affect the functionality of the device.

The following sub-sections of this appendix provide more depth of understanding of the rationale for the recommendations offered in the PSRC report[19]. WG B5.38 assessment of the implications of these recommendations is clearly identified as comments to the text.

E.1 Remote access should be available

Access should be available within the substation and corporate offices. A limited number of personnel will require full access at non-company locations. The expectation of round the clock analysis capabilities and the quantity of data available often requires access via the Internet. A dial up connection may also be used for less demanding requirements. Access to the corporate "Data" network via the Internet raises the highest level of concern for cyber security.

Typically, a utility utilizes the extended capability of microprocessor relays to provide status, control and metering functions to a station RTU via a serial communication link. This functionality has replaced traditional analog transducer and hard-wired alarm connections to a central station RTU in all new installations and many retrofit locations. Any settings required for these extended functions should be communicated to the protection engineer during the schematic and/or relay setting development phase. The automation engineer may also initiate setting changes through the protection engineer if only changes associated with automation are required. Ultimately, the protection engineer should be the individual responsible for all protective relay settings and documentation – the automation engineer works through the protection engineer to implement necessary automation settings.

E.1.1 The need for role based access control

Preferably, relay access passwords should be established that allow view-only user access to automation engineers (and maintenance personnel or system operators). A second, more secure level in which setting changes may be made should be reserved for relay engineers and test technicians. Testing contractors may utilize temporary passwords to complete necessary setting changes and testing.

Relays have settings that can be generally grouped into the following categories: protection, communication (usually related to integration and automation, not teleprotection), and security. Utilities may have processes in place that dictate if any relay setting has changed,

[19] This rationale is extracted nearly verbatim from the PSRC report.

including the communication and security settings, the relay must be re-commissioned. This re-commissioning policy can be beneficial when relay communication settings are changed. With the deployment of protective relays on substation LANs using IEC 61850, it is possible that communication settings could be changed (such as IP address) that would adversely impact the protective functions of the relay. This re-commissioning policy may adversely impact the procedures put in place for securing relays, where relay passwords must be changed under certain situations (employee leaving, contractors leaving, password aging, etc). In these situations where relay passwords must be changed, requiring a re-commissioning of all relays where the password(s) are changed can quickly become impractical because there may be hundreds or thousands of passwords to change, and in some cases, re-programming of devices that include passwords in the retrieval of SCADA data from relays.

Relay re-commissioning after a settings change should include a careful review of how communication and security settings impact overall device integration and security policies. This review should include not only relay engineers, but automation engineers and security professionals as well. For example, relays that do not perform protective functions over a LAN and are polled using DNP over the LAN may only require a quick point check to confirm that polling has been re-established after a communication settings change; relays that do not perform protective functions over a LAN and are polled using DNP do not require re-commissioning after a password change. It is possible that the relay setting change process may drive the technological solution for the security process, or vice-versa.

Although PSRC describes this issue in terms of DNP polling; the WG B5.38 concluded that the same issue is applicable to IEC 61850.

E.1.2 Don't neglect the need for confidentiality

Electronic eavesdropping can be achieved in all communications media by intercepting or tapping into communication signals. Dial-up phone lines are especially vulnerable as the device connected to it can be directly accessed through the public telephone network. Any security should be handled by the device itself. Leased phone lines are more likely to suffer from denial of service rather than interception due to the highly specialized and often-proprietary data they carry. Eavesdropping in Local Area Networks (LAN) and Wide Area Networks (WAN) is called sniffing. A sniffer is a program that accepts and opens network packets that are not addressed to your equipment. Wireless eavesdropping and sniffing can occur on virtually all commonly used wireless networks including, radio, satellite, and microwave transmissions.

The issue is not what can be gained by listening (reading) SMV, GOOSE or other IED-to-IED messages. Rather, the need for confidentiality is to protect configuration data, settings data and other information which is used to control protection and automation functions in IEC 61850 systems.

E.1.3 Unique requirements for the data link and network layers

Although PSRC describes this issue in terms applicable to any protocol, WG B5.38 concluded that the issues are directly applicable to the assessment of cyber-security impacts using IEC

61850[20]. The seven foundational requirements used for assessment by CIGRE B5.38 included consideration of the unique requirements for the data link and network layers of the OSI model.

Cyber Security in the Substation can be addressed at both the Data link and Network layers of the OSI model. The addressing mechanism at the Data link layer is the Mac address that is predefined by the manufacturer of the Ethernet enabled communications equipment. At the Network Layer the IP address is used. The network should be secured at both layers. Each communications device used on the network has specific vulnerabilities and in most cases features to deal with them. Many of these features need to be configured.

Security design within the network is paramount in the process of securing the network. While securing the network the following features should be considered.

E.1.3.1 The data link layer

- The Data link layer is commonly called layer 2. At this layer switches are the most prevalent communications equipment used. Many different features are available on the switches that can impact the Security on the network.
- Switches have their own security to protect against intrusion or unauthorized configuration. Switches should be configured with passwords and secrets that are unique and follow strong password standards. SSL or SSH should be used when configuring switches to prevent sniffing these passwords.
- Individual ports on the switch can be secured using several methods. In the simplest form they may be enabled or disabled. It is recommended unused ports be disabled. Each port may be further secured using MAC based security, 802.1x or VLAN filtering.
- When MAC based security is used each port on the switch can be configured to allow communications only from one specific MAC address. With this method of security, only the IEDs intended to communicate on any given port (or a hacker spoofing an IED's MAC address) can do so.
- With IEEE 802.1x technology devices are forced to authenticate with a predefined user name / password before they gain access to the network. 802.1x clients are required on the IED in order to make this effective. Most windows clients available today have integrated 802.1x clients. The authentication is usually done by a third party entity, such as a RADIUS server.
- When VLAN based security is used, all traffic entering the network comprises (or is assigned) IEEE 802.1Q "tagged" frames, with each tag's "VID" field identifying a specific VLAN. Un-trusted sources are assigned (on ingress) an appropriate VID to guarantee the isolation of such sources from the traffic assigned to other VID's.

[20] As mentioned before, CIGRE SC B5 should consider writing a user's guide to recommend procurement language in a request for proposal.

E.1.3.2 The network layer

- The Network layer is commonly called Layer 3. At the Network layer many devices can be used to secure the network. The devices commonly used at this layer are Routers, Firewalls and Intrusion detection devices. Some Security appliances are available that offer all three functions in one box.
- Routers / Firewalls / Intrusion detection devices have their own security to protect against intrusion or unauthorized configuration. These devices should be configured with passwords and secrets that are unique and follow strong password standards. SSL or SSH should be used when configuring these devices to prevent sniffing these passwords.
- Routers and Firewalls can do IP filtering. Filtering can be used to deny access to the Substation network from unauthorized IP networks. In order to use this feature effectively the IP address space within the entire Utility should be assigned effectively.
- Filtering can be done at the Port / Socket layer. Ports / Sockets are used to identify traffic by type. These can be services such as FTP, HTTP or Telnet. Many organizations prohibit some of these services on the Substation LAN by policy.
- Intrusion Detection devices can be used to look for network anomalies. This is done by comparing traffic against a known database of signatures, which identify traffic patterns that are known to present network vulnerabilities. When an anomaly is detected on the network the network administrator is notified. The network administrator will generally take action by configuring filters on the Routers or Firewalls.
- Encryption can be used on the LAN to secure traffic against unauthorized access. This can be done for Routers, Firewalls and some IED's. Several different types of Encryption algorithms are commonly available. These include DES, 3DES or AES. 3DES is the most common. AES is a newer standard that offers a higher level of security.

Multiple sources in the open literature have stated that DES and 3DES are not secure and should not be used. For this reason, utility engineers should consider upgrading legacy installations that use DES and 3DES to AES.

E.2 WG B5.38 assessment of the PSRC report

The strength of the PSRC report is that it provides a comprehensive discussion of the cyber security issues that are directly related to the protective relaying functions. The emphasis is on access control, and many technical enabling options are discussed. For the most part, discussions of use control, data integrity, data confidentiality, and restricting data flows are offered in the context of security policy, not enabling technical options.

Two foundational requirements received no attention in the PSRC report: Timely reporting of events (TRE) and network resource availability (NRA).

Another area not addressed by PSRC is the impact of adding security on software certification as related to certifying the hardware and software needed to for the security mechanisms.

Lastly, although key management was discussed in general terms, no real insight was provided on the requirements or life-cycle costs of managing the access and use privileges.

It is important to note that PSRC created WG H13 to address the application issues associated with the various cyber security requirements. Their stated objectives are:

1. To address utility issues in the definition of cyber security requirements adherence,
2. To reference typical substation automation architectures including all communicating devices interfacing to and within substation protection and control system and their relevance to cyber security requirements,
3. To provide guidance on best technical practices which can aid in the fulfilment of NERC CIP and other cyber security standards, and
4. Create a guide that can be referenced in substation automation system specifications.

F Contributions from the GRID report

The GRID Roadmap[21] identifies three main areas for investigation:

Risk and vulnerability assessment tools and methods: Future work should focus particularly on the relations between the ICT functions and the power system. The assessment should support the risk management by a single operator as well as the governance of the whole infrastructure, including cross-border aspects.

Control architectures and technologies: Due to their complexity, full redesign of control architectures for power systems is not suitable, so that research and development must focus on their upgrade. ICT upgrades in control centers that expose protection and control functions to unsecured access along with the existing use of telecommunications may introduce vulnerabilities. In that context, understanding the cascading effects of ICT faults on power system functionality and developing mitigation failure mechanisms is crucial.

Awareness and governance of risk in society: A general culture of risk awareness will have to permeate the human, organizational and societal dimension of the power infrastructure, embracing the physical and ICT aspects of the systems. Future development should also focus on the creation of educational tools and methods that not only make power engineers aware of ICT security risks and vulnerabilities, but also of how such vulnerabilities interact with the electric grid and what can be done to prevent and mitigate risks.

[21] Only the GRID report is discussed in detail to conserve space in this technical brochure. The reader should be aware that the US DOE roadmap report [6]to secure control systems contains the same recommendations with slightly different milestone dates to reach their objectives.

All foundational requirements are addressed in GRID roadmap, but there is no specific detail that addresses the enabling technologies. However, one statement of need was of particular interest to WG B5.38.

> *"The needs expressed by the stakeholders focus on simple and standard vulnerability and risk macro indices and criteria and corresponding micro indices for dependability characteristics. Moreover, the need is perceived for methods and tools that handle a very broad spectre of risk and vulnerability, including human and organizational factors covering "all relevant" hazards and threats. These are truly ambitious needs, and it must be expected that they cannot be satisfied with a comprehensive method. Instead it will probably be necessary to subdivide the total system and process in several sub-processes, and for each define a framework of risk and vulnerability analysis."*

WG B5.38 certainly agrees with this statement of need, and looked for enabling specifications in the documents considered in their analysis.

F.1 The scope of power system security and ICT in GRID

The purpose of this action concerns ultimately the security of the power system while fully taking advantage of the ICT functionality. The power grid consists of both transmission and distribution grids. However, since large blackouts occur mainly on the bulk transmission grid where the cascading effects are clearly inherent, the focus is on the transmission grid. In addition, critical events triggered by distribution with large impact on transmission have to be considered. A large blackout is an outage resulting in significant loss of load that can cover a country/TSO (Transmission System Operator) jurisdiction or several countries/TSOs. Figure 5 shows a conceptual view of the power system, dividing the system in five hierarchical levels, of which Level 1 and 2 concerns measurements (voltage, current, power, etc.) used for all other functionality.

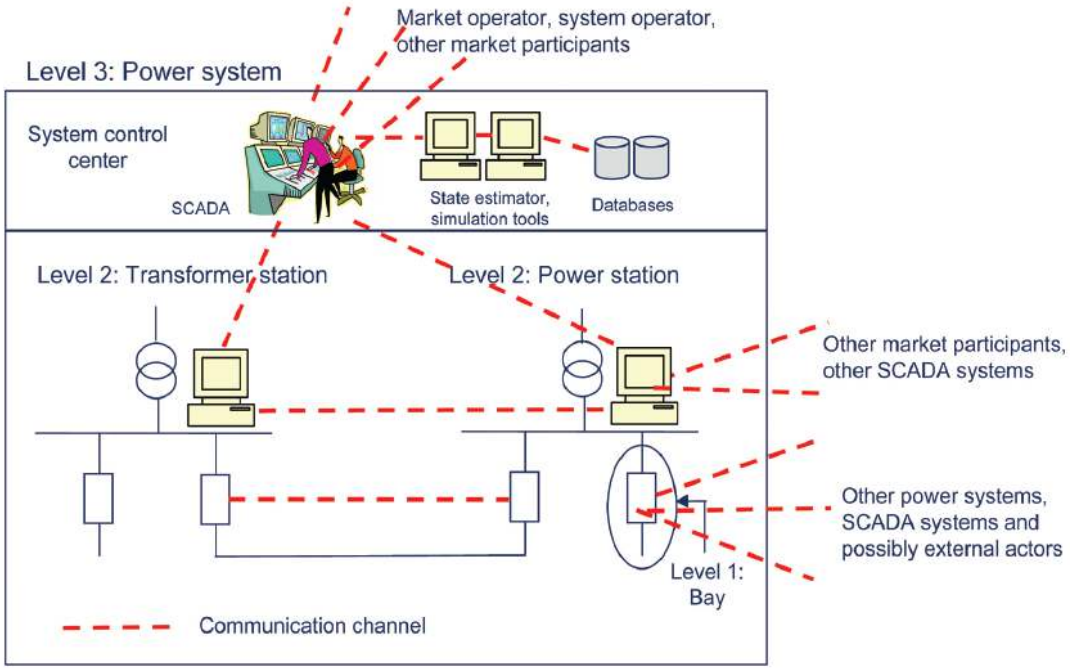


Figure 5 ICT conceptual view of the power system

At Level 1, the bay level, relevant functions are related to bay protection, control and automation, monitoring and locally controlled system functions like load shedding schemes or generator tripping.

Level 2 is the station level, involving conceptually similar functions as Level 1, but that involve station level interactions. Level 3 is the power system (or rather control area) level with functionality like data exchange and processing, state estimation, system management and coordination, and operator decision support. At the highest level, not shown in Figure 5, is the total power system, including the interactions between the control areas and external actors.

In today's power systems, ICT is involved at every level and in virtually all functions. The interaction between ICT and the power system is viewed in terms of the consequences of the vulnerability and criticality of these ICT functions on the reliability of the power grid. Direct effects of ICT failures at the transmission grid level can be as follows:

- Loss of or corrupted observability of mission critical operating parameters
- Corruption of Energy Management System (EMS) functions
- Loss of generation capacity caused by unbalances of power and load
- Loss of lines and corridors
- Malfunction of protection or power control devices
- Power system instability

Direct effects on distribution grids or on generation plants may also have significant indirect impact on transmission grids. The direct effects on distribution relevant to the GRID action can be loss of local generation or loss of substations and feeders. Relevant direct effects on generation plants can be loss of generation capacities and power system instability.

F.2 GRID's research roadmap

Table 14 summarizes the main drivers for the evolution of the EU power grid. Table 14 distinguishes positive, negative and neutral effects from the perspective of the security of the power grid. Hence, positive factors have to be understood as those factors having the potential to improve the security of the system, while negative factors are those considered as potentially jeopardizing the security of the system. The neutral factors are those that can act to improve or degrade security, or can have no effect on power system security. To meet these challenges, GRID identified three main priorities that represent the main pillars for achieving a secure and reliable energy transport infrastructure with the next 15 years.

Risk and vulnerability assessment tools and methods[22]**:** The review process has emphasized insufficient focus on action concerning risk and vulnerability assessment tools and methods. Focused R&D is required on the relations between the ICT functions and the power system. This work should produce tools and methods applicable by industry.

Control architectures and technologies[23]**:** Due to their complexity, full redesign of control architectures for power systems in not suitable, so the investigation must focus on their upgrade. The current difficulty or barrier is to integrate innovative control technologies allowing effective protective measures and defense strategies to be envisaged with regards to various levels of ICT failures. Meanwhile, new control paradigms are emerging based on the use of decentralized intelligence with the aim of enhancing the level of security with respect to responsibility levels.

Awareness and governance of risk in society: There is strong need to increase awareness of control and ICT vulnerabilities among policy and business circles, technical actors and the public at large. A basic and widespread education on risk is lacking. Future developments should also focus on the creation of educational tools and methods that not only make power system engineers aware of ICT security risks and vulnerabilities, but also of how such vulnerabilities interact with the electric grid and what can be done to prevent and mitigate risks.

[22] CIGRE D2.22 is concentrating their effort on the subject of risk vulnerability assessment tools and methods. They have produced a series of excellent technical brochures on this topic.
[23] WG B5.38 considers the ICT GRID roadmap emphasis on control architectures and technologies to be one of the strongest motivations to implement the security requirements of IEC 62351 into IEC 61850 as soon as practical.

Table 14 ICT GRID view of the evolution of the EU power grid

Context	
Power Systems Trends and Drivers	Control Trends and Drivers
Factors with Negative Impact on Security	
• Power systems become increasingly more important for the society with growing demand for electricity • Increased interdependencies between systems and infrastructures • Intensification of cross border trade: growing demand, hectic transactions • Power systems become increasingly more dependent on an efficient and reliable information system • More uncertainties with distributed generation and renewable energies • Emergence of malicious attacks against infrastructures	• Control systems grow more and more complex and integrated with business/ enterprise systems • More and more interconnections to other utilities, power markets, external partners etc • Large installed base of (older) communication and control technology
Factors with Neutral/Unknown Impact on Security	
• Enlargement & integration of the EU electricity market • Market restructuring, growing number of stakeholders	• Control systems more and more distributed • Impact of advanced control and communication technologies
Factors with Positive Impact on Security	
• Important investments forecasted in generation and transmission	• New systems and functions are quickly adopted • Layered and distributed control and ICT systems

F.3 GRID consortium's vision for the year 2020

The role of ICT for flexible, secure and cost effective operation and control of the present and even more the future power system is essential. Indeed, with the present trends and drivers, a power system without widespread utilization of ICT is difficult to imagine. However, ICT also brings about new challenges with respect to power system security. Therefore, the GRID consortium has developed the following Vision for the power systems of 2020.

The power system maintains efficient and secure operation and continues fully utilizing its ICT functionalities without loss of load, in spite of incidents occurring in supporting ICT systems or intentional cyber assaults

To fulfill this vision, GRID Roadmap presents a set of recommendations out of a consultation process among stakeholders and the research community. The most import recommendations are:

- Launch EU research on risk assessment of power systems and their supportive ICT systems, ensuring the stakeholders' involvement.
- Launch research efforts to upgrade control architectures for better handling ICT threats, with special regard to interdependencies and cascading effects.
- Progress towards establishing EU wide consensus on risk governance arrangements for the EU power infrastructure, based on the thorough analysis of current and future physical and cyber threats.

To support these recommendations, there is a need to:

- Sponsor the establishment of EU security databases containing information based on real security incidents, countermeasures, consequence, etc.
- Promote the development of standards for security assessment, management and communication, based on shared security metrics.
- Promote the establishment of EU lab tests and test procedures.
- Dedicate a significant effort to education on security, in particular with respect to the role of ICT in power systems.

G Vulnerabilities of IP-based networks

With the convergence of control systems and modern networking technologies comes some inherited security vulnerabilities. As an IEC 61850 system is based on the very popular TCP/IP/Ethernet protocols, it is subject to the same threats as any other industry distributed control system based on these protocols. Some examples are listed below.

- Denial of Service (DoS) attacks by, for example, the use of excessively fragmented packets.
- Scanning attacks typically consisting of a host that tests the accessibility of every IP address in a LAN by looking for backdoor access opportunities.

- Incomplete sessions, such as TCP SYN attacks, which try to block attacked hosts by running out of resources.
- Interface overloads.
- IP spoofing, where a packet uses an incorrect source IP address to obscure its true source.

Note the obvious relationship between the above list and the seven foundational requirements used for the assessments in this technical brochure.

G.1 Some thoughts on intrusion prevention

A brief definition of TCP/IP and TCP/IP virtual ports is first discussed better understand what a firewall or other defensive scheme must achieve in order to effectively provide computer port security.

G.1.1 First, a basic understanding of TCP/IP virtual ports

All TCP/IP communication is facilitated by the exchange of IP data packets between two computers. For this discussion an IED is a specialized computer. Each IP data packet is transmitted from the source "sending" device to the destination "receiving" device. These two devices agree that they are connected and maintain their connection to allow transmission of data between them. Each device also sends and receives data packets that acknowledge the receipt of the other device's transmitted data. IP data transmission requires that every data packet contain a destination address and a port number.

Also, so that the receiving computer knows the origin of the message, the data packet must also contain the IP address and port number of the sending computer. In general terms every IP data packet must contain its complete source and destination address.

An IP port on a computer is only opened when the computer accepts the request from the first arriving data packet to establish a connection. If a request for a connection is denied, then that port is effectively invisible and nothing will be able to connect to it.

G.1.2 The objective of a stateful firewall

The function of a stateful firewall is to inspect each and every packet before it arrives at the receiving device and prior to it being seen by any other application running on the device. The firewall is programmed to distinguish legitimate packets for different types of connections. Only packets matching a known connection state will be allowed by the firewall; others will be rejected[24]. A comprehensive discussion of firewalls is available in the book "Best Damn Firewall Book Period."[43]

[24] Early attempts at producing firewalls operated at the application level of the seven-layer OSI model but this required too much CPU speed. Packet filters operate at the network layer (layer-3) and function more

When properly configured a stateful firewall has total power to veto the receipt of any IP packet by blocking access to the requested IP port. The uniqueness of a stateful firewall is its ability to be “selective” about what data packets it allows thru and which ones it blocks out. The selective “filtering” is based on any combination of the originating IP and port addresses as well as the destination device’s IP and port address.

Other methods used by substation engineers to provide port security include port scanning, Network Management System (NMS), user authentication, corporate firewalls and passwords.

G.1.3 IEC 61850 substation stateful firewall with intrusion protection

As with any other IP/Ethernet network, there are well-known security measures that can be deployed in order to defend against these threats. For instance, stateful inspection firewalls protect against the unauthorized use of network resources. To do so, they must make access control decisions to determine what type of network traffic is allowed in and out of the network.

Some attacks against networks today are often based on the application level traffic. For protection against application level attacks, intrusion prevention systems (IPS) may be used. A well-designed IPS should understand enough of the application protocols to look for deviations. Once an application-level attack is detected, a variety of responses can be triggered.

As in any modern network, an IEC 61850 system requires application protection throughout the network. As shown in Figure 6, the IPS should be deployed behind a stateful firewall and in front of the main mission critical servers to protect application level data from both external and internal attacks.

---

efficiently because they only look at the header part of a packet. However, pure packet filters have no concept of state as defined by computer science using the term finite state machine and are subject to spoofing attacks and other exploits.

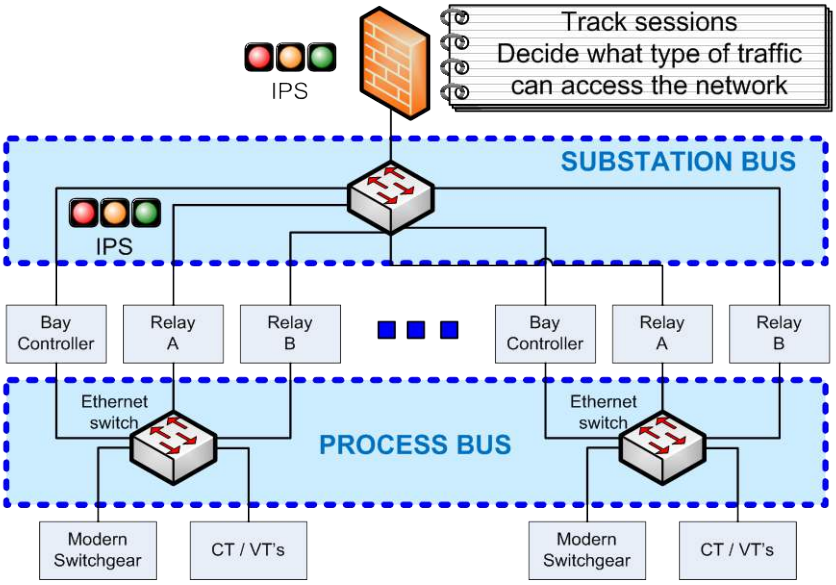


Figure 6 Recommended location of firewall and IPS

G.2 Stack implementation vulnerability

Some cyber attacks succeed by exploiting features is protocol stacks[25]. IEC 61850 stacks are not immune to these flaws. In a substation environment where many IEC 61850 IEDs are running un-patched software applications or operating systems, if single stack vulnerability is exploited on one IED, the entire network may be affected.

Clearly, an IEC 61850 system shares the same vulnerabilities as any other system that runs over TCP/IP/Ethernet and well-proven security measures need to be employed; e.g., stateful firewalls, IPS, and careful attention to up-to-date software patches.

Software patch management is a topic of current discussion within ISA99 and the Microsoft Manufacturing Users Group (MSMUG). MSMUG uses a team discussion list to hold newsgroup-style discussions – see http://www.msmug.org. The Idaho National Laboratory (INL) reported that patch management of industrial control systems software[26] used in critical infrastructure and key resources is inconsistent at best, nonexistent at worst. Recommended patch management practices for industrial control systems owners are identified for consideration and deployment in their report[44].

[25] Specific protocol stack implementation vulnerabilities can be found in NIST's National Vulnerability Database – see http://nvd.nist.gov/. To illustrate the type of IEC 61850 stack vulnerabilities reported in this database, WG B5.38 reviewed VU#372878. *It is important to note that this vulnerability has been corrected in later versions of the communications software.*

[26] IEC 61850 systems are categorized as industrial control systems software.

H Security assurance level mathematics and issues

One of the major challenges addressed by the project team developing ISA standards is the specification of the security assurance level mathematics and the related quantitative security metrics. This challenge may be described as follows.

H.1 System security assurance

The security level of the system (S_{system}) is the sum of the weighted security levels of the components ($w_i s_i$).

Where, the asset owner, based on the owners' risk assessment and evaluation of consequences, assigns the weighting and security level of the component.

The target security level of the system is given by the NIST 800-53 Special Publication [29]. There is no insight in the NIST publication as to how an asset owner should allocate system level security target to component (or subsystem) security levels.

The target value for the system should be greater than the estimated (calculated) value for the system.

There are three issues that must be addressed – this is the hard part!

1. How does one account for the coupling (interdependencies) of component security levels?

   If the component security levels are independent, then

   If the component security levels are coupled, then the coupling is:

2. Does defense-in-depth provide the mathematical foundation to decouple security levels from a common cause point of view?

Another way of implementing conditional situations is through pre-requisites. For instance, you may only want your user to be able to access a component once that user has permission to pass through a gatekeeper, such as a firewall. The prerequisites feature enable analysts to include these and other conditions in a scenario by allowing you to easily create rules governing the availability of locations, items and actions.

3. The security level of a component is not static. How does one account for the time dynamics or the event dynamics?

= and

The easy way out is to only address the static case and assume that the component levels are independent. The problem is that this will not address the real world problem, and one could develop a false sense of security. WG B5.38 does not have the expertise to address these issues, but the issue is on the table for others with strong mathematical backgrounds to ponder.

H.2 Security metrics are the keys to a cost-effective solution

Utility owners struggle to make cost-effective cyber security investment decisions because they lack widely accepted and unambiguous metrics for decision support. ISA99 in cooperation with ISA100 (wireless systems) and ISA84 (safety) is developing a set of system level metrics related to the security assurance levels described in H.1. These System Security Compliance Metrics will be specified in ISA-99.03.03[21].

For their standard, ISA99 is currently tailoring the security metrics offered by The Center for Internet Security (CIS)[33]. Changes include the modifications needed to specify metrics in the context of an Industrial Automation Control System (IACS), extending the formulas to IACS requirements and associating the CIS metrics to IACS system security assurance level requirements. This well-defined set of standard compliance metrics will provide IEC 61850 users the following capabilities:

Clear guidance for IEC 61850 system suppliers on implementing security metrics: Practical definitions of security metrics based on data most protection and automation engineers are already collecting. This will make it easier, faster and cheaper to implement a security metrics program that supports effective decision-making. Furthermore, these metrics provide a means of communicating security performance and can be used to guide resource allocation, identify best practices, improve risk management effectiveness and demonstrate compliance.

Define a security metric framework for IEC 61850 products and services: A clear set of data requirements and consensus-based metric definitions will enable IEC 61850 vendors to efficiently incorporate and enhance their security products with metrics.

Consensus-driven metrics will provide ways to for IEC 61850 vendors to demonstrate the effectiveness of their products, processes and services.

Common standards for meaningful data sharing and benchmarking: Security metric measurements will be used to calculate a uniformly meaningful benchmark among business partners and regulatory agencies. A shared security metric framework and the ability to track and compare results will standardize incident reporting, leading to best practice identification and improvements in overall cyber security practices.

I Is IEC 61850 security cost and testing affordable?

Impacts of cyber security on substation protection and automation are both general to any IP/Ethernet-based communication network and specific to IEC 61850 networks. In the context of IEC 61850 architecture, this chapter describes the need for defense-in-depth, security costs and benefits that influence return on investment (ROI), and the need for adequate security testing.

The question on the table is “Is IEC 61850 security cost and testing affordable?” To address this question, WG B5.38 first examined the need for defense-in-depth security. Given this insight WG B5.38 then turned their attention to major cost drivers and questions regarding return on security investment (ROI). Lastly, security testing was addressed.

I.1 IEC 61850 systems need defense-in-depth security

In a generic sense, IEC 61850 systems need defense-in-depth security that can be achieved through the accumulation of security barriers installed at each level of the substation automation system: remote control center, remote maintenance center, substation level, bay level and the process level. Each IEC 61850 level includes IEDs for which some level of security is expected for the operating system and applications to provide OS hardening, denial of service detection, patch management, anti-virus, application authentication, role-based access control, etc.

When an IED is not implanting the required level of security due to process capability limitations, cost or other factors, then a proxy device is needed to provide security. Such a proxy would be in charge of a series of IEDs and be located at any level in the IEC 61850 architecture depending on the vulnerability assessment performed by the utility.

A certificate server is needed for authentication. It seems logical that management of these certificates by a certificate authority be established at the regional grid level.

Remote downloading of patches, at least for OS security and possibly for application (software, configuration database or setting) also needs a secure communication infrastructure.

At the system level, some security objects defined in IEC 62351-7 [45] need to be carefully monitored and supervised and retrieved by any communication protocol.

Figure 7 shows a very simplified view of the logical associations between an IED enabled with security mechanisms and the rest of the environment (within and outside of the substation).

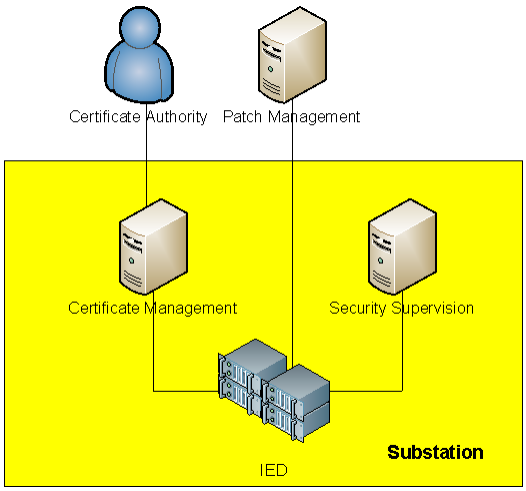


Figure 7 Logical associations between IED and security subsystems

Redundant storage, whether for archive, software, configuration database or settings is a good idea for many recovery and continuity of business reasons, including security. The risk is not only to backup IEC 61850 IEDs, but to enhance defense-in-depth through diversity by providing the means to reach to the telecontrol through an indirect route. The defense architecture depends on the speed and quality of service of this redundant communication path; for example, a slow telecom network connected by modem simply should provide a callback function while high-speed Ethernet requires a firewall.

I.2 Potential cost impacts need attention

GOOSE and SMV are really specific to IEC 61850, with multicast and hard real time data flow requirements; e.g., the famous ¼ cycle state change message called GOOSE. Furthermore, the consequences of a denial of service attack could be severe because these system protection messages are mission critical. However, this is where the cost of security per IED is likely to be significant due to their computational requirements. IEC 62351-6 (IEC TC57WG15, January 2007) was particularly sensitive to these issues.

I.3 The bad news: Return on Investment (RoI) is difficult to estimate

The cost to implement security in a specific project is relatively easy to identify. However apart from these costs, there are significant ongoing operational and costs, particularly those needed for secure communication outside the substation. For example, patch management is a particularly high maintenance cost endeavor. Hence it is difficult to accurately identify the ROI

with an ill-defined life-cycle cost that is subject to a multitude of outside influences – particularly those related to patch management.

I.4 More bad news: Benefits are even harder to estimate

Because the frequency and gravity of cyber attacks is either unknown or not well defined, benefits are very hard to quantify. Experience shows that viruses on Windows operating systems represent common problems with two root causes.

1. Operator access: first for updating software, storing archives, etc., some customers have reported operators installing games to play.
2. Connection of the substation automation system with process automation systems in industrial plants resulting in widespread dissemination of viruses over the common network.

As the number of IEDs connected to IEC 61850 networks expand and new functionality is added, if nothing is done widespread dissemination of viruses will only get worse. According to Metcalfe's law, the number of exchanges grows with the square of the elements connected to a communication network.

I.5 At last some good news: security has some measurable benefits

One indirect measurable benefit is the result of implementing quality security mechanisms.

Deploying truly secure access control with strong use control mechanisms will reduce the risk of incorrectly setting mission critical protection parameters in IEDs. The traditional uses of passwords (sometimes three levels of passwords) managed by the IED hardly protect anything. A utility has to manage several thousand IEDs, which results in most passwords being the same or similar, and known by everyone. Thus, some insufficiently trained operator might set a critical protection parameter.

I.6 Don't forget to adequately test security mechanisms

Some utilities are paying hackers to test their operational system for cyber vulnerabilities. This is a scary thought – what is the level of trustworthiness of these people! The tests results are kept highly confidential, which some consider a variation of the "security by obscurity" motto. The lack of feedback to the IED vendors to correct flaws that can be exploited is a concern. If "hackers" are used, this should only be undertaken after a complete and thorough security credential review of their organization and staff is completed.

Self-assessment testing methodologies and tools are emerging. Two sources for this information are:

http://www.us-cert.gov/control_systems/index.html
http://www.wurldtech.com/library/pdf/WST_Achilles_Overview.pdf

These tools are said to run millions of tests for generic TCP/IP protocols and may be good candidates for testing IEC 61850 stacks.

J Utility executive's view of security management

Utility executives have not been silent on the issue of security. They have stated over-and-over again that security must be cost-effective, and to this end they do not want stovepipe solutions. They want a coherent security policy that can be enforced. For this reason WG B5.38 included in their assessment of solutions in this report.

J.1 Results of the Newton-Evans international survey

Newton-Evans included in their worldwide survey of market trends on adoption of control center security measures and use/plans for IEC 61850 implementation several questions that helped guide WG B5.38 assessments (Newton-Evans, May 2008). The response captured how the utility executives viewed the threats and prioritized the need for comprehensive security solutions.

J.1.1 North American approaches used for reducing vulnerability on T&D operations networks

The top four approaches being taken today (May 2008) by North American electric power utilities in an attempt to reduce cyber vulnerabilities include: 1) password protection (92%); 2) firewalls and DMZ between control center-based systems and the enterprise LAN (84%); 3) VPN use (virtual private network) now established by 80% and 4) advanced virus protection software (75%). Three of these represent significant increases from the percentages reported (below) in the 2005 study, which themselves were significant measurable increases taken by operators of control centers since the 2003 study.

In most categories among the 24 listed on the survey, Independent Owned Utilities (IOUs) were more likely to have implemented additional vulnerability reduction measures by a wide margin over their counterparts in public power, cooperatives or those reported among the Canadian utilities.

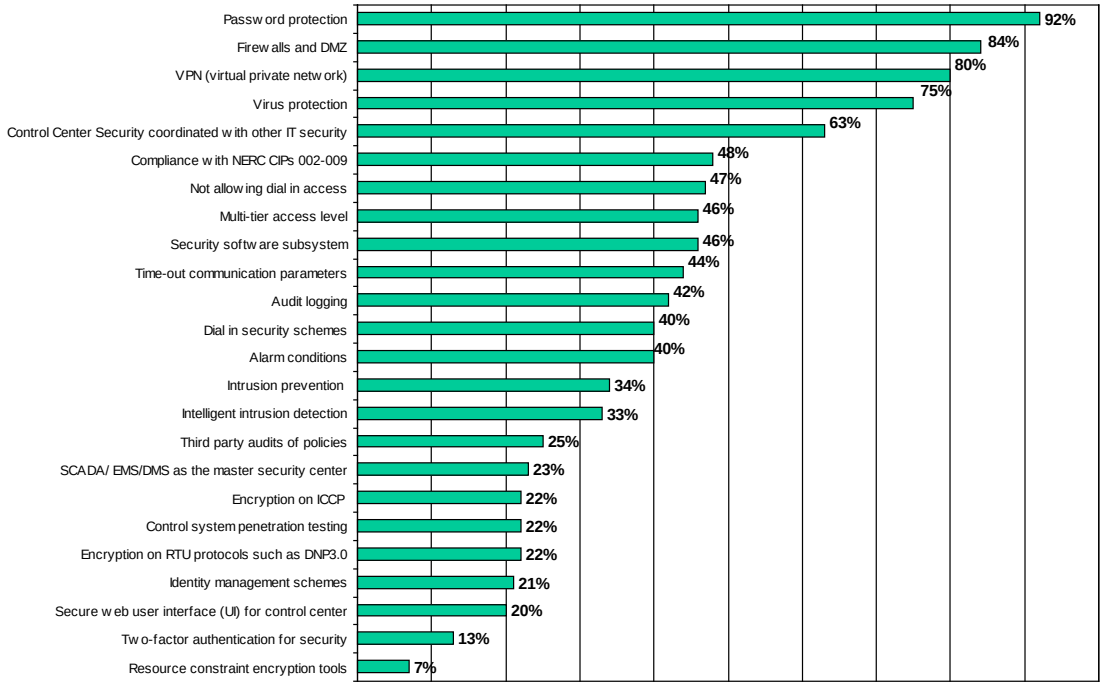
Some interesting exceptions included many public power utilities disallowing any remote dial in to the control center systems; almost all cooperative utilities adopting at least password protected access and being more likely to use their SCADA as the master security center for substation IEDs requiring additional passwords. Canadian utilities were stronger adopters of ICCP encryption than were their US counterparts and were somewhat more likely to be protecting SCADA systems with firewalls and DMZ measures.

On a summary basis, there are more cyber protection measures being taken by North American electric utilities of all sizes and types than in any previous study over the past decade in which these measures were researched. In part, these are pure defensive strategies. In large part, we believe, the increased adoption of these measures is due to the impact of NERC CIPS compliance

requirements. If the even "stricter" (more robust) NIST cyber security guidelines being proposed for electric power cyber security become mandatory over the next two years, the subsequent Newton-Evans research study will undoubtedly find increases in the extent of adoption and in the number of sophisticated measures being utilized by North America's electric power industry infrastructure, numbering over 3,000 distinct utilities serving approximately 160 million metered customers.

Responses from the utility executives in North America are shown below.

Figure 1: North American Electric Power Utilities:
Different Approaches for
Reducing Vulnerability on Operational Networks



Newton-Evans Research Co. 04/08

J.1.2 North American utility participation with ongoing cyber security initiatives

In a related follow-on to Question 1, North American utilities were asked to indicate their awareness of, and participation in, various ongoing cyber initiatives. These included: EPRI's Enterprise Information Security Program; CERT CC (Computer Emergency Response Team Coordination Center); FIRST (Forum of Incident Response and Security Teams); TISP (The Infrastructure Security Partnership); and, NERC's (North American Electric Reliability Corporation) ES-ISAC (Electricity Sector Information Sharing and Analysis Center).

In the new 2008 study, three important new IEEE standards that are focused on control systems cyber security in the substation environment were also included in this question regarding participation in, and awareness of groups fostering cyber security measures.

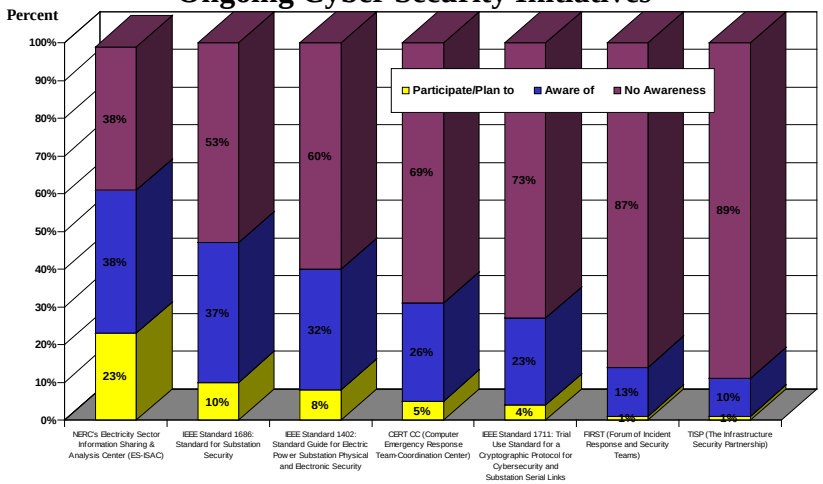
Participation in development of IEEE cyber security standards was low, consisting of some support from the IOU community, but very little from the other industry groupings. Ten percent of the respondents indicated some degree of participation with IEEE Standard 1686 (standard for substation security); only four percent cited any participation or use of IEEE Standard 1711 (Trial Use Standard for a Cryptographic Protocol for Cyber Security and Substation Serial Links); and eight percent indicated some involvement with IEEE Standard 1402 (Standard Guide for Electric Power Substation Physical and Electronic Security). Awareness of these standards ranged from 23% (for IEEE 1711) to 37% (for IEEE 1686).

Involvement with CERT CC stood at 5% (11% among IOUs), with 26% of the respondents at least aware of this organization. FIRST (Forum of Incident Response and Security Teams) and TISP (The Infrastructure Security Partnership) received minimal indications of participation or awareness by this group of utility officials. The NERC's ES-ISAC carries much more weight with this group, with nearly one quarter of the respondents indicating some participation or involvement with ES-ISAC – including one half of the IOUs. Awareness of the organization brought in another 39% of the respondents.

As observed in earlier studies, the largest utilities remain much more likely to be aware of, and involved in, cyber security initiatives than were their smaller counterparts.

A graphical representation of the results is shown below.

Figure 2
North American Electric Power Utilities:
Utility Participation with
Ongoing Cyber Security Initiatives



Newton-Evans Research Co. 04/08

J.1.3 Current and planned use of substation security measures in North America

Newton-Evans mid-2008 study findings are based on eight options responses in response to the question on substation security methods and practices. Utilities were asked to indicate whether they were using or had plans to use any of the following: encryption of RTU communications, password protection for IEDs, video camera surveillance, improved intrusion detection, secure facilities, eye/fingerprint identification, limited accessibility to substation-related keys and substation firewall.

- As late as mid-2008, only 24% of the officials from 103 utilities reported using encryption of RTU communications. They relied more on physical security measures: 85% for locked buildings and enclosures and 79% for limiting access to substation keys. 79% relied on password protection for cyber security.
- Plans for adding defense-in-depth during 2008-2010 are centered on substation firewalls (32%), improved intrusion detection (25%) and video camera surveillance (24%).

On average, each of the utilities reported implementation of four of the eight measures shown in Figure 8. Other substation security measures mentioned by the respondents include personnel background checks, monitoring substation networks, perimeter detection cameras, personnel authentication and logging, and card readers. One respondent replied that they intend to migrate to digital communications for substation data and control; use Virtual Private Network (VPN) and multilayered security controls, encrypted dial-in or LAN based access, and an enterprise security server/proxy to establish the encrypted communication link to the substation IEDs.

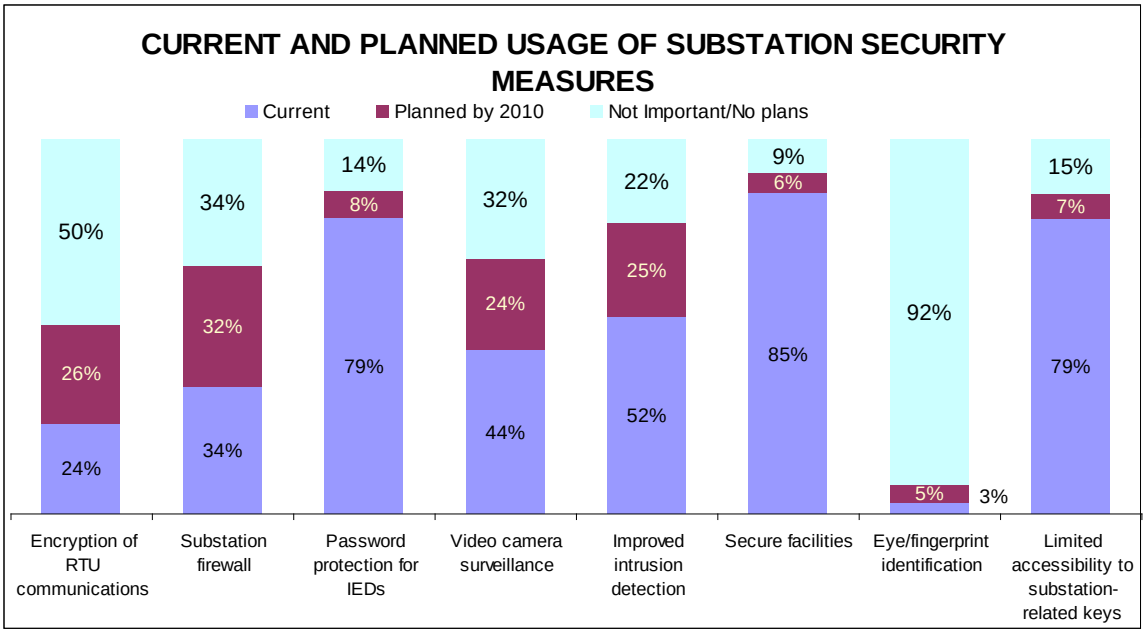


Figure 8 Mid-2008 study findings for North American utilities

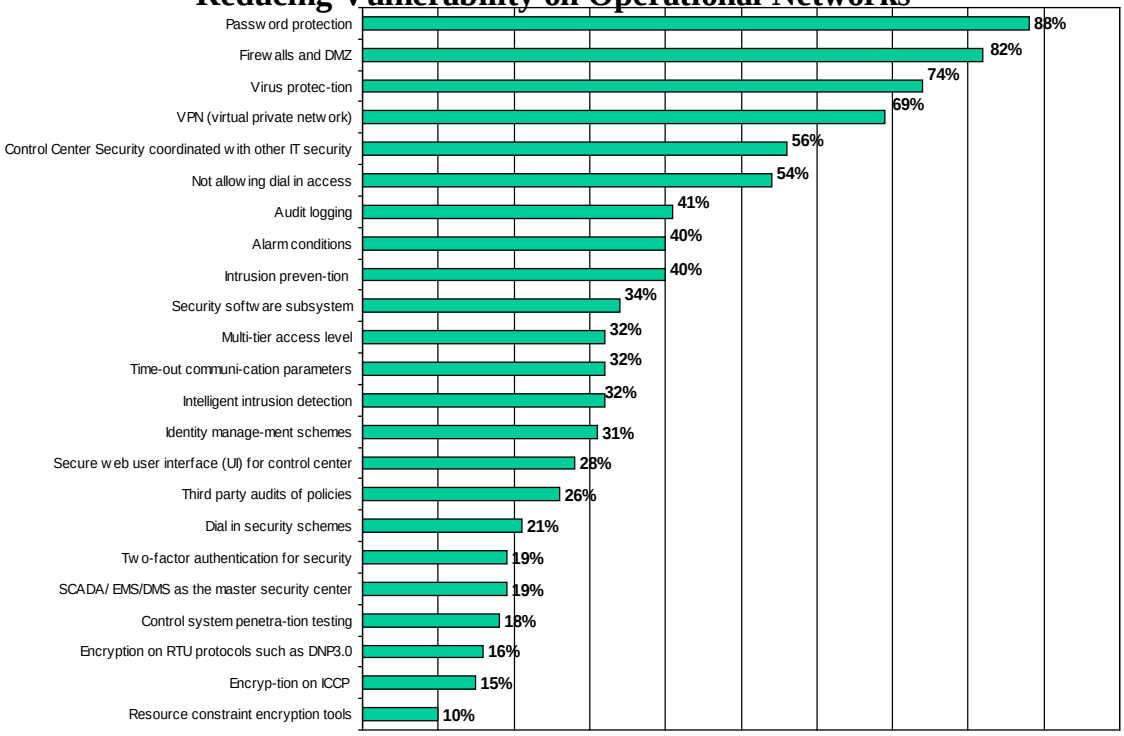
J.1.4 International utility approaches used for reducing vulnerability on T&D networks

In this large sample of major and midsize international utilities (71 surveys from 51 countries) note the subtle changes from results of prior years 2005 and 2003 regarding the multiple approaches being taken by utility managers to help reduce vulnerability of operational control systems.

The emphasis in this year's study has moved password protection into the top spot (similar to the North American study findings) followed by virus protection software. The use of VPNs, control center security efforts coordinated with IT security efforts and not allowing any dial-in access to the control center all received mentions by more than one half of this group, including most of the largest utility respondents. Interestingly the same top five measures had been adopted by North American utilities.

The graphical representation of these responses is shown below.

Figure 3:
International Utilities:
Different Approaches for
Reducing Vulnerability on Operational Networks



Newton-Evans Research Co. 04/08

J.1.5 Current and planned use of substation security measures outside North America

In the third-quarter of 2008 utility officials outside of North America responded to the eight optional questions described in Appendix J.1.3. The most frequently cited security measures currently in use included secure facilities (locked gated buildings and enclosures) mentioned by nearly 70% of the respondents. Limited access to substation keys was cited by about two-thirds of the group, while password protection for substation resident IEDs was mentioned by 58% of the respondents.

Figure 9 shows the current and planned use of substation security measures outside of North America. Plans centered on adding substation firewalls and video camera surveillance over the 2008-2010 time period.

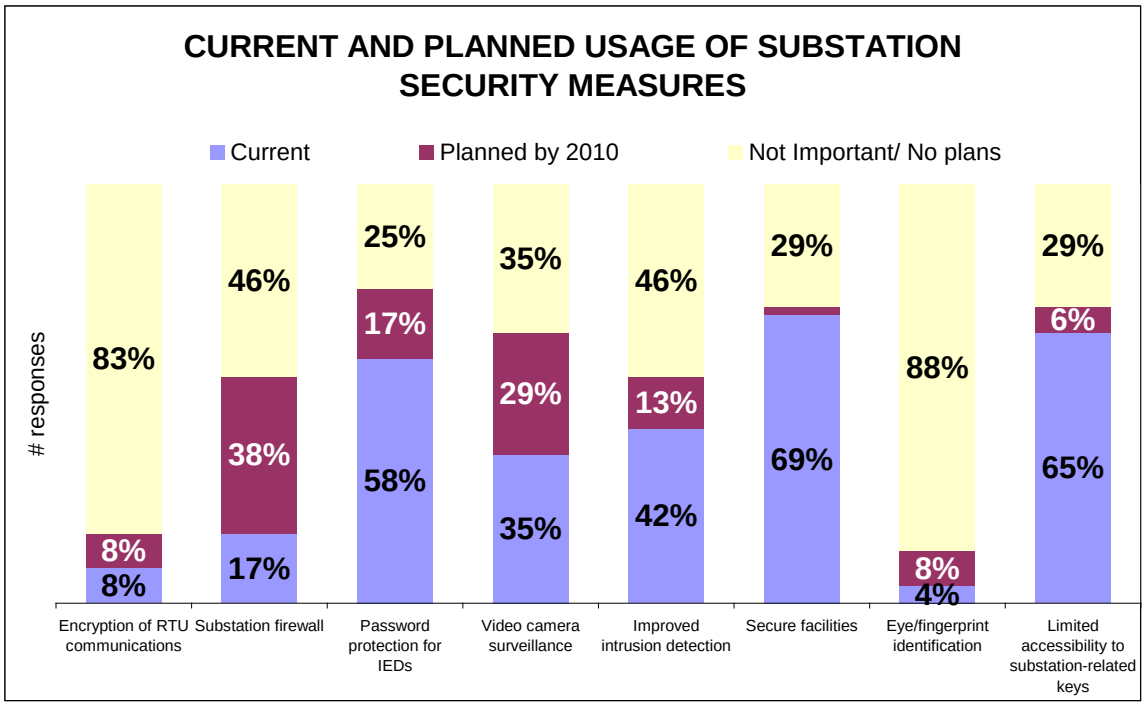


Figure 9 Current and planned use of security measures outside of North America

J.2 Who is responsible for implementing IEC 61850 security?

As usual, WG B5.38 discovered several conflicted answers to the question "who is responsible for implementing IEC 61850 security – vendor or utility?"

- Clearly, the utility should design and state requirements for security as a part of their procurement specification.
- It is the responsibility of the vendor (system supplier or system integrator) to implement security functionality that can be enabled when the IEC 61850 system is commissioned.
- Given the possibility to interconnect networks (including IEC 61850 networks), the utility should procure and manage security functions and devices to ensure the security of the IEC 61850 network. Special attention should be given to the following:
    - Ways of identifying entities and rejecting data packets from entities that are not on utility's approved list.
    - Specify a level of robustness (security assurance level – see Appendix H) of IEC 61850 IED operating systems, firmware, etc. so that devices and networks cannot be easily compromised.
    - Consider the use of VLAN (virtual local area network) tagging so that a local network can be configured with VLANs.
    - Provide strong access control, such as two-factor authentication, roles and permissions, password management or remote authentication (e.g., RADIUS server).

Each action listed requires TC57WG10 to address in the IEC 61850 standard modifications with normative specifications to ensure the interoperability of the needed security functions. WG B5.38 analysis reached the following conclusions:

- Securing an IEC 61850 substation protection and automation system is primarily the responsibility of the utility with possible support from system manufacturers and system integrators to provide information on the system architecture and capability.
- In order to provide the infrastructure to enable local access, the most cost effective approach is to combine with the business infrastructure.
- Access identification and control is necessary for both systems, but there is also a need to ensure either network cannot be maliciously compromised.
- Local access security is necessary to ensure that user access activity can be controlled and logged.

J.3 Should the IEC 61850 system be kept on a closed network?

The simple answer is NO! Remote access should be provided. In the past, substation automation systems have generally been an isolated domain with little exposure outside the substation fence. However the increasing requirement to remotely operate and maintain these systems has resulted in deployment of standardized (open) communication systems. Two essential aspects must be included in the deployment of IEC 61850 systems.

- The IEC 61850 substation LAN should be remotely accessible, but security mechanisms are needed to satisfy the seven foundational requirements.
- The security assurance level needed must be defined by the utility – see Appendix H.

J.4 What security measures are needed for local access?

Given the need for remote access to the IEC 61850 substation protection and automation system, there is no question that a high-level security assurance must be implemented. However, for local access to the physically secured substation, the requirements for high-level security assurance measures are more complex and in some cases conflicting.

- Some utilities want local security with the substation to be as high as possible while still being user friendly for local operation and maintenance. Other utilities were ambivalent, and are waiting for some guidance from government or regulators.
- The vendor community favors strong access and use control measures for local operation and maintenance. Coupled with the necessary defense-in-depth cyber security controls, management should enforce a locked cubicle policy to prevent ad hoc physical access without authorization.

WG B5.38 concluded that a high-level security assurance is required for local access.

J.5 Research initiatives favored by utility management

The National Grid UK contributed their view of the research initiatives needed to achieve the desired level of security assurance.

J.5.1 National Grid's vision

In order to facilitate ongoing R&D projects, there is a need for R&D establishments to remotely connect to substation data collection and information systems using computer-based software applications. This requirement is to enable information to be downloaded for analysis and integration into systems developed through their R&D projects. The sources of information are likely to incorporate operational systems that are used to control the substation or protect HV systems infrastructure or systems that perform a monitoring function only. As control and protection systems are critical to the reliability of the transmission system, connection to these sources require users to be identified and authenticated in order to maintain security levels. To ensure security is maintained, it is desirable to apply a consistent solution regardless of the level of security required by the data collection and information system.

J.5.2 Connection by almost any means is desired

National Grid, UK, proposes to enable a suitable system to be evaluated on a limited basis where remote access to systems is required. The proposed method would be to facilitate these users to connect using a number of different connection types; e.g., the National Grid Corporate LAN via the Internet using broadband communications, General Packet Radio Service (GPRS), Global System for Mobile communications (GSM), and dialup connections. The preferred connection is the National Grid Corporate LAN, and this will provide an additional layer of security in the form of identification and authorization.

A standalone system is required to enable other connection types to be secure, and it would be wise to consider a method of securing these connections that utilizes the following:

- Authenticate each individual user using a token and passkey that is authorized by a gateway system.
- Only allow authenticated users to connect to systems for which they have been pre-authorized.
- Ensure that the connection between authenticated user and the data collection system is protected to prevent intrusion, information capture, replaying of captured events and viewing of information while the connection is in progress.
- Prevent authenticated users from using the target data collection and information system as platforms to gain access to other areas on the network.

A well designed token and passkey scheme should include a random and individual code to be generated that will allow a user remote access for the current session only. Each remote access session should generate a new code.

Once a user has been authenticated, access to individual IEDs should be limited on a per user or per user group basis. Such a limit should be designed so that user access is granted only to IEDs or systems for which they have been granted permission to access. It is probably best to grant access to these IEDs by a request to a central remote access management operator. Furthermore, no access to any device should be the default position for all users until permission has been requested and granted.

To strengthen security, the system implemented should be designed so as to prevent target IEDs and systems connecting to each other unless the remote access management operator has granted permission. This will prevent systems that are accidentally infected from passing on malicious software components or causing network overloads.

Details relating to user access should be logged, and each log should include the user ID, times and dates of each access attempt and the IEDs that they are remotely accessing.

J.6 Leveraging authorization from effective identity management

IEC 61850 systems require human interaction at all stages of the life cycle. Utilities would be wise to include effective identity management (IM) requirements in their procurement specifications via the process defined in FIPS 201 [28]. The utility should clearly state in their procurement specification the following requirements:

- Administration of IM should not require modification of existing infrastructure and specialized training of existing staff.
- SmartCard should be designed with sufficient memory to contain appropriate security attributes to support multiple applications and organizational units including utility partners, suppliers, and internal organizational units.
- SmartCard should provide cryptographic data separation at the object level owned by each IEC 61850 application uniquely.

Figure 10 shows an example of a common framework for identity proofing, issuance and verification. To mitigate the risk of a person using a stolen or loss card, access and use control should include a minimum of two factor authentication. For example, after swiping (or reading the SmartCard) the user must enter a Private Identification Number (PIN).

Figure 10 Example of a common framework for identity verification

Using such a SmartCard has several advantages:

- It creates a comprehensive interface between all entities that have access to IEC 61850 system hardware, software and data.
- It provides a consistent identity establishment process that the utility can enforce with its partners, suppliers and all internal organizational units, and with regulators and other government oversight organizations.

The goal of identity assignment is to ensure that resources are only accessed by the appropriate personnel and that personnel are correctly identified. The first step is to create access control lists with access privileges for personnel. The next step is to implement security mechanisms to enforce the access control lists. Mechanisms also need monitor access activities for inappropriate activity. The access control lists need to be managed through adding altering and removing access rights as necessary.

J.6.1 Identity assignment and authentication policy and procedures are required

In accordance with NERC CIP requirements, see Appendix D, WG B5.38 assumes that the responsible organization develops, disseminates and periodically updates the following:

- A formal, documented, identity assignment and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among all appropriate organizational entities, and compliance.
- Formal, documented procedures to facilitate the implementation of the identity assignment and authentication policy and associated access controls.
- Identity assignment and authentication policy and procedures consistent with applicable laws, directives, policies, regulations, standards and guidance:

    - The identity assignment and authentication policy can be included as part of the general information security policy for the organization.
    - Identity assignment and authentication policy procedures can be developed for the security program in general, and for a particular control system, when required.

J.6.2 IEC 61850 supports the need to effectively implement identity schemes

IEC 61850 supports the need to effectively implement appropriate identity schemes for mission critical operations (e.g., configuration changes that could reduce the effectiveness of a protection scheme, select-fefore-operate commands to open a breaker). Specifically, Part 6 provides in SCSM (Specific Communication Service Mapping) the optional feature for authentication.

IEC 61850-8-1 states for two-party association that the ACSI model is mapped to the MMS Environment specified in ISO/IEC 9506-1. From the ACSI model, associationID is used in Part 8-1. Assuming the option is implemented, associationID is a local issue that must be included in the negotiated parameters:

- Client establishes association with the required parameters in the association request. MMS can use the password for identify clients during the MMS-Environment establishment:
    - MMS allows the inclusion of passwords composed by an ASN.1 string with information identifying the client in the negotiation process.
    - IEC 62351-4 recommends using digital signatures and certificates as authentication information to be included in the association request if authentication is required.
- User authentication can be turned on and off in MMS:
    - If password or certificate-based authentication is used, the client adds this to the association request message.
    - Server checks whether this client has the right to connect, and if so it stores the Client information for future use. For example, to check whether this client has the privilege to perform a control operation.
- In peer-to-peer communication, user authentication is not used because the association between IEDs is established during the system configuration phase and the data publisher is recognized with different address fields.

Future editions of IEC 61850 will refer to the security mechanisms recommended in IEC 62351.

K Other related work in progress

WG B5.38 selected specific cyber security standards, reports and technical materials for their work. Other related work is in progress and future CIGRE working groups should consider their contributions. Table 15 describes this work as understood by WG B5.38 at the time of writing this technical brochure. Each entry in the table identifies the venue or sponsor for the work, the topic of discussion, a point of contact with an email address, and a description of the scope of work.

Table 15 Other related cyber security work-in-progress

Venue/Sponsor	*Topic of Discussion*	*Point of Contact*	*Scope/Remarks*
IEEE	Task Force on Cyber Security of Power Systems	Manimaran Bovindarasu gmani@iastate.edu	Advance the state-of-the-art research and education in modeling, algorithms and analysis. Develop an integrated taxonomy of faults and attacks on SCADA control systems.
IEEE/PSRC	WG H13 on Cyber Security for Protective Relaying	Steve Kunsman steven.a.kunsman@us.abb.com	Develop a guide for implementing cyber security for protective relaying.
NERC	Task Force to rewrite the CIP 002-009 standards	Keith Stouffer keith.stouffer@nist.gov	Strengthen CIP 002-009 standards to address issues raised by FERC.
UCA International	User Group supporting development and extensions of IEC 61850	Kay Clinard kay@kcassociates.biz	Develop technical issues and position papers to support IEC 61850 development.
US DHS	Recommended Practice – Control System Network Cryptography	DHS National Cyber Security Division, Control Systems Security Program	Addresses the use of cryptographic technology within critical control systems.
US DOE	SmartGrid Architecture	Keith Stouffer keith.stouffer@nist.gov	Multiple working groups formed to address all SmartGrid technical issues.
US DOE & DHS	National SCADA Testbed Program	Henry Kenchington henry.kenchington@hq.DOE.gov	Develop a government baseline to assess cyber security requirements for selected critical infrastructure sectors.