

IEC TC57 WG15: Security Standards for the Power System's Information Infrastructure – IEC 62351 Standards

By Frances Cleveland, Xanthus Consulting International

Dual Infrastructures: the Power System and the Information System

In the power industry, the focus has been almost exclusively on implementing equipment that can keep the power system reliable. Until recently, communications and information flows have been considered of peripheral importance. However, increasingly the Information Infrastructure that supports the monitoring and control of the power system has come to be critical to the reliability of the power system. With the exception of the initial power equipment problems in the August 14, 2003 blackout, the on-going and cascading failures were almost exclusively due to problems in providing the right information to the right place within the right time.



Figure 1: August 14, 2003 Blackout (NOAA processed the data from the Defense Meteorological Satellite Program. Please credit NOAA/DMSPP)

Communication protocols are one of the most critical parts of power system operations, responsible for retrieving information from field equipment and, vice versa, for sending control commands. Despite their key function, to-date these communication protocols have rarely incorporated any security measures, including security against inadvertent errors, power system equipment malfunctions, communications equipment failures, or deliberate sabotage. Since these protocols were very specialized, “Security by Obscurity” has been the primary approach. After all, only operators are allowed to control breakers from highly protected control center. Who could possibly care about the megawatts on a line, or have the knowledge of how to read the idiosyncratic bits and bytes the appropriate one-out-of-a-hundred communication protocols. And why would anyone want to disrupt power systems?

However, security by obscurity is no longer a valid concept. In particular, the electricity market is pressuring market participants to gain any edge they can. A tiny amount of information can turn a losing bid into a winning bid – or withholding that information from your competitor can make their winning bid into a losing bid. And the desire to disrupt power system operations can stem from simple teenager bravado to competitive game-playing in the electrical marketplace to actual terrorism.

It is not only the market forces that are making security crucial. The sheer complexity of operating a power system has increased over the years, making equipment failures and operational mistakes more likely and their impact greater in scope and cost. In addition, the older, “obscure” communications protocols are being replaced by standardized, well-documented protocols that are more susceptible to hackers and industrial spies.

As the power industry relies increasingly on information to operate the power system, two infrastructures must now be managed: not only the **Power System Infrastructure**, but also the **Information Infrastructure**. The management of the power system infrastructure has become reliant on the information infrastructure as automation continues to replace manual operations, as market forces demand more accurate and timely information, and as the power system equipment ages. The reliability of the power system is increasingly affected by any problems that the information infrastructure might suffer, and therefore **the information infrastructure must be managed to the level of reliability needed to provide the required reliability of the power system infrastructure.**

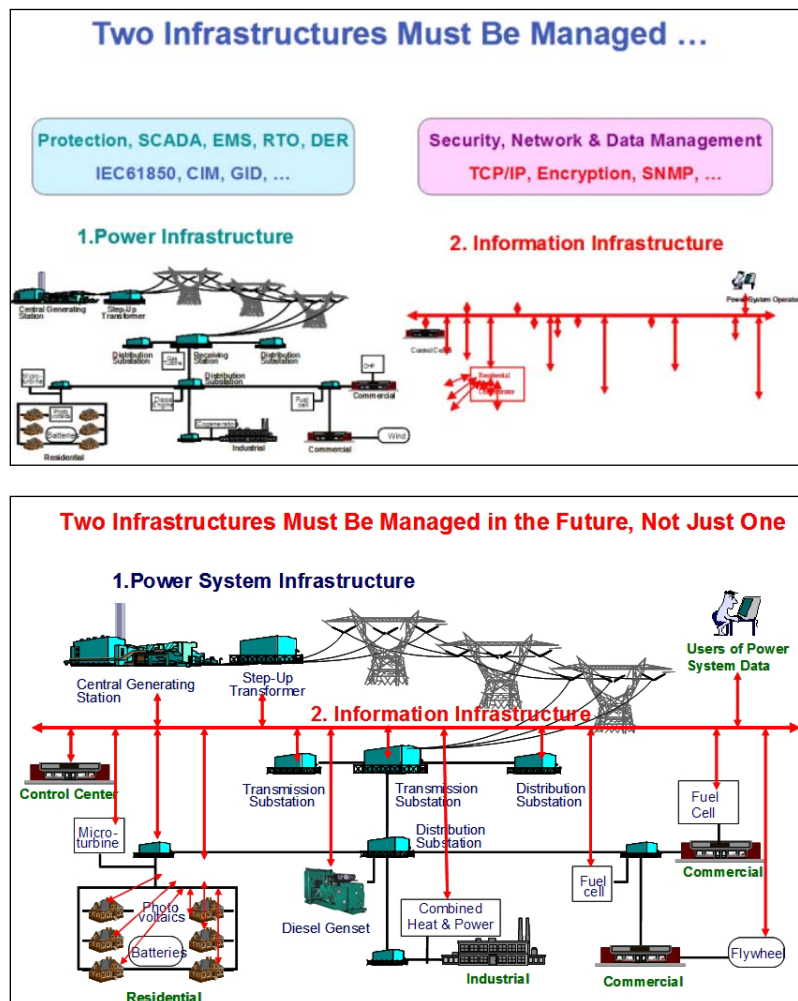


Figure 2: Two Infrastructures Must Be Managed, Not Just One

IEC TC57 as Developer of International Standards for SCADA Protocols

The International Electrotechnical Commission (IEC) Technical Council (TC) 57 **Power Systems Management And Associated Information Exchange** is responsible for developing international standards for power system data communications protocols. Its scope is “*To prepare international standards for power systems control equipment and systems including EMS (Energy Management Systems), SCADA (Supervisory Control And Data Acquisition), distribution automation, teleprotection, and associated information exchange for real-time and non-real-time information, used in the planning, operation and maintenance of power systems. Power systems management comprises control within control centres, substations, and individual pieces of primary equipment including telecontrol and interfaces to equipment, systems, and databases, which may be outside the scope of TC 57. The special conditions in a high voltage environment have to be taken into consideration.*”

IEC TC57 has developed three widely accepted protocols, and has been the source of a fourth. These protocols are:

- **IEC 60870-5** which is widely used in Europe and other non-US countries for SCADA system to RTU data communications. It is used both in serial links (Part 101) and over networks (Part 104).
- **DNP 3.0** which was derived from IEC 60870-5 and is in use in the US and now is widely used in many other countries as well, primarily for SCADA system to RTU data communications
- **IEC 60870-6 (also known as TASE.2 or IEC 61850)** which is used internationally for communications between control centers and often for communications between SCADA systems and other engineering systems within control centers.
- **IEC 61850** which is used for protective relaying, substation automation, distribution automation, power quality, distributed energy resources, substation to control center, and other power industry operational functions. It includes profiles to meet the ultra fast response times of protective relaying and for the sampling of measured values, as well as profiles focused on the monitoring and control of substation and field equipment.
- **IEC 61334 (DLMS)** which is used for retrieving metering information and managing meter settings.

All together, these international standards account for close to 90% of the data communications protocols in newly implemented and upgraded power industry SCADA systems and substation automation (Modbus, Fieldbus, and other proprietary protocols are still used in older systems and in other industries).

Security Concepts

Security Threats

Security entails a much larger scope than just the authentication of users and the encryption of communication protocols. End-to-end security involves security policies, access control

mechanisms, key management, audit logs, and other critical infrastructure protection issues. It also entails securing the information infrastructure itself.

Security threats include:

1. Inadvertent Threats
 - Safety Failures
 - Equipment Failures
 - Carelessness
 - Natural Disasters
2. Deliberate Threats
 - Disgruntled Employee
 - Industrial Espionage
 - Vandalism
 - Cyber Hackers
 - Viruses and Worms
 - Theft
 - Terrorism

The key point is that the overall security of power system operations is threatened not only by deliberate acts of espionage or terrorism but by many other, sometimes deliberate, sometimes inadvertent threats that can ultimately have more devastating consequences than direct espionage.

Security Purposes

The purposes for security protection are often described as 5 layers, with security measures addressing one or more of these layers:

- **Deterrence and delay**, to try to avoid attacks or at least delay them long enough for counter actions to be undertaken. This is the primary defense, but should not be viewed as the only defense.
- **Detection of attacks**, primarily those that were not deterred, but could include attempts at attacks. Detection is crucial to any other security measures since if an attack is not recognized, little can be done to prevent it. Intrusion detection capabilities can play a large role in this effort.
- **Assessment of attacks**, to determine the nature and severity of the attack. For instance, is the entry of a number of wrong passwords just someone forgetting or is it a deliberate attempt by an attacker to guess some likely passwords.

- **Communication and notification**, so that the appropriate authorities and/or computer systems can be made aware of the security attack in a timely manner. Network and system management can play a large role in this effort.
- **Response to attacks**, which includes actions by the appropriate authorities and computer systems to mitigate the effect of the attack in a timely manner. This response can then deter or delay a subsequent attack.

Security Issues

Security is an issue that several industries and most businesses are attempting to come to terms with. However, the implementation of a robust security infrastructure often appears to be a daunting and overwhelming task. This can be attributed to several factors:

There is no defined mechanism to decompose the security problem space and therefore it is perceived to be an impossible task.

Typically there are two major discussion/analysis methods in regards to security: Enterprise based analysis and/or Technology/Threat based analysis. There are obvious pitfalls to both approaches. The instantiation of an Enterprise is continuously evolving/changing and may encompass more than one business entity where a single set of security policies and technologies cannot be enforced. Thus any security decisions require a large amount of coordination and tend to make the security process frustrating.

However, the security problem can be decomposed into smaller regions of security analysis/management. This is the “Security Domain” concept that allows a set of resources to be managed (from a security perspective) independently. However, this raises the issue of how to provide a security mechanism for inter-domain exchanges. To solve this issue, the appendix introduces several abstract security services that may be bound to different security technologies.

The technology only based analysis approach could be classified as flawed from the outset. Since security is an ongoing and evolving process, selection of security based upon today’s technology may prevent adopting more advanced security technologies in the future. This appendix introduces a set of abstract security services that can be mapped to current or future technologies, in order to resolve this analysis dilemma.

There may be a lack of understanding in regards to the importance of a security policy and a commitment to implement that policy.

The first problem that is typically encountered is that Enterprise policy development is overwhelming. However, the use of the Security Domain concept should help mitigate this issue. Nonetheless, the use of the Security Domain concept means that the domains need to be identified and then the policy needs to be developed for the domains.

The second issue is there is typically a lack of understanding of what constitutes a security policy. In particular, the policy must address the entire suite of security processes, security functions, security services, and security management.

The third issue, and typically most daunting, is how to decide what needs to be secured within the security policy. Some contend that every asset needs to be secured. However, this approach

makes security deployment/adoption costly and could prevent entities from even attempting to deploy security.

Therefore, **all assets do not need to be secured**, although all assets *could* be secured. However, **all assets should be analyzed in regards to the need of security**.

Thus the issue is raised of the type of analysis that should be performed. This appendix recommends that a risk assessment approach to the analysis be taken. The appendix discusses risk analysis at a high level and then references emerging work regarding risk assessment are given instead of embedding the intellectual content.

Therefore, Security Policies are a key security service that should be performed in advance of any security deployment. This is discussed in greater detail under the Technical Analysis of Security.

There has been no authoritative work in regards to defining abstract security services.

Many books, articles, groups, and internet sites discuss security at various levels and depths. EPRI's IntelliGrid Architecture (<http://IntelliGrid.info>) defines several abstract security services that are relevant to implementing inter-domain and intra-domain security. However, that discussion also identifies that some of the abstract services have no deployment technologies that can be used to implement the security service, although it does attempt to define what emerging standards could be used/modified in order to allow the security service to actually be instantiated.

There is typically a lack of understanding in regards to the impact of security measures on the communication requirements of power system operations.

The security services/technologies have been developed for industries that do not have many of the strict performance and reliability communications requirements that are needed by power system operations.

Security Processes

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

- Need for greater levels of integration with a variety of business entities
- Increased use of open systems based infrastructures that will comprise the future energy system
- The need for appropriate integration of existing or “legacy” systems with future systems
- Growing sophistication and complexity of integrated distributed computing systems
- Growing sophistication and threats from hostile communities

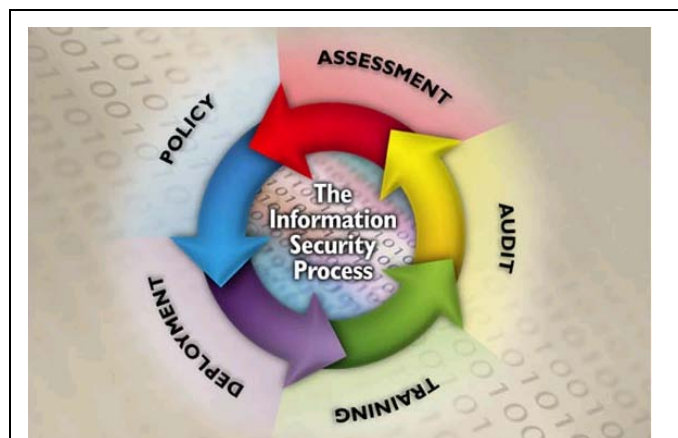


Figure 3: General Security Process – Continuous Cycle

Security must be planned and designed into systems from the start. Security functions are integral to the designs of systems. Planning for security, in advance of deployment, will provide a more complete and cost effective solution. Additionally, advanced planning will ensure that security services are supportable (may be cost prohibitive to retrofit into non-planned environments). This means that security needs to be addressed at all levels of the architecture.

As shown in Figure 3, security is an ever evolving process and is not static. It takes continual work and education to help the security processes keep up with the demands that will be placed on the systems. Security will continue to be a race between corporate security policies/security infrastructure and hostile entities. The security processes and systems will continue to evolve in the future. By definition there are no communication connected systems that are 100% secure. There will be always be residual risks that must be taken into account and managed. Thus, in order to maintain security, constant vigilance and monitoring are needed as well as adaptation to changes in the overall environment.

The process depicts five high level processes that are needed as part of a robust security strategy. Although circular in nature, there is a definite order to the process:

Security Assessment – Security assessment is the process of assessing assets for their security requirements, based on probable risks of attack, liability related to successful attacks, and costs for ameliorating the risks and liabilities. The recommendations stemming from the security requirements analysis leads to the creation of security policies, the procurement of security-related products and services, and the implementation of security procedures.

The implication of the circular process is that a security re-assessment is required periodically. The re-evaluation period needs to be prescribed for periodic review via policy. However, the policy needs to continuously evaluate the technological and political changes that may require immediate re-assessment.

Security Policy – Security policy generation is the process of creating policies on managing, implementing, and deploying security within a Security Domain. The recommendations produced by security assessment are reviewed, and policies are developed to ensure that the security recommendations are implemented and maintained over time.

Security Deployment – Security deployment is a combination of purchasing and installing security products and services as well as the implementation of the security policies and procedures developed during the security policy process. As part of the deployment aspect of the Security Policies, management procedures need to be implemented that allow intrusion detection and audit capabilities, to name a few.

Security Training – Continuous training on security threats, security technologies, corporate and legal policies that impact security, Security measures analysis is a periodic, and best

practices is needed. It is this training in the security process that will allow the security infrastructure to evolve.

Security Audit (Monitoring) – Security audit is the process responsible for the detection of security attacks, detection of security breaches, and the performance assessment of the installed security infrastructure. However, the concept of an audit is typically applied to post-event/incursion. The Security Domain model, as with active security infrastructures, requires constant monitoring. Thus the audit process needs to be enhanced.

When attempting to evaluate the security process on an enterprise basis, it is impossible to account for all of the business entities, politics, and technological choices that could be chosen by the various entities that aggregate into the enterprise. Thus to discuss security on an enterprise level is often a daunting task that may never come to closure. In order to simplify the discussion, allow for various entities to control their own resources, and to enable the discussion to focus on the important aspects, security will be discussed in regards to Security Domains.

Security Requirements, Threats, Attacks, and Countermeasures

Security Requirements and Threats

Users, whether they are people or software applications, have zero or more of four basic security requirements, which protect them from four basic threats:

- Confidentiality – preventing the unauthorized access to information
- Integrity – preventing the unauthorized modification or theft of information
- Availability – preventing the denial of service and ensuring authorized access to information
- Non-Repudiation/Accountability – preventing the denial of an action that took place or the claim of an action that did not take place.

Security Attacks

The threats can be realized by many different types of attacks, some of which are illustrated in Figure 4. As can be seen, the same type of attack can often be involved in different security threats. This web of potential attacks means that there is not just one method of meeting a particular security requirement: each of the types of attacks that presents a specific threat needs to be countered.

Security Needs vs. Threats and Attacks

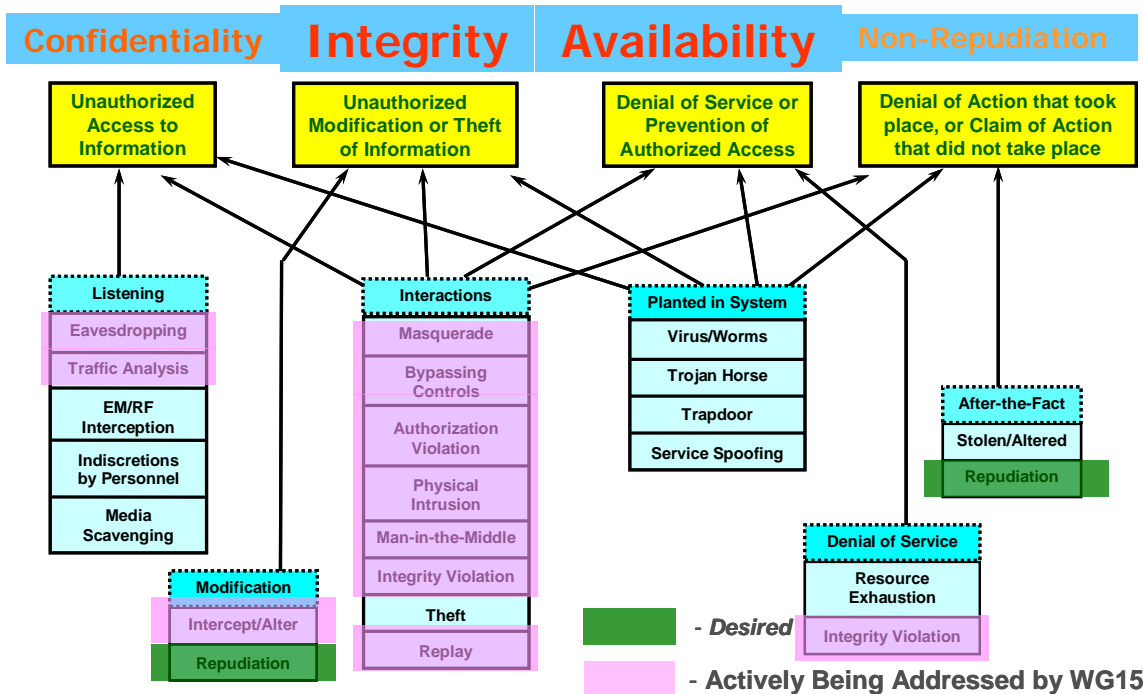


Figure 4: Security Requirements, Threats, and Possible Attacks, indicating those being addressed by WG15

Security Countermeasures

Security countermeasures, as illustrated in Figure 5, are also a mesh of interrelated technologies and policies. Not all security countermeasures are needed or desired all of the time for all systems: this would be vast overkill and would tend to make the entire system unusable or very slow. Therefore, the first step is to identify which countermeasures are beneficial to meet which needs. These breakdowns are illustrated in Figure 6, Figure 7, Figure 8, and Figure 9.

In these figures, the four security requirements (confidentiality, integrity, availability, and non-repudiation) are shown in red words. The security threats are shown with a yellow background. The key security services and technologies used to counter the threats are shown in purple and tan, while security management items are shown in blue. Security policy is shown in green.

Security Requirements, Threats, Countermeasures, and Management

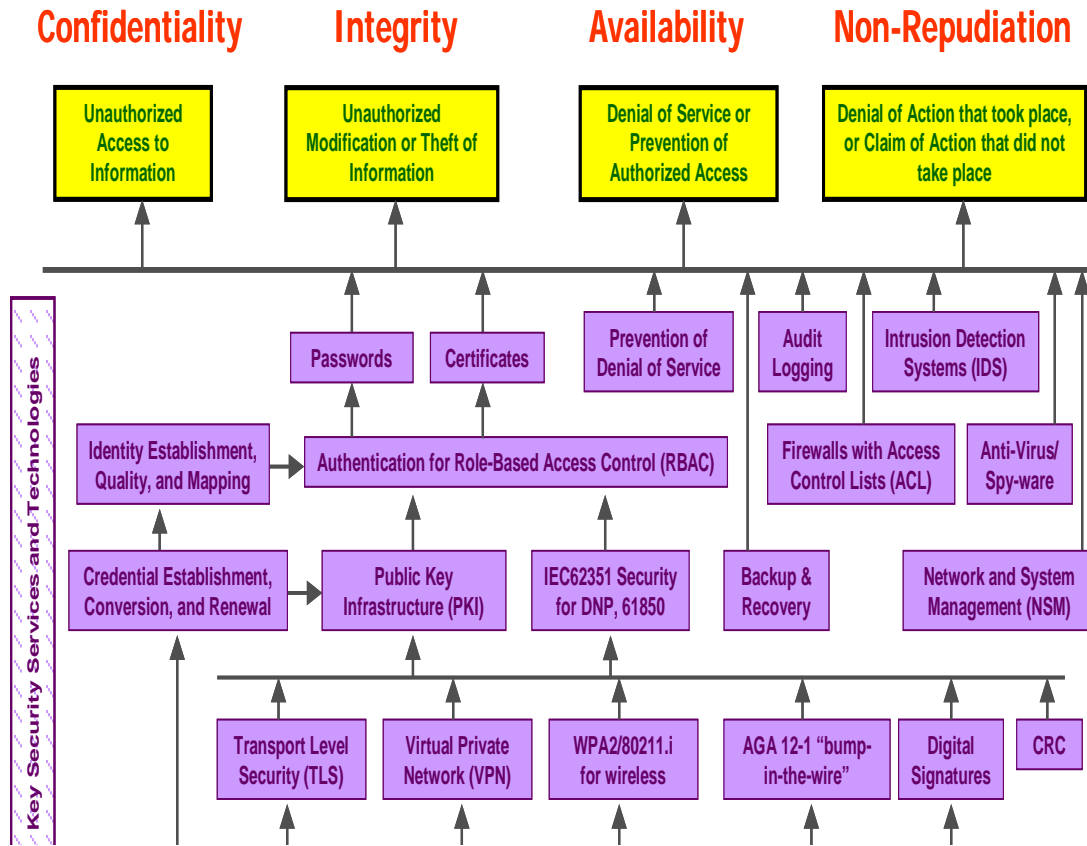


Figure 5: Overall Security: Security Requirements, Threats, Countermeasures, and Management

Confidentiality Security Countermeasures

Confidentiality

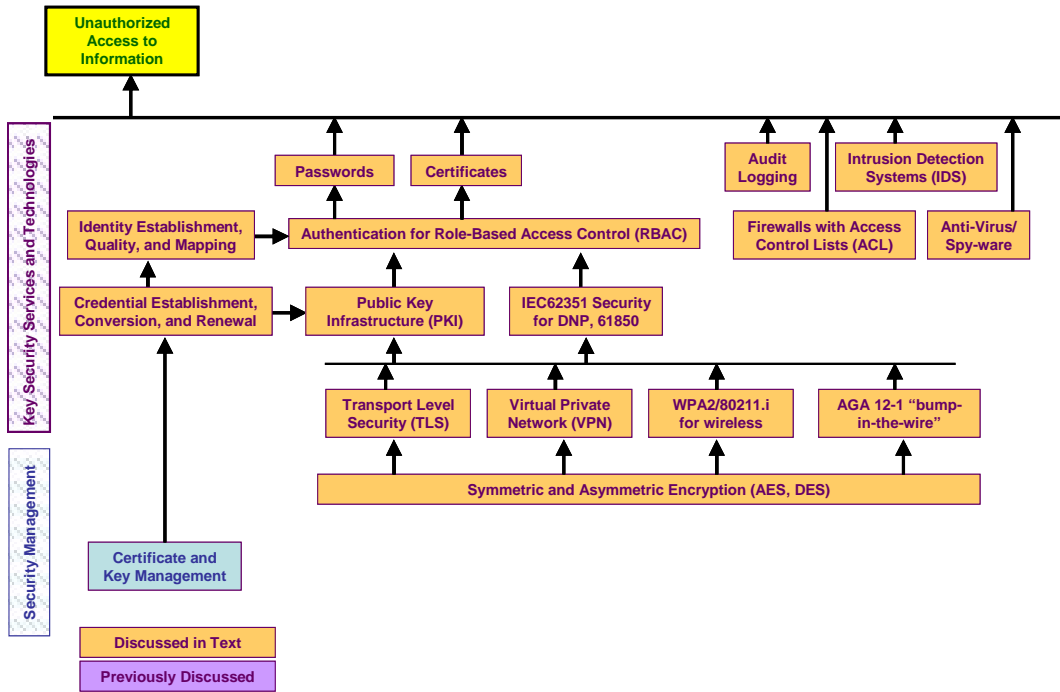


Figure 6: Confidentiality Security Countermeasures

Integrity Security Countermeasures

Integrity

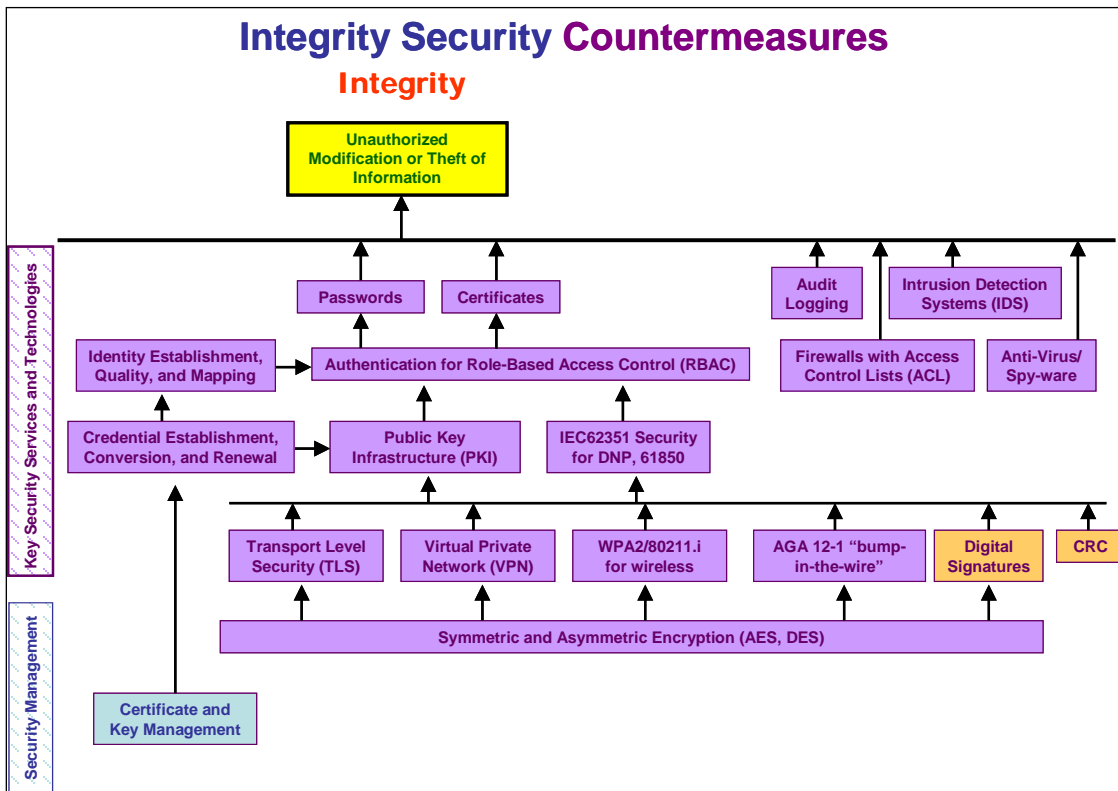


Figure 7: Integrity Security Countermeasures

Availability Security Countermeasures

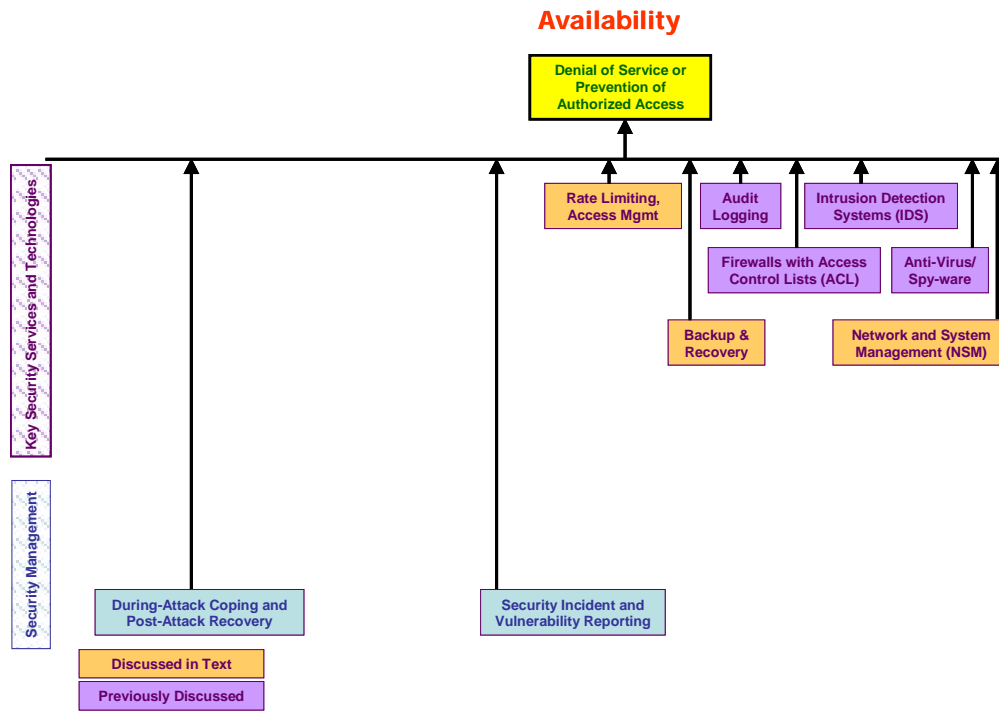


Figure 8: Availability Security Countermeasures

Non-Repudiation Security Countermeasures

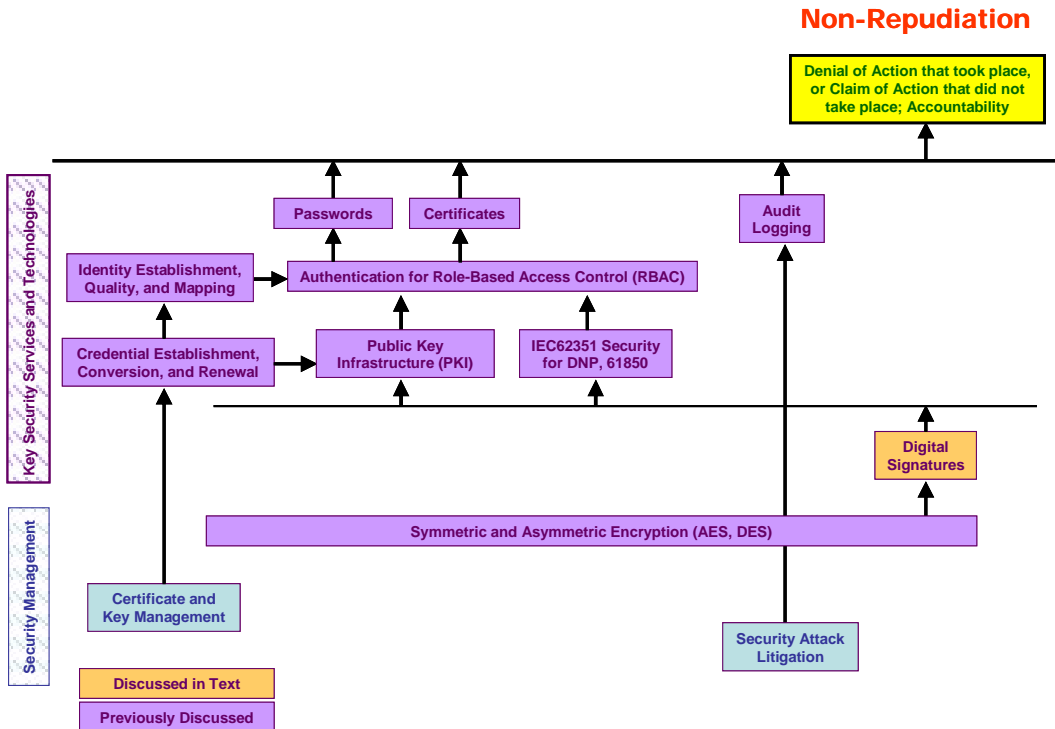


Figure 9: Non-Repudiation Security Countermeasures

Applying Security to Power System Operations

Understanding the Security Requirements and Impact of Security Measures on Power System Operations

Power system operations pose many security challenges that are different from most other industries. For instance, most security measures were developed to counter hackers on the Internet. The Internet environment is vastly different from the power system operations environment. Therefore, in the security industry there is typically a lack of understanding of the security requirements and the potential impact of security measures on the communication requirements of power system operations.

In particular, the security services and technologies have been developed primarily for industries that do not have many of the strict performance and reliability requirements that are needed by power system operations. For instance:

- Preventing an authorized dispatcher from accessing power system substation controls could have more serious consequences than preventing an authorized customer from accessing his banking account. Therefore, denial-of-service is far more important than in many typical Internet transactions.
- Many communication channels used in the power industry are narrowband, thus not permitting some of the overhead needed for certain security measures, such as encryption and key exchanges.
- Most systems and equipment are located in wide-spread, unmanned, remote sites with no access to the Internet. This makes key management and some other security measures difficult to implement.
- Many systems are connected by multi-drop communication channels, so normal network security measures cannot work.
- Although wireless communications are becoming widely used for many applications, utilities will need to be very careful where they implement these wireless technologies, partly because of the noisy electrical environment of substations, and partly because of the very rapid and extremely reliable response required by some applications.

Security Measures Important to Power System Operations

Because of the large variety of communication methods and performance characteristics, as well as because no single security measure can counter all types of threats, **it is expected that multiple layers of security measures will be implemented.** For instance, VPNs only secure the transport level protocols, but do not secure the application level protocols, so that additional security measures, such as IEC 62351-4, provide the application level security, possibly running over VPNs. In addition, role-based access passwords, intrusion detection, access control lists, locked doors, and other security measures are necessary to provide additional levels of security.

It is clear from Figures 5-9 that authentication plays a large role in many security measures. In fact, for most power system operations, authentication of control actions is far more important than “hiding” the data through encryption.

Also because connection to the Internet is (should not be) a factor, since power system operations should be well-protected by isolation and/or firewalls, some of the common threats are less critical, while others are more critical. Although importance of specific threats can vary greatly depending upon the assets being secured, some of the more critical threats are:

- Indiscretions by personnel – employees stick their passwords on their computer monitors or leave doors unlocked.
- Bypass controls – employees turn off security measures, do not change default passwords, or everyone uses the same password to access all substation equipment. Or a software application is assumed to be in a secure environment, so does not authenticate its actions.
- Authorization violation – someone undertakes actions for which they are not authorized, sometimes because of careless enforcement of authorization rules, or due to masquerade, theft, or other illegal means.
- Man-in-the-middle – a gateway, data server, communications channel, or other non-end equipment is compromised, so the data which is supposed to flow through this middle equipment is read or modified before it is sent on its way.
- Resource exhaustion – equipment is inadvertently (or deliberately) overloaded and cannot therefore perform its functions. Or a certificate expires and prevents access to equipment. This denial of service can seriously impact a power system operator trying to control the power system.

IEC TC57 Response to Security Requirements

By 1997, IEC TC57 recognized that security would be necessary for these protocols. It therefore first established a temporary group (AdHoc WG06) to study the issues of security. This group published a Technical Report IEC 62210 on the security requirements. One of the recommendations of this Technical Report was to form a Working Group to develop security standards for the IEC TC57 protocols and their derivatives (i.e. DNP).

Therefore, IEC TC57 WG15 was formed in 1999, and has undertaken this work. The WG15 title is “***Power system control and associated communications - Data and communication security***” and its scope and purpose are to

- “Undertake the development of standards for security of the communication protocols defined by the IEC TC 57, specifically the IEC 60870-5 series, the IEC 60870-6 series, the IEC 61850 series, the IEC 61970 series, and the IEC 61968 series.
- Undertake the development of standards and/or technical reports on end-to-end security issues.”

The scope of the work of WG15 is to develop standards that increase the informational security assurance aspects of the protocols specified within TC57. As part of this work, concrete and implementable, standards are intended to be developed. These standards are intended to be specified, as needed, by utilities and implemented by responding vendors. WG15 is committed to develop relevant standards that increase the overall informational security assurance aspects of utility infrastructures.

The justification was that safety, security, and reliability have always been important issues in the design and operation of systems in the power industry, and cyber security is becoming increasingly important in this industry as it relies more and more on an information infrastructure. The deregulated market has imposed new threats as knowledge of assets of a competitor and the operation of his system can be beneficial and acquisition of such information is a possible reality. Since 9/11 the additional threat of terrorism has become more visible.

The final sentence in the scope/purpose statement is very important: it was recognized that the addition of just simple encryption of the protocols, for instance by adding “bump-in-the-wire” encryption boxes or even virtual private network (VPN) technologies would not be adequate for many situations. Security truly is an “end-to-end” requirement to ensure authenticated access to sensitive power system equipment, reliable and timely information on equipment functioning and failures, backup of critical systems, and audit capabilities that permit reconstruction of crucial events.

This work is published by the IEC as IEC 62351, Parts 1-7, titled:

- IEC 62351-1: Data and Communication Security – Introduction
- IEC 62351-2: Data and Communication Security – Glossary of Terms
- IEC 62351-3: Data and Communication Security – Profiles including TCP/IP
- IEC 62351-4: Data and Communication Security – Profiles including MMS
- IEC 62351-5: Data and Communication Security – Security for IEC 60870-5 and Derivatives (i.e. DNP 3.0)
- IEC 62351-6: Data and Communication Security – Security for IEC 61850 Profiles
- IEC 62351-7: Data and Communication Security – Security through Network and System Management
- IEC 62351-8: Data and Communication Security - Role-Based Access Control for Power System Management

IEC 62351 Parts 1-2 – Introduction and Glossary

IEC 62351-1: Introduction

This first part of the standard covers the background on security for power system operations, and introductory information on the series of IEC 62351 security standards.

IEC 62351-2: Glossary of Terms

This part includes the definition of terms and acronyms used in the IEC 62351 standards. These definitions are based on existing security and communications industry standard definitions as much as possible, given that security terms are widely used in other industries as well as in the power system industry.

The terms in this glossary are provided for free access on the IEC web site at <http://std.iec.ch/terms/terms.nsf/ByPub?OpenView&Count=-1&RestrictToCategory=IEC%2062351-2>

IEC 62351 Parts 3-6 – Security Standards for IEC TC57 Protocols

Overview

Since it was formed, WG15 has undertaken the development of security standards for the four communication protocols listed above: IEC 60870-5, its derivative DNP, IEC 60870-6 (ICCP), and IEC 61850. These security standards must meet different security objectives for the different protocols, which vary depending upon how they are used.

Some of the security standards can be used across a few of the protocols, while others are very specific to a particular profile. The different security objectives include authentication of entities through digital signatures, ensuring only authorized access, prevention of eavesdropping, prevention of playback and spoofing, and some degree of intrusion detection. For some profiles, all of these objectives are important; for others, only some are feasible given the computation constraints of certain field devices, the media speed constraints, the rapid response requirements for protective relaying, and the need to allow both secure and non-secured devices on the same network.

This work has been (or is in process to be) published by the IEC as IEC 62351, Parts 3-6, titled:

- **IEC 62351-3: Data and Communication Security – Profiles Including TCP/IP** (*these security standards cover those profiles used by ICCP, IEC 60870-5 Part 104, DNP 3.0 over TCP/IP, and IEC 61850 over TCP/IP*)
- **IEC 62351-4: Data and Communication Security – Profiles Including MMS** (*these security standards cover those profiles used by ICCP and IEC 61850*)
- **IEC 62351-5: Data and Communication Security – Security for IEC 60870-5 and Derivatives (i.e. DNP 3.0)** (*these security standards cover both serial and networked profiles used by IEC 60870-5 and DNP*)
- **IEC 62351-6: Data and Communication Security – Security for IEC 61850 Peer-to-Peer Profiles** (*these security standards cover those profiles in IEC 61850 that are not based on TCP/IP – GOOSE, GSSE, and SMV*)

The interrelationship of these security standards and the protocols are illustrated in Figure 10.

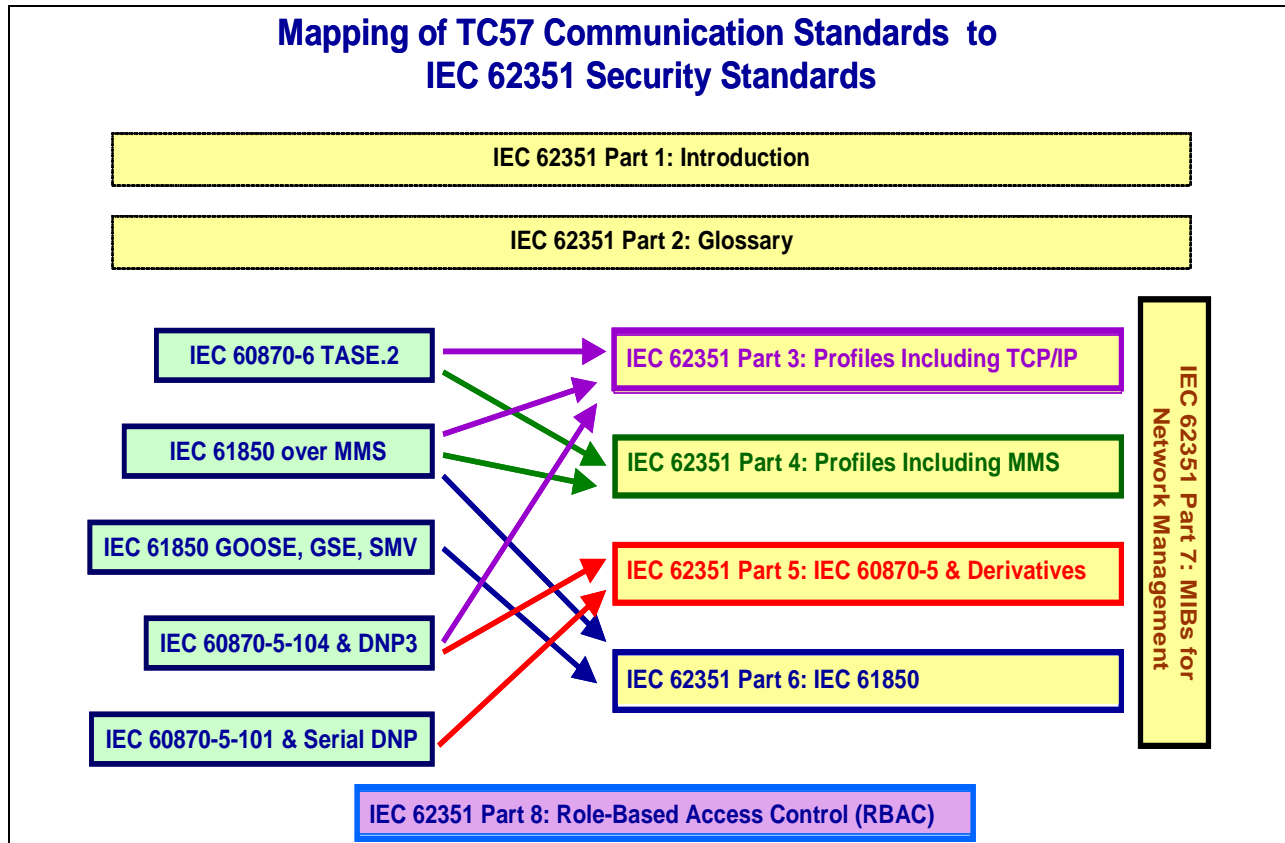


Figure 10: Interrelationship of IEC 62351 Security Standards and the TC57 Protocols

IEC 62351-3: Security for Profiles That Include TCP/IP

IEC 62351-3 provides security for any profile that includes TCP/IP, including IEC 60870-6 TASE.2, IEC 61850 ACSI over TCP/IP, and IEC 60870-5-104.

Rather than re-inventing the wheel, it specifies the use of TLS which is commonly used over the Internet for secure interactions, covering authentication, confidentiality, and integrity. This part describes the parameters and settings for TLS that should be used for utility operations.

Specifically, IEC 62351-3 protects against eavesdropping through TLS encryption, man-in-the-middle security risk through message authentication, spoofing through Security Certificates (Node Authentication), and replay, again through TLS encryption. However, TLS does not protect against denial of service. This security attack should be guarded against through implementation-specific measures.

IEC 62351-4: Security for Profiles That Include MMS

IEC 62351-4 provides security for profiles that include the Manufacturing Message Specification (MMS) (ISO 9506), including TASE.2 (ICCP) and IEC 61850.

It primarily works with TLS to configure and make use of its security measures, in particular, authentication: the two entities interacting with each other are who they say they are. It requires additional security measures in ACSE.

It also allows both secure and non-secure profiles to be used simultaneously, so that not all systems need to be upgraded with the security measures at the same time.

IEC 62351-5: Security for IEC 60870-5 and Derivatives (i.e. DNP 3)

IEC 62351-5 provides different solutions for the serial version (primarily IEC 60870-5-101, as well as parts 102 and 103) and for the networked versions (IEC 60870-5-104 and DNP 3).

Specifically, the networked versions that run over TCP/IP can utilize the security measures described in IEC 62351-3, which includes confidentiality and integrity provided by TLS encryption. Therefore, the only additional requirement is authentication.

The serial version is usually used with communications media that can only support low bit rates or with field equipment that is compute-constrained. Therefore, TLS would be too compute-intensive and/or communications-intensive to use in these environments. Therefore, the only security measures provided for the serial version include some authentication mechanisms which address spoofing, replay, modification, and some denial of service attacks, but do not attempt to address eavesdropping, traffic analysis, or repudiation that require encryption. These encryption-based security measures could be provided by alternate methods, such as VPNs or “bump-in-the-wire” technologies, depending upon the capabilities of the communications and equipment involved.

Key management issues need to be addressed in Part 5. The primary areas of concern are:

- **Should There Be a Public Key Option?** There are two levels of keys in the existing Part 5: the Session Key, which is changed frequently in order to protect against attacks, and the Update Key, which is used to initialize and change the Session Key. Both keys are symmetric keys, meaning they are the same at both ends. The Update key is pre-shared, meaning it must be provisioned by some means outside the protocol before communications begins. One alternative would be that the Session Key and Update Key would remain symmetric, but the Update Key could optionally be changed using a third level of keys, which would be an asymmetric public/private key pair. The Update Key would not be changed frequently, perhaps not for months or years, perhaps only when personnel changed.
- **Should We Permit Multiple Users/Update Keys?** One of the arguments for using a third level of keys is that it would permit authentication of the *user* of the IEC 60870-5 link, not just the device. If multiple Update Keys were permitted, they could be associated with certificates assigned to individual people. This would permit the actions of individual people to be traced from end-to-end within an automation system.
- **Should We Permit Multiple SIMULTANEOUS Users?** A more complicated issue is whether multiple users should be permitted to use the same communications connection **simultaneously**. In the mechanism proposed by the comments on the 2CD of Part 5, each security message would contain additional octets identifying the user that was initiating the communications.

The general consensus is that all three of these key management issues should be available. However, the exact mechanisms for key management is still under discussion, since there are no easy answers or existing standards (e.g. from NIST or ISO/IEC) for key management under the

conditions of widespread, low bandwidth configurations, where “rolling out trucks” just to handle key updates is not an economic option.

IEC 62351-6: Security for IEC 61850 Peer-to-Peer Profiles (e.g. GOOSE)

The IEC 61850 profile that includes the MMS protocol running over TCP/IP uses IEC 62351-3 and IEC 62351-4. Additional IEC 61850 profiles that run over TCP/IP (web services or other future profiles) will use IEC 62351-3 plus possible additional security measures developed by the communications industry for application-layer security (out-of-scope for this set of standards).

IEC 61850 contains three protocols that are peer-to-peer multicast datagrams on a substation LAN and are not routable. The main protocol, GOOSE, is designed for protective relaying where the messages need to be transmitted within 4 milliseconds peer-to-peer between intelligent controllers. Given these stringent performance requirements, encryption or other security measures which may significantly affect transmission rates are not acceptable. Therefore, authentication is the only security measure included as a requirement, so IEC 62351-6 provides a mechanism that involves minimal compute requirements for these profiles to digitally sign the messages.

IEC 62351 Part 7: Security Through Network and System Management

End-to-End Security Requirements

WG15 undertook a fifth task in addition to the security standards for the SCADA protocols when it was urged by TC57 to work toward end-to-end security, which entails a much larger scope than protecting communication protocols. End-to-end security involves security policies, access control mechanisms, key management, audit logs, and other critical infrastructure protection issues. The first effort in this expanded scope was to develop network and system management data objects to help manage the information infrastructure.

Scope and Objectives of IEC 62351-7

The scope of IEC 62351-7 focuses on Network and System Management (NSM) of the information infrastructure. Power systems operations are increasingly reliant on information infrastructures, including communication networks, intelligent electronic devices (IEDs), and self-defining communication protocols. Therefore, management of the information infrastructure is crucial to providing the necessary high levels of security and reliability in power system operations. WG15 has therefore developed abstract Network and System Management (NSM) data objects for the power system operational environment (currently a Working Group draft). These NSM data objects reflect *what information is needed to manage the information infrastructure as reliably as the power system infrastructure is managed* (see Figure 11).

The ISO CMIP and the IETF SNMP standards for Network Management can provide some of this management. In SNMP, Management Information Base (MIB) data is used to monitor the health of networks and systems, but each vendor must develop their own set of MIBs for their equipment. For power system operations, SNMP MIBs are only available for common networking devices, such as routers. No standard MIBs have been developed for IEDs, so vendors use “ad hoc” or proprietary methods for monitoring some types of equipment health.

This standard thus provides MIB-like data objects (termed NSM data objects) for the power industry.

The abstract SNMP client/agent model is assumed within the standard, but SNMP is not presumed to be the protocol of choice. Instead, the NSM data objects defined in this document represent the set of information that is deemed mandatory, recommended, or optional in order to support network and system management and security problem detection. These abstract NSM data objects are currently represented in tables, but may possibly be represented in UML classes.

The NSM data objects can then be mapped to any appropriate protocol, including IEC 61850, IEC 60870-5, IEC 60870-6, SNMP, Web Services, or any other appropriate protocol. An initial mapping to SNMP will be developed before the document is submitted to the IEC.

The general philosophy of this document is to document the type and definition of the information required to perform End-to-End security detection within a TC57 environment. The use/non-use of the recommended MIBs outside of the TC57 environment is out-of-scope for this document.

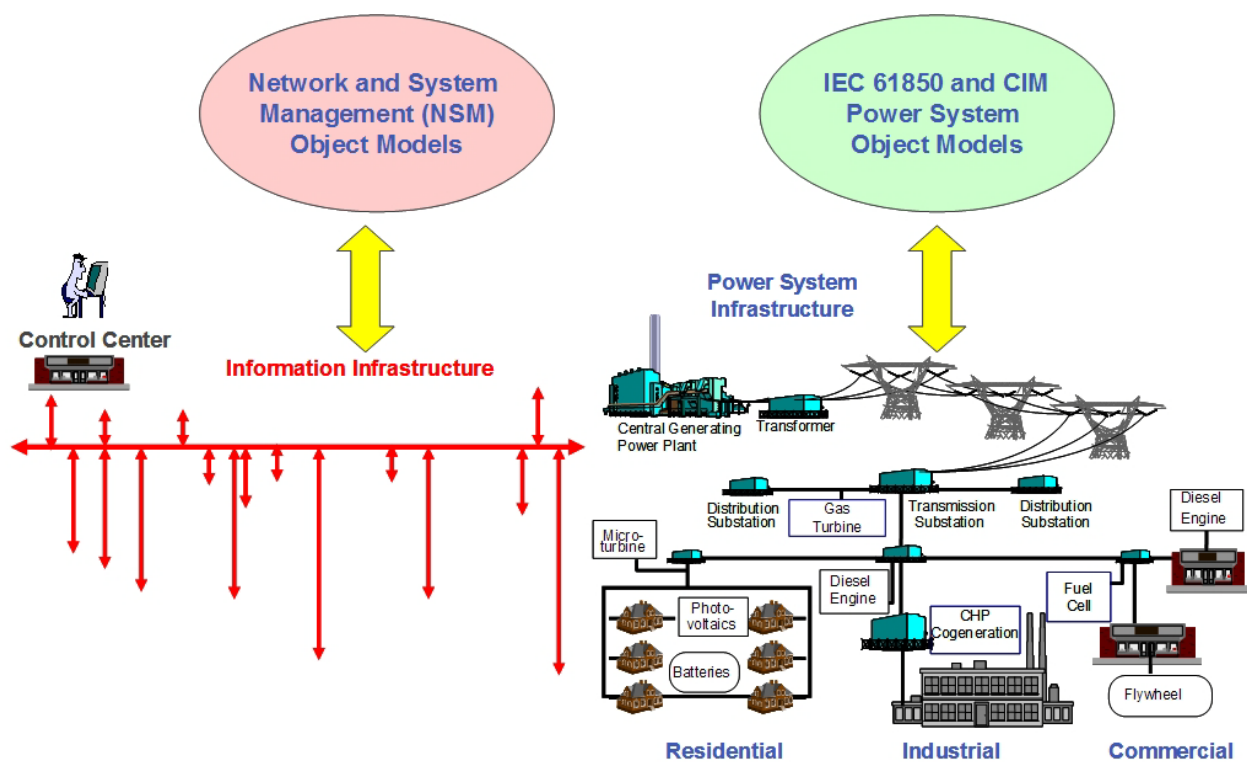


Figure 11: NSM object models are the Information Infrastructure equivalent to the CIM and IEC 61850 object models of the Power System Infrastructure

Information Infrastructure Security

The Information Infrastructure in power operations is not typically treated as a coherent infrastructure, but is viewed as a collection of individual communication channels, separate databases, multiple systems, and different protocols. Often SCADA systems perform some

minimal communications monitoring, such as whether communications are available to their RTUs, and then they flag data as “unavailable” if communications are lost. However, it is up to the maintenance personnel to track down what the problem is, what equipment is affected, where the equipment is located, and what should be done to fix the problem. All of this is a lengthy and ad hoc process. In the mean time, the power system is not being adequately monitored, and some control actions may be impossible. As the analysis of the August 14, 2003 blackout showed, the primary reason behind the blackout itself was the lack of critical information made available to the right user at the right time.

Every utility is different in what information is available to its maintenance staff.

Telecommunication technicians are generally responsible for tracking down any microwave or fiber cable problems; telecommunication service providers must track their networks; database administrators must determine if data is being retrieved correctly from substation automation systems or from GIS databases; protocol engineers must correct protocol errors; application engineers must determine if applications have crashed, have not converged, or are in an endless loop; and operators must filter through large amounts of data to determine if a possible “power system problem” is really an “information system problem”.

In the future, the problem of information management will become increasingly complex. SCADA systems will no longer have exclusive control over the communications to the field, which may be provided by telecommunication providers, or by the corporate networks, or by other utilities. Intelligent Electronic Devices (IEDs) will have applications executing within them whose proper functioning is critical to power system reliability. Field devices will be communicating with other field devices, using channels not monitored by any SCADA system. Information networks in substations will rely on local “self-healing” procedures which will also not be explicitly monitored or controlled by today’s SCADA systems.

Network and System Management Requirements

Security and reliability NSM data object requirements need to be defined that are specific for the power industry. These NSM data objects will support communications network integrity, system and application health, Intrusion Detection Systems (IDS), firewalls, and other security/network management requirements that are unique to power system operations. The basic elements of power system operations system with the addition of a security monitoring architecture are shown in Figure 12.

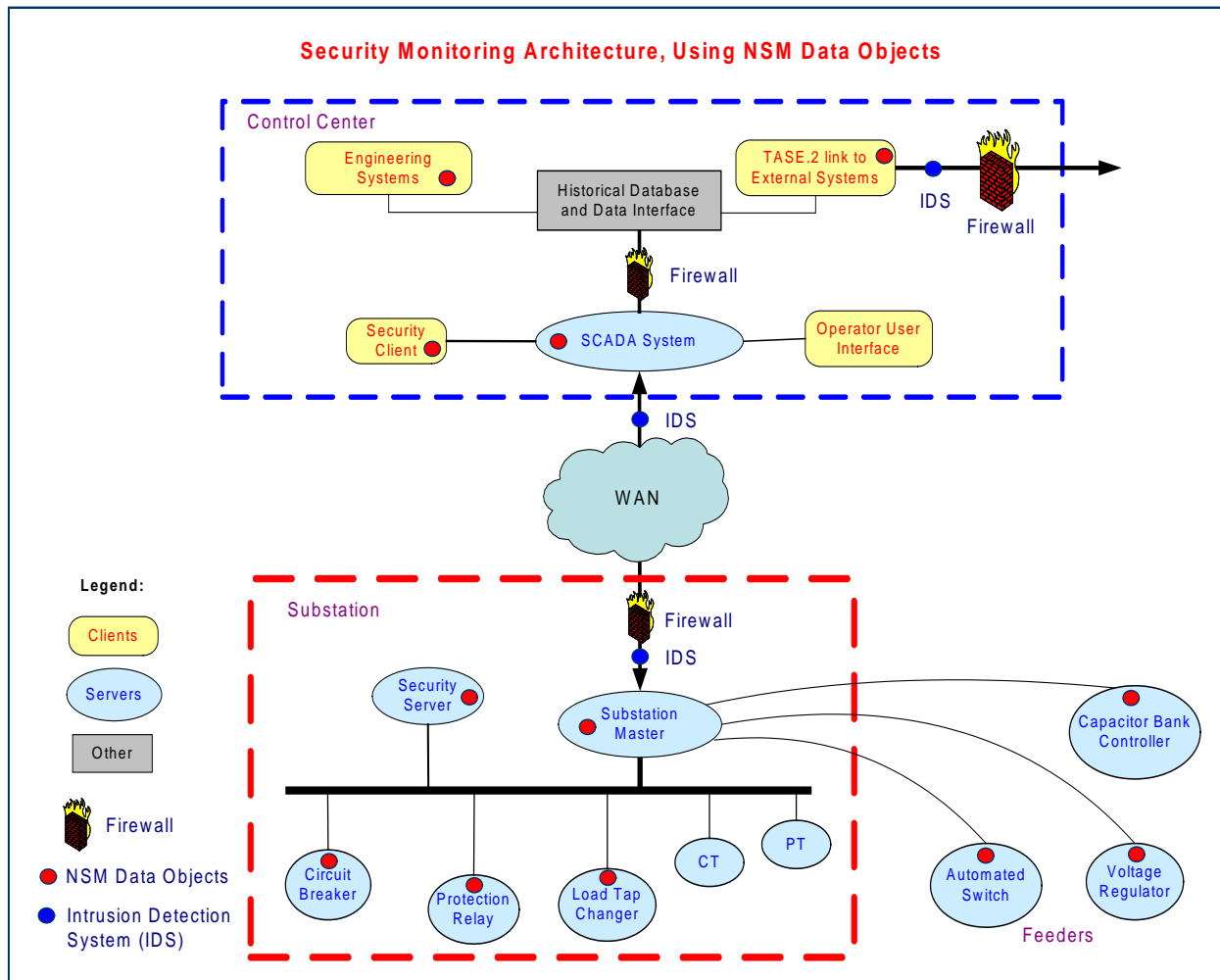


Figure 12: Power system operations systems, illustrating the security monitoring architecture

Examples of the network and system management requirements that the NSM data objects fulfill include:

1. Communications Network Management: Monitoring the Networks and Protocols

- a. Detecting network equipment permanent failures
- b. Detecting network equipment temporary failures and/or resets
- c. Detecting network equipment failovers to backup equipment or communication paths
- d. Detecting the status of backup or spare equipment
- e. Detecting communication protocol version and status
- f. Detecting mis-matches of differing protocol versions and capabilities
- g. Detecting tampered/malformed protocol messages
- h. Detecting inadequately synchronized time clocks across networks
- i. Detecting resource exhaustion forms of Denial of Service (DOS) attacks.
- j. Detecting buffer overflow DOS attacks
- k. Detecting physical access disruption
- l. Detecting invalid network access
- m. Detecting invalid application object access/operation
- n. Ability to detect coordinated attacks across multiple systems

- o. Collecting statistical information from network equipment
 - Determining average message delivery times, slowest, fastest, etc.
 - Counting number of messages, size of messages
- p. Providing audit logs and records

2. Communications Network Management: Controlling the Networks

- a. Manual issuing of on/off commands to network equipment
- b. Manual issuing of switching commands to network equipment
- c. Setting parameters and sequences for automated network actions
- d. Automated actions in response to events, such as reconfiguration of the communications network upon equipment failure

3. System Management: Monitoring Intelligent Electronic Devices (IEDs)

- a. Numbers and times of all stops and starts of systems, controllers, and applications
- b. Status of each application and/or software module: stopped, suspended, running, not responding, inadequate or inconsistent input, errors in outputs, error state, etc.
- c. Status of all network connections to an IED, including numbers and times of temporary and permanent failures
- d. Status of any “keep-alive” heartbeats, including any missed heartbeats
- e. Status of backup or failover mechanisms, such as numbers and times these mechanisms were unavailable
- f. Status of data reporting: normal, not able to keep up with requests, missing data, etc.
- g. Status of access: numbers, times, and types of unauthorized attempts to access data or issue controls
- h. Anomalies in data access (e.g. individual request when normally reported periodically)

4. System Management: Control Actions within Intelligent Electronic Devices (IEDs)

- a. Start or stop reporting
- b. Restart IED
- c. Kill and/or restart application
- d. Re-establish connection to another IED
- e. Shut down another IED
- f. Provide event log of information events
- g. Change password
- h. Change backup or failover options
- i. Providing audit logs and records

Role-Based Access Control for Power System Management

The scope of this technical specification is the access control of users and automated agents to data object in power systems by means of role-based access control (RBAC).

RBAC is not a new concept; in fact, it is used by many operating systems (e.g. Solaris, Windows 2000 and above) to control access to system resources. RBAC is an alternative to the all-or-nothing super-user model. RBAC is in keeping with the security principle of least permission, which states that no user should be given more permission than necessary for performing that

The scope of this specification is the lower part of Figure 1, i.e., everything that is needed for interoperability between systems from different vendors. The purpose of this specification is therefore:

- Firstly, to introduce ‘users-roles-permissions’ as authorization concept;
- Secondly, to promote role-based access solutions for the entire pyramid in power system management; and
- Thirdly, to enable interoperability in the multi-vendor environment of substation automation.

To achieve these goals, this part of IEC 62351 specifies the following items:

- Format of credentials, including subject name for logging;
- Mandatory security roles and permissions for administration, audit, and maintenance;
- Transmission of roles for TCP/IP and serial communications;
- Extensions in data models of power systems necessary to implement RBAC; and
- Verification of credentials in the target system to ensure secure access control.

Status of WG15 Standards (October 2010)

As of October 2010, the status of the WG15 documents is:

1. Parts 1 (Introduction), 3 (TLS), 4 (MMS), and 6 (IEC 61850) were approved as IEC Technical Specifications in June 2007.
2. Part 2 (Glossary) was approved as an IEC Technical Specification in mid 2008.
3. Part 5 (IEC 60870-5 and derivatives (e.g. DNP3) was approved as an IEC Technical Specification in July 2009.
4. Part 7 (Network and System Management) was approved as an IEC Technical Specification and will be released by the IEC shortly.
5. Part 8 (Role-based Access Control) is a CD with comments resolved in October 2009, and will be submitted as a CDV after revisions reflecting the comments.
6. Part 9 (Key Management) was approved by WG15 to start work and will be submitted as a New Work Item Proposal (NWIP) to the IEC.

WG15 Roadmap

The WG15 Roadmap for October 2010 is shown below in Figure 13:

TC57 Security (IEC 62351) Roadmap

As of Oct 2010

Completed and Current Work	Updates & New Work	On-Going Coordination
<ul style="list-style-type: none"> Parts 1, 2, 3, 4, 5, 6 – Finalized as TS Standards Part 2 (Glossary) can be found at http://std.iec.ch/terms/terms.nsf/BvPub?OpenView&Count=1&RestrictToCategory=IEC%2062351-2) Part 7: Network & System Management – Finalized as TS in July 2010 Part 8: Role-Based Access Control – CDV MCR for Part 5 on remote changing of update keys 	<ul style="list-style-type: none"> Part 5 Implementation Specification for IEC 60870-5 thru WG3 Part 6 – Updates due to cryptography issues found in implementations Security Architecture White Paper Key Management as NWIP – to become IEC 62351 Part 9 IEC 61850-90-5 Edition 2 or Amendments to Parts 1, 3, 4, & 6?? 	<ul style="list-style-type: none"> IEC TC65C WG10 ISA SP99 CIGRE D2.22 EPRI, NERC Research Labs NIST CSWG IEEE PSRC IEEE PES PSCC Security Subcommittee TC57 WG03 ISO/IEC 27000

Figure 14: WG15 Roadmap

Conclusions

Security measures should be built into every system from the moment they are conceived. Security includes not only the “encryption” that some people may assume is the only security measure necessary, but also authentication, role-based access control, prevention of denial of services, monitoring and audit functions for the information infrastructure, and last, but by no means least, security policies that enforce and supplement the security measures.

WG15 will continue to work to provide the security standards and recommended practices to assist utilities in meeting their security requirements.