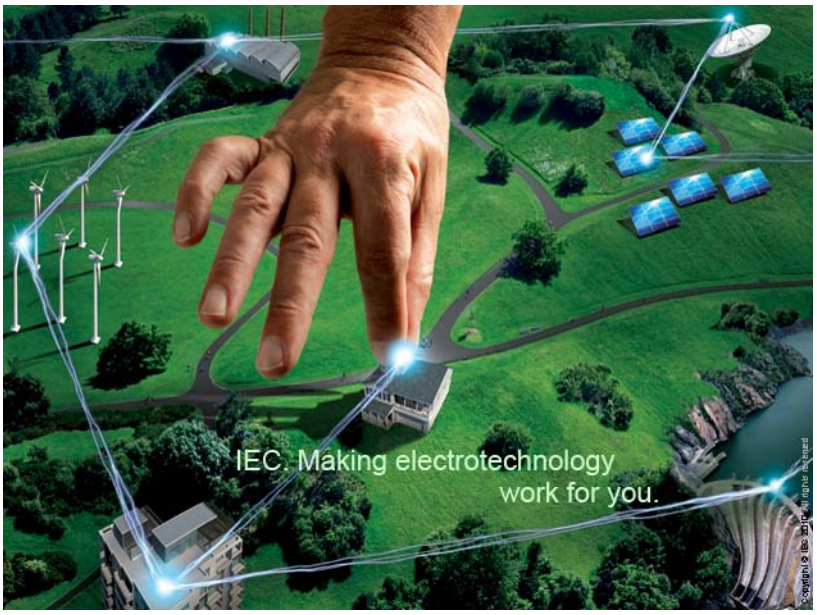
INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

IEC TC57 WG15:

IEC 62351 Security Standards for the Power System Information Infrastructure

Frances Cleveland, WG15 Convenor

Xanthus Consulting International



Contents

1. Overview: IEC TC57 WG15 Security for Power System Communications

IEC TC57 WG15 was formed to undertake the development of cybersecurity standards for power system communications. 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 IEC 62351 standards (some under development or update) consist of:

- IEC/TS 62351-1: Introduction
- IEC/TS 62351-2: Glossary
- IEC/TS 62351-3: Security for profiles including TCP/IP
- IEC/TS 62351-4: Security for profiles including MMS
- IEC/TS 62351-5: Security for IEC 60870-5 and derivatives
- IEC/TS 62351-6: Security for IEC 61850 profiles
- IEC/TS 62351-7: Objects for Network Management
- IEC/TS 62351-8: Role-Based Access Control
- IEC/TS 62351-9: Key Management
- IEC/TS 62351-10: Security Architecture
- IEC/TS 62351-11: Security for XML Files

There is not a one-to-one correlation between the IEC TC57 communication standards and the IEC 62351 security standards. This is because many of the communication standards rely on the same underlying standards at different layers. The interrelationships between the IEC TC57 standards and the IEC 62351 security standards are illustrated in Figure 1.

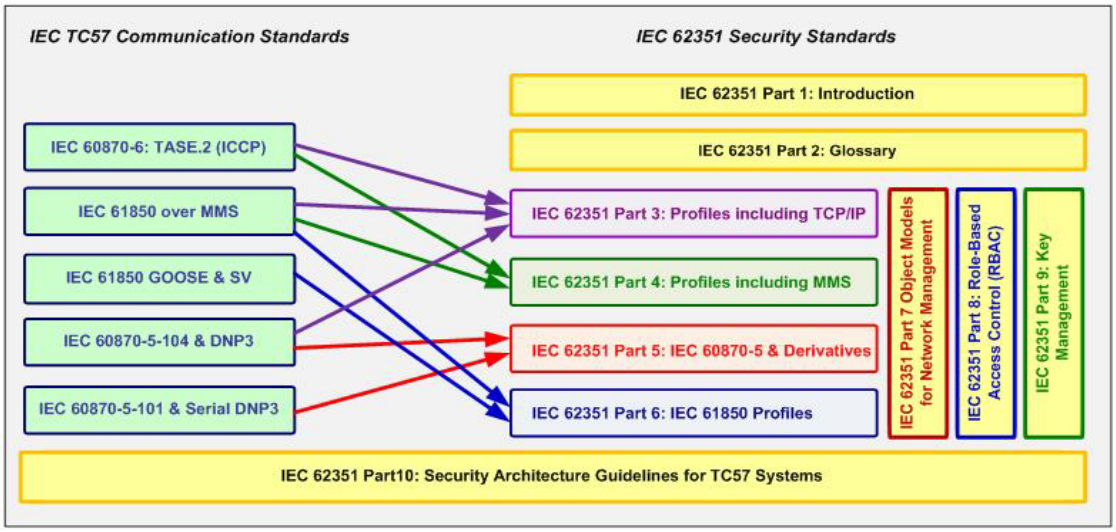


Figure 1: Interrelationships between the IEC TC57 Standards and the IEC 62351 Security Standards

2. 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.

For instance, 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.

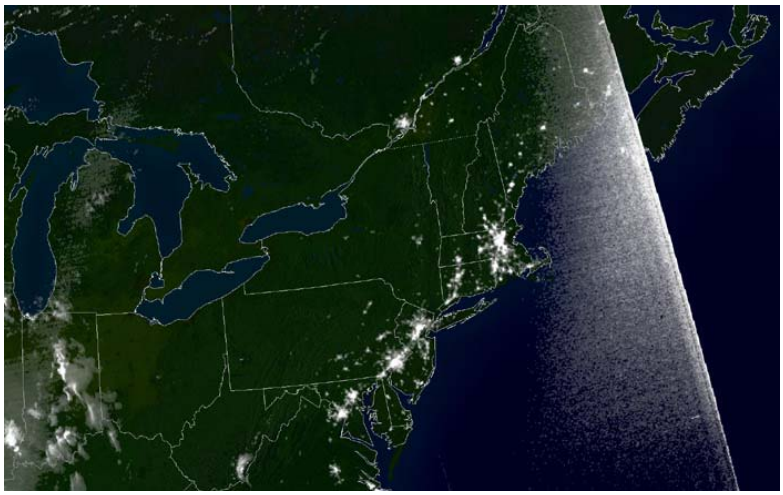
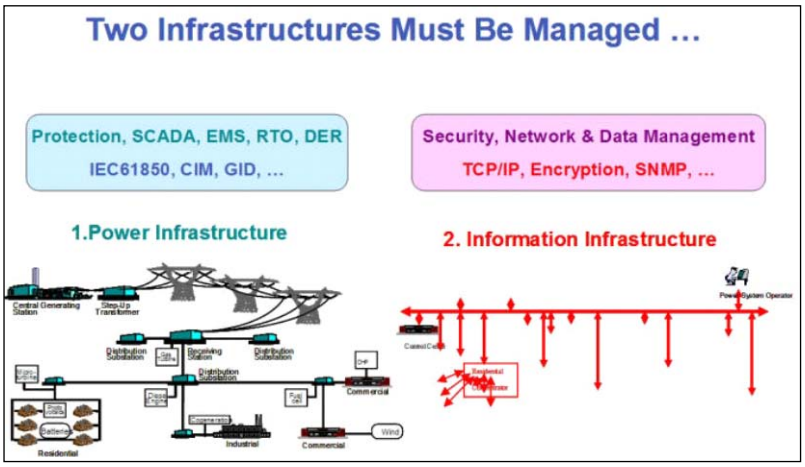


Figure 2: Illustration of the August 14, 2003 Blackout

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***.



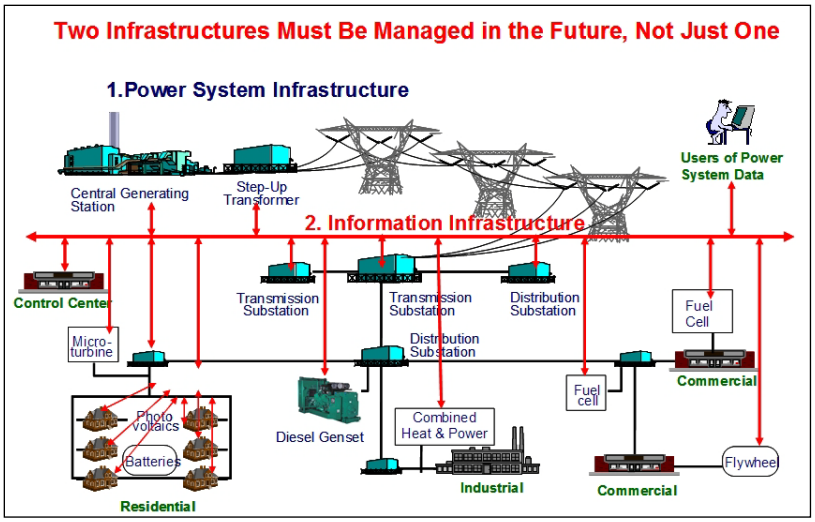


Figure 3: Two Infrastructures Must Be Managed, Not Just One

3. Why Cybersecurity?

3.1 Legacy Approach: Security by Obscurity

Communication protocols are one of the most critical parts of power system operations, both 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. Electric power is a critical infrastructure in all nations and therefore an attractive target for cyber attacks. The increasing cybersecurity threats from rogue individuals and nation states have become particularly evident in the recent Stuxnet worm and Flame malware attacks.

In addition to the national security concerns, industrial espionage threats are becoming more prevalent. 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 a disgruntled employee setting out to embarrass and damage a utility.

It is not only the malicious cyber threats 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. Natural disasters add to the need not just to prevent problems but to develop coping plans and recovery measures. On the positive side, these same coping and recovery plans can be used to mitigate malicious cyber attacks.

3.2 Smart Grid as Cyber-Physical Systems

Smart Grid systems are cyber-physical systems which combine power system operational equipment with cyber-based control of that equipment. Cyber-physical systems are designed not only to provide the functions that the equipment was developed for, but also to protect that equipment against equipment failures and often against certain types of "mistakes". In addition, they are usually designed to operate in "degraded mode" if communications are lost or some other abnormal condition exists. "Coping" with attacks is also critical, since power system equipment cannot just be shut off if an attack is occurring, but must try to remain functional as much as possible. "Recovery" strategies after attacks are also critical, since again the power must remain on as much as feasible even if equipment is removed for repair. Finally, time-stamped forensic alarm and event logs need to capture as much information as possible about the attack sequences for both future protection and possible legal actions.

Therefore, cybersecurity for cyber-physical systems are mostly the same as for purely cyber systems, but there are some important differences.

- **Physical impacts.** First, cyber attacks (whether deliberate or inadvertent) can cause physical results, such as power outages and damaged equipment. So the threats are against the functions of these systems, not directly on the data itself. Successful attacks on data not only may affect that data, but more importantly can cause some physical world impact.
- **Cyber-physical protections.** Secondly, since cyber-physical systems already are designed with many protections against "equipment and software failures" (since these are common inadvertent problems), some cyber attacks may already be protected against or may simply invoke existing cyber-physical reactions to mitigate the impact of the attack. These intrinsic mitigations should be utilized and possibly enhanced to meet additional types of threats.
- **Cyber-physical mitigations.** Thirdly, overall cyber-physical systems (e.g. the power systems themselves) are designed to "cope" with "attacks" through fault-tolerant designs, redundancy of equipment, and applications that model the physical systems using the laws of physics (e.g. power flow-based applications). Again, these types of system designs should also be utilized and enhanced to make these systems less vulnerable to malicious attacks.
- **Impacts from cybersecurity.** Fourthly, some types of cyber mitigation procedures and technologies can negatively impact cyber-physical systems. Therefore the types of cybersecurity mitigations must be carefully woven into cyber-physical mitigations to ensure that the primary functionality is maintained, even during attacks.

4. Security Concepts

4.1 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:

- Inadvertent Threats
  - Safety Failures
  - Equipment Failures
  - Carelessness
  - Natural Disasters
- 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.

4.2 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.

4.3 Security Processes

Large and small utilities face substantial cybersecurity challenges that are both institutional and technical due to the following major changing business and technical environments:

- **Interactions with more stakeholders:** Utilities must exchange information with many other stakeholders, including other utilities, retail energy service providers, smart meters at customer sites, widely distributed small generation and storage systems, and many other businesses.
- **Network configurations:** Although sensitive operational systems are never supposed to be "directly connected with the Internet" or other unauthorized networks, sometimes they are indirectly connected through mis-configurations, handheld devices, and even thumb-drives.
- **Internet-based technologies:** Utilities increasingly use "open systems", Internet-based technologies, and general consumer products rather than their legacy, one-of-a-kind products. These modern technologies are less expensive and generally more interoperable, but are also more familiar to malicious threat agents who are able to access them and find the inevitable vulnerabilities.
- **Integration of legacy systems:** At the same time, the existing or "legacy" systems have to be integrated with these more modern systems, often through "gateways" and "wrapping" which lead to their own cybersecurity vulnerabilities.
- **Increased attraction of the power industry to cyber attackers:** The power industry, as a Critical Infrastructure that is vital to national security, is subject to the growing sophistication of cyber attackers and to the increasing desire of these cyber attackers to cause financial and/or physical harm the power industry.

4.4 Security Planning

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.

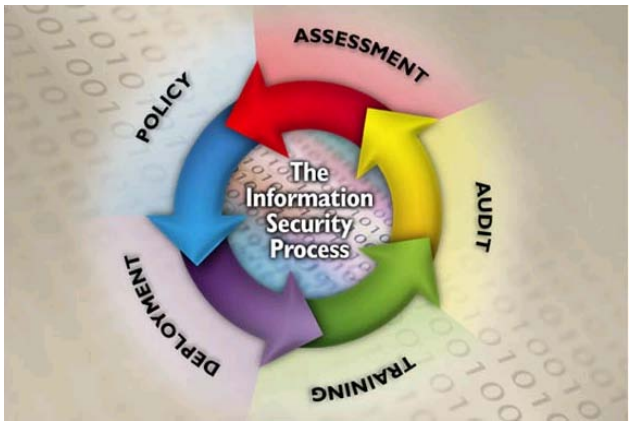


Figure 4: General Security Process – Continuous Cycle

As shown in Figure 4, 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.

4.5 Security Requirements

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.

4.6 Security Attacks

The threats can be realized by many different types of attacks, some of which are illustrated in Figure 5. 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 present a specific threat needs to be countered.

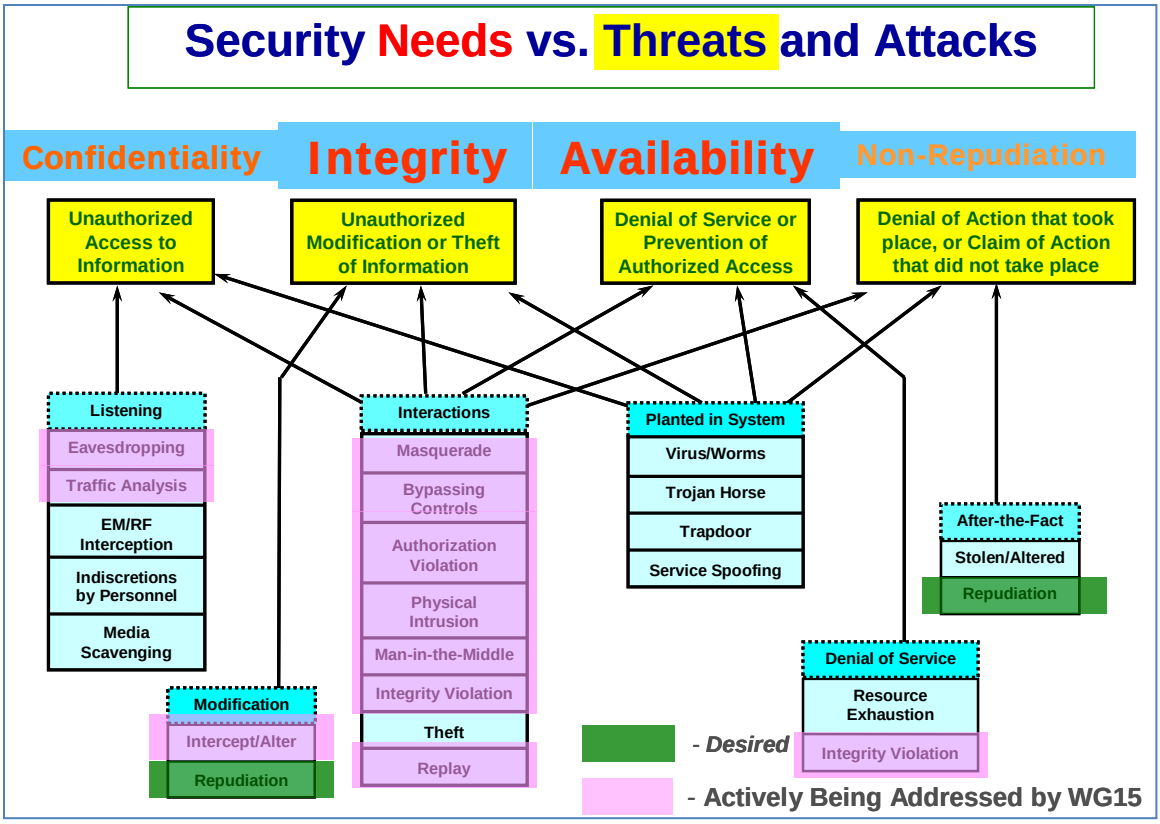


Figure 5: Security Requirements, Threats, and Possible Attacks, indicating those being addressed by WG15

4.7 Security Countermeasures

Security countermeasures, as illustrated in Figure 6, 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 7, Figure 8, Figure 9, and Figure 10.

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.

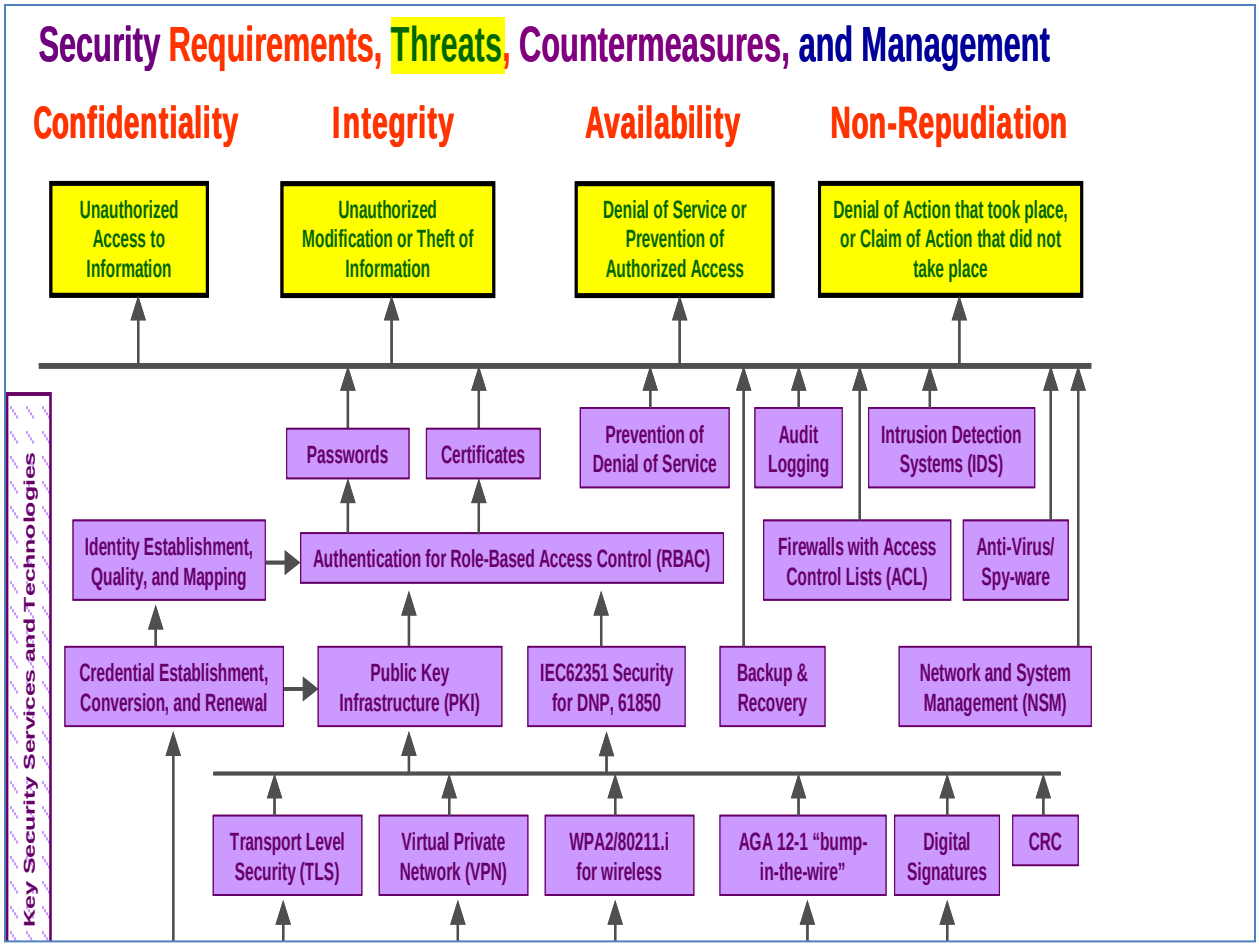


Figure 6: Overall Security: Security Requirements, Threats, Countermeasures, and Management

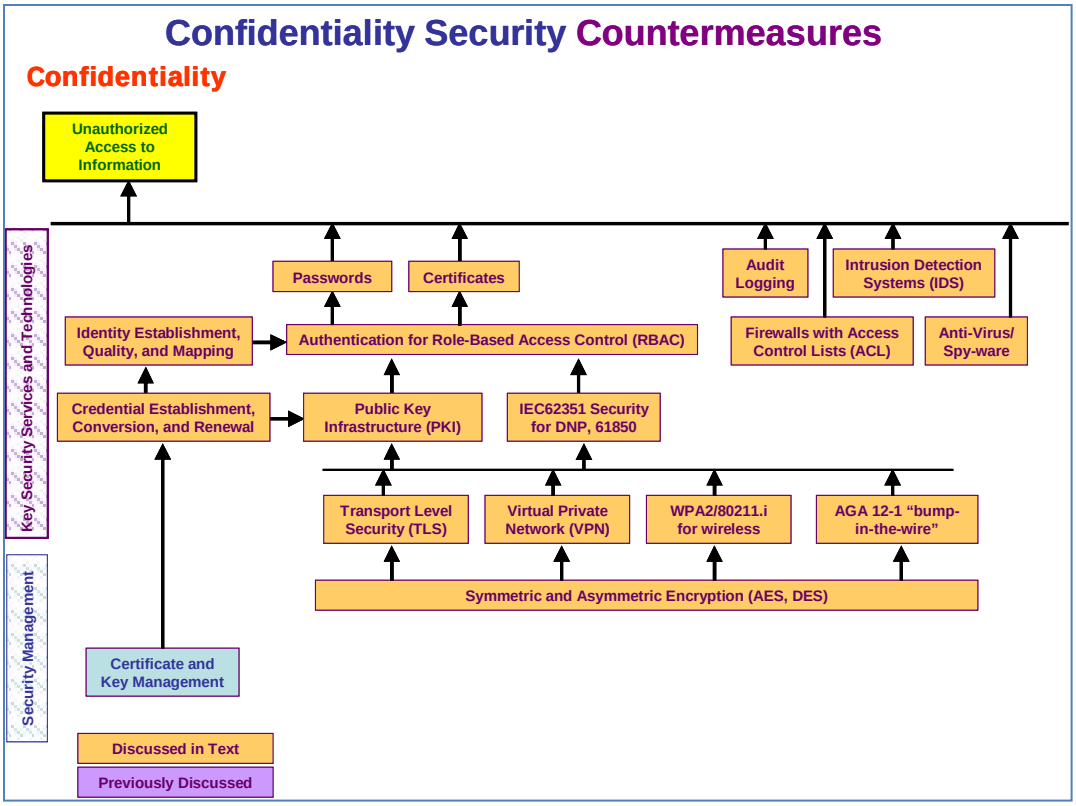


Figure 7: Examples of Confidentiality Security Countermeasures

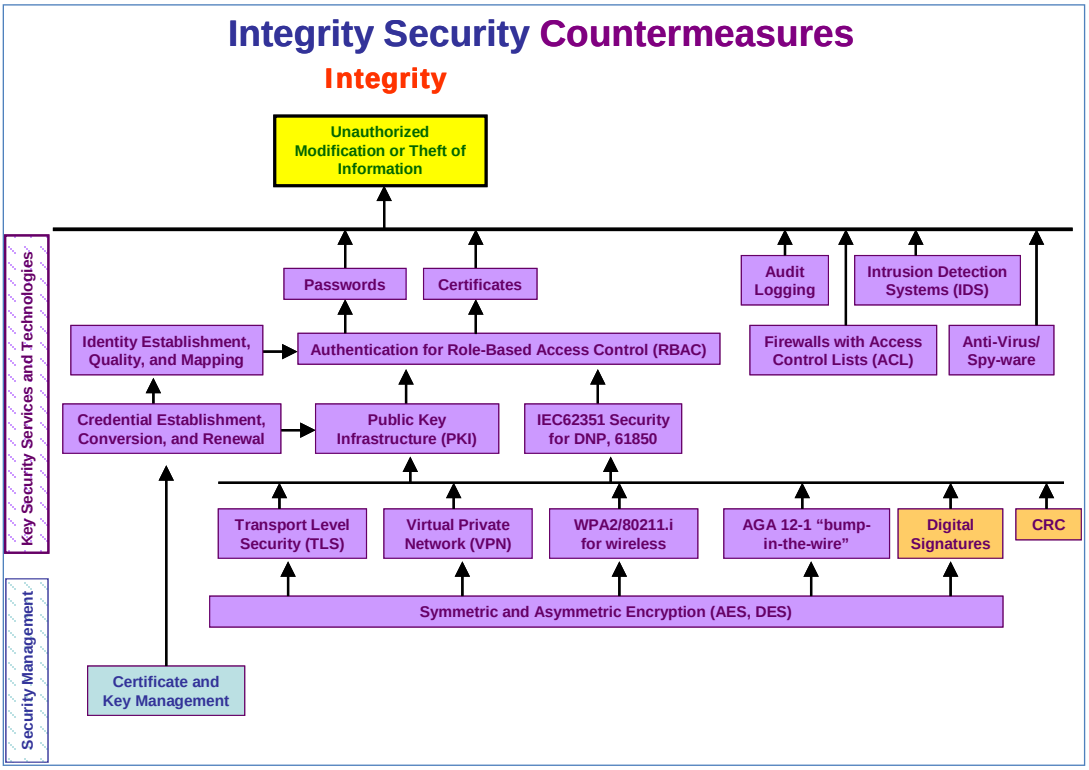


Figure 8: Examples of Integrity Security Countermeasures

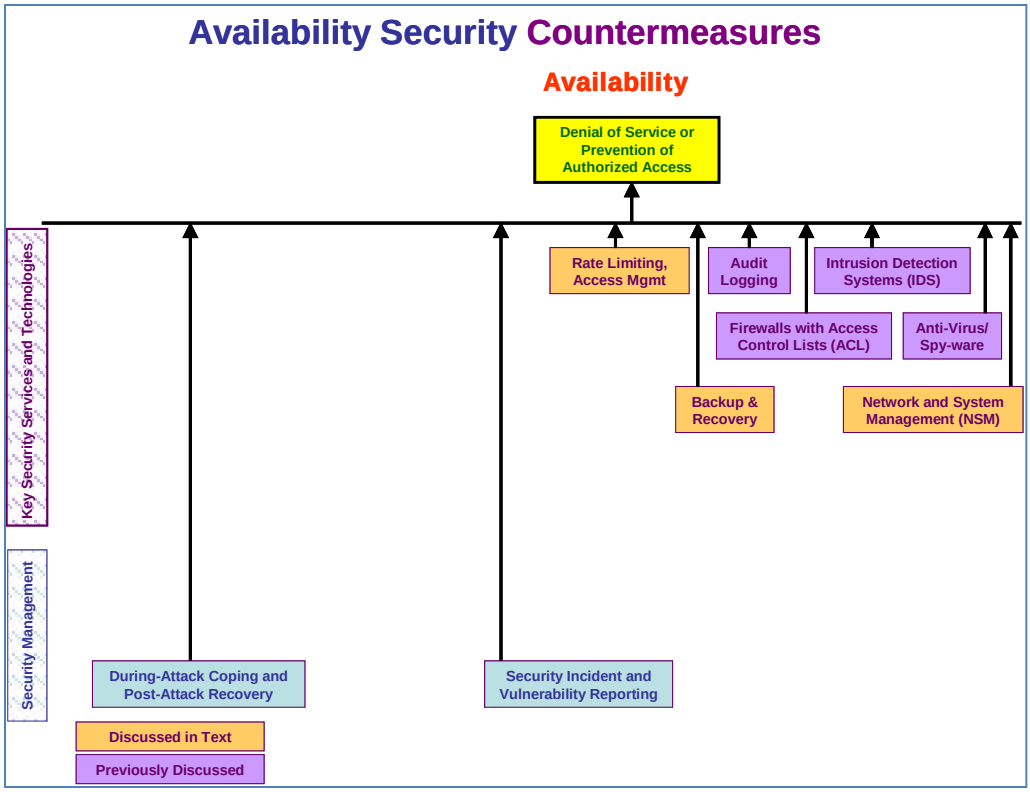


Figure 9: Examples of Availability Security Countermeasures

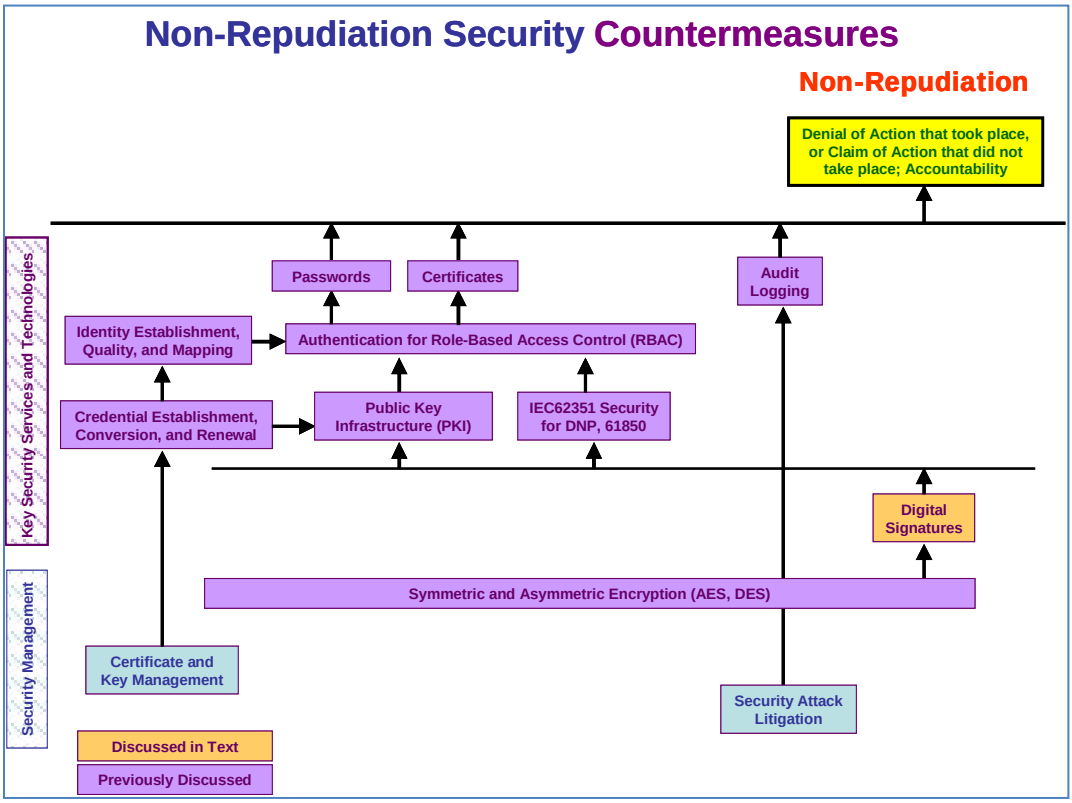


Figure 10: Examples of Non-Repudiation Security Countermeasures

5. Applying Security to Power System Operations

5.1 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.

5.2 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 than 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 that “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.
- Introduction

5.3 Correlation of Cybersecurity with Information Exchange Standards

Correlating cybersecurity with specific information exchange standards, including functional requirements standards, object modeling standards, and communication standards, is very complex. There is rarely a one-to-one correlation, with more often a one-to-many or many-to-one correspondence.

First, communication standards for the Smart Grid are designed to meet many different requirements at many different "layers" in the reference model. Two commonly used reference models are the International Organization for Standardization (ISO) / Open Systems Interconnection model (OSI) 7-layer reference model[1] and the GridWise Architecture Council (GWAC) Stack[2] (see Figure 11), where the OSI 7-layer model maps to the Technical levels of the GWAC Stack. Some standards address the lower layers of the reference models, such as wireless media, fiber optic cables, and power line carrier. Others address the "transport" layers for getting messages from one location to another. Still others cover the "application" layers, the semantic structures of the information as it is transmitted between software applications. In addition, there are communication standards

[1] ISO 7498-1:1994, *Information technology-Open Systems Interconnection-Basic Reference Model: The Basic Model.*

[2] The GWAC Stack is available at http://www.gridwiseac.org/ in the *GridWise Interoperability Context-Setting Framework.*

that are strictly abstract models of information – the relationships of pieces of information with each other. Cybersecurity is a cross-cutting issue and should be reflected in requirements at all levels: cybersecurity policies and procedures mainly cover the GWAC Stack Organizational and Informational levels, while cybersecurity technologies generally address those requirements at the Technical level.

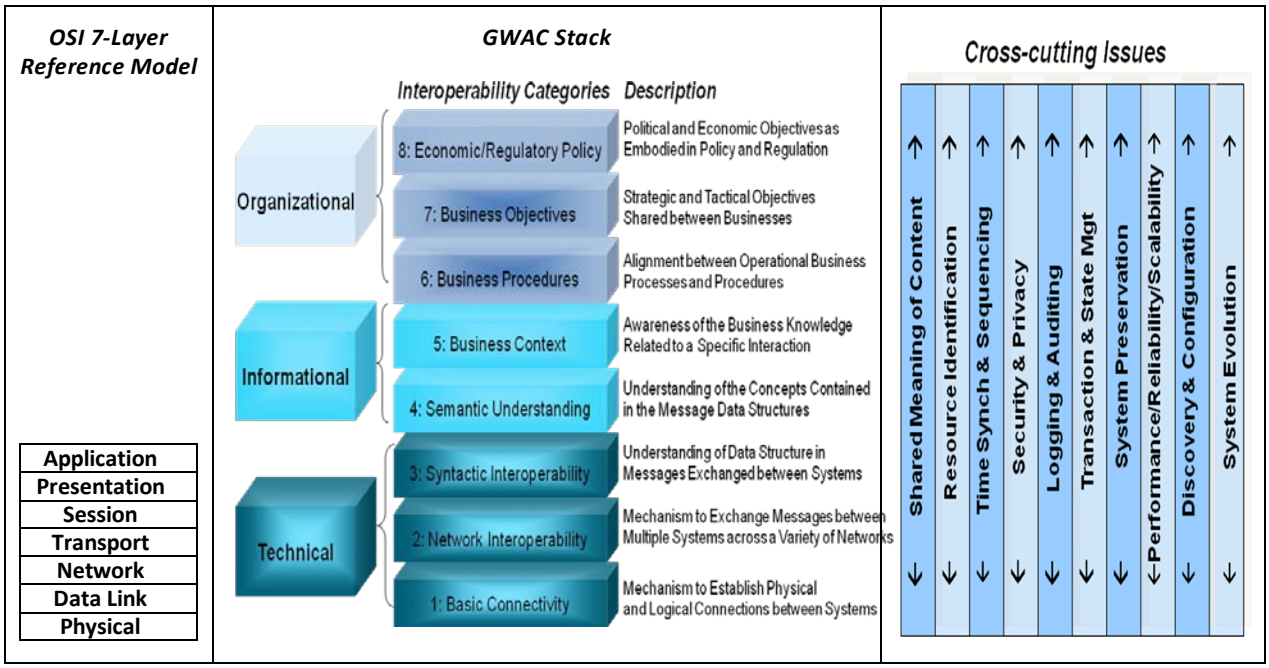


Figure 11: ISO/OSI 7-Layer Reference Model and GWAC Stack Reference Model

Second, regardless of what communications standards are used, cybersecurity must address all layers – end-to-end – from the source of the data to the ultimate destination of the data. In addition, cybersecurity must address those aspects outside of the communications system in the upper GWAC Stack layers that may be functional requirements or may rely on procedures rather than technologies, such as authenticating the users and software applications, and screening personnel. Cybersecurity must also address how to cope during an attack, recover from it afterwards, and create a trail of forensic information to be used in post-attack analysis.

Third, the cybersecurity requirements must reflect the environment where a standard is implemented rather than the standard itself - how and where a standard is used must establish the levels and types of cybersecurity needed. Communications standards do not address the importance of specific data or how it might be used in systems; these standards only address how to exchange the data. Standards related to the upper layers of the GWAC Stack may address issues of data importance.

Fourth, some standards do not mandate their provisions using "shall" statements, but rather use statements such as "should," "may," or "could." Some standards also define their provisions as being "normative" or "informative." Normative provisions often are expressed with "shall" statements. Various standards organizations use different terms (e.g., standard,

guideline) to characterize their standards according to the kinds of statements used. If standards include security provisions, they need to be understood in the context of the "shall," "should," "may," and/or "could" statements, "normative," or "informative" language with which they are expressed.

Therefore, cybersecurity must be viewed as a stack or "profile" of different security technologies and procedures, woven together to meet the security requirements of a particular implementation of policy, procedural, and communication standards designed to provide specific services. Ultimately cybersecurity, as applied to the information exchange standards, should be described as profiles of technologies and procedures which can include both "power system" methods (e.g. redundant equipment, analysis of power system data, and validation of power system states) and information technology (IT) methods (e.g. encryption, role-based access control, and intrusion detection).

There also can be a relationship between certain communication standards and correlated cybersecurity technologies. For instance, if Transmission Control Protocol (TCP)/Internet Protocol (IP) is being used at the transport layer and if authentication, data integrity, and/or confidentiality are important, then transport layer security (TLS) should be used.

Figure 12 and Figure 13 illustrate the profiles of different communication standards against the GWAC Stack and the OSI Reference Model.

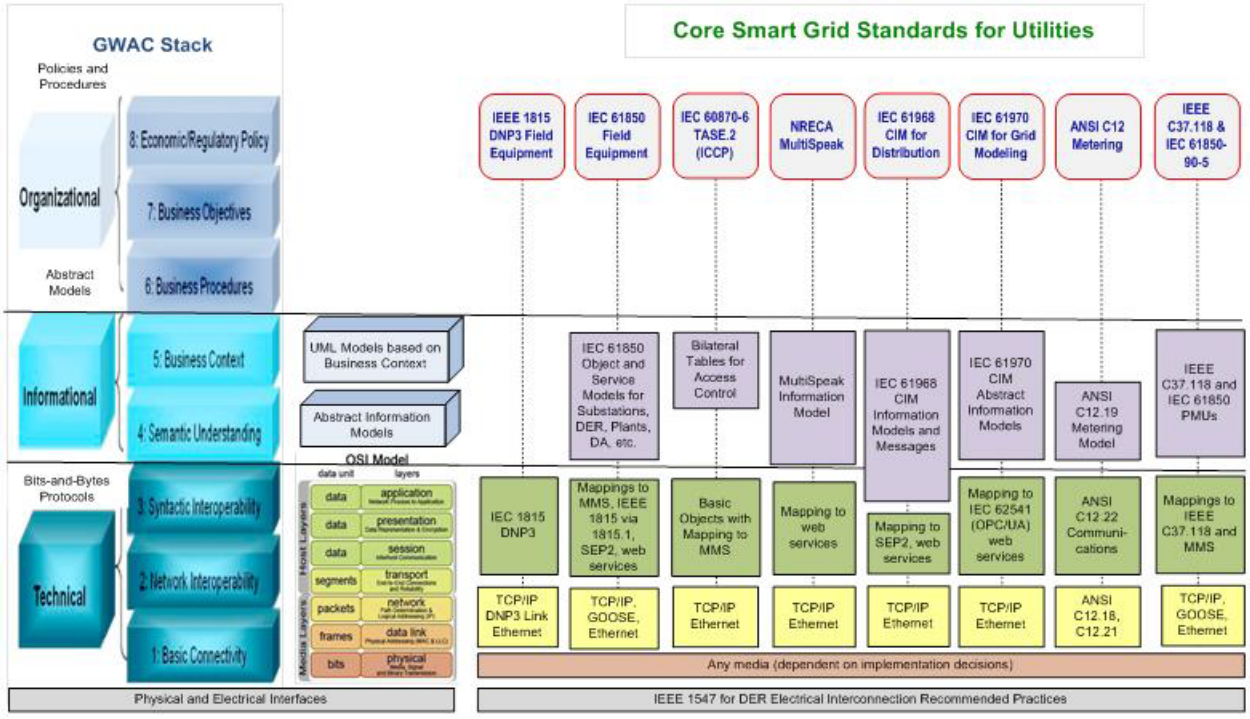


Figure 12: Core Smart Grid Standards for Utilities

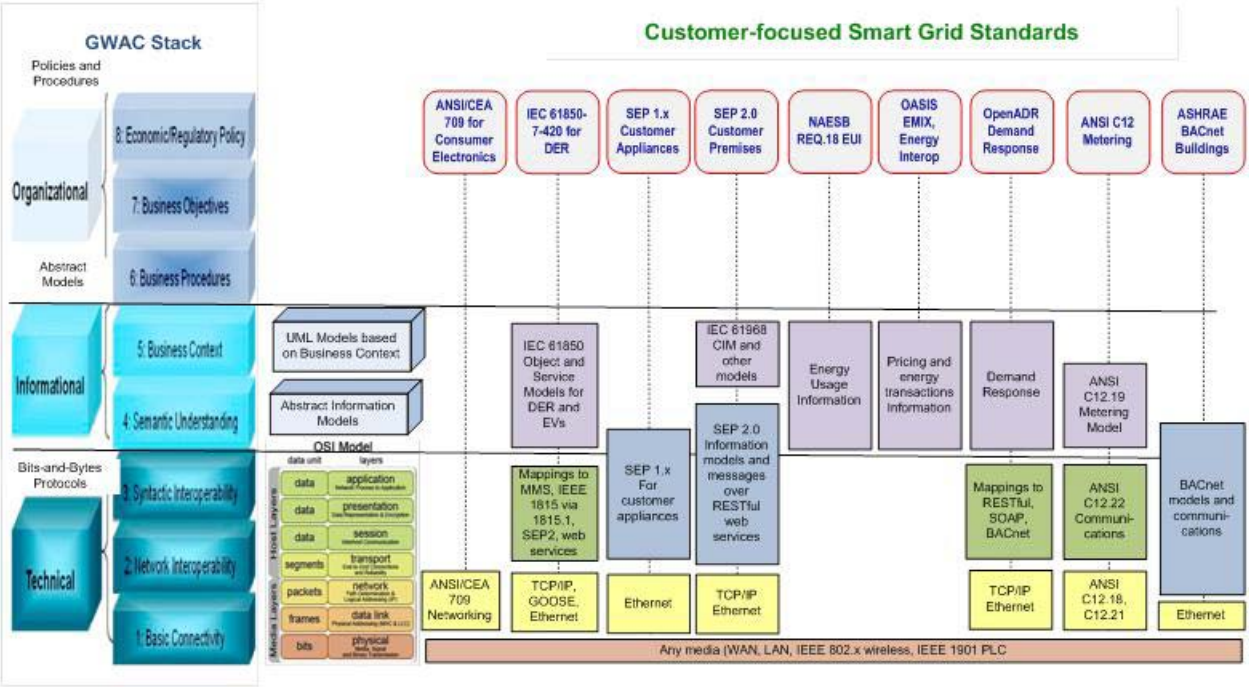


Figure 13: Customer-focused Smart Grid Standards

5.4 Correlation of Cybersecurity Requirements with Physical Security Requirements

Correlating cybersecurity requirements with specific physical security requirements is very complex since they generally address very different aspects of a system. Although both cyber and physical security requirements seek to prevent or deter deliberate or inadvertent attackers from accessing a protected facility, resource, or information, physical security solutions and procedures are vastly different from cybersecurity solutions and procedures, and involve very different expertise. Each may be used to help protect the other, while compromises of one can definitely compromise the other.

Physical and environmental security that encompasses protection of physical assets from damage is addressed by the NISTIR 7628 only at a high level. Therefore, assessments of standards that cover these non-cyber issues must necessarily also be at a general level.

5.5 Standardization Cycles of Information Exchange Standards

Information exchange standards, regardless of the standards organization, are developed over a time period of many months by experts who are trying to meet a specific need. In most cases, these experts are expected to revisit standards every five years in order to determine if updates are needed. In particular, since cybersecurity requirements were often not included in standards in the past, existing communication standards often have no references to security except in generalities, using language such as “appropriate security technologies and procedures should be implemented.”

With the advent of the Smart Grid, cybersecurity has become increasingly important within the utility sector. However, since the development cycles of communication standards and

cybersecurity standards are usually independent of each other, appropriate normative references between these two types of standards are often missing. Over time, these missing normative references can be added, as appropriate.

Since technologies (including cybersecurity technologies) are rapidly changing to meet increasing new and more powerful threats, some cybersecurity standards can be out-of-date by the time they are released. This means that some requirements in a security standard may be inadequate (due to new technology developments), while references to other security standards may be obsolete. This rapid improving of technologies and obsolescence of older technologies is impossible to avoid, but may be ameliorated by indicating minimum requirements and urging fuller compliance to new technologies as these are proven.

6. IEC TC57 Response to Security Requirements

6.1 IEC TC57 Scope: Standards for Power System Information Exchanges

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 information exchanges. 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.*"

IEC TC57 has developed five widely accepted communication standards, and has been the source of a sixth. These protocols are:

- **IEC 60870-5** 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 (IEEE 1815)** was derived from IEC 60870-5 and is in use in North America and in many other countries as well, primarily for SCADA system to RTU data communications
- **IEC 60870-6 (also known as TASE.2 or ICCP)** is used internationally for communications between control centers and often for communications between SCADA systems and other engineering systems within control centers.
- **IEC 61850** is used for interactions with field equipment, including protective relaying, substation automation, distribution automation, power quality, distributed energy resources, substation to control center, and other power industry operational functions.

It also includes profiles to meet the ultra fast response times of protective relaying and for the sampling of measured values.

- **IEC 61968 and IEC 61970 (Common Information Model CIM)** is used for application-to-application interactions, primarily within utility operations centers. It consists of a UML abstract model of the power system and includes information models and messaging for application-level information exchanges for transmission, distribution, and market functions.
- **IEC 61334 (DLMS)** is used for retrieving metering information and managing meter settings, primarily outside of North America.

This architecture is illustrated in Figure 14.

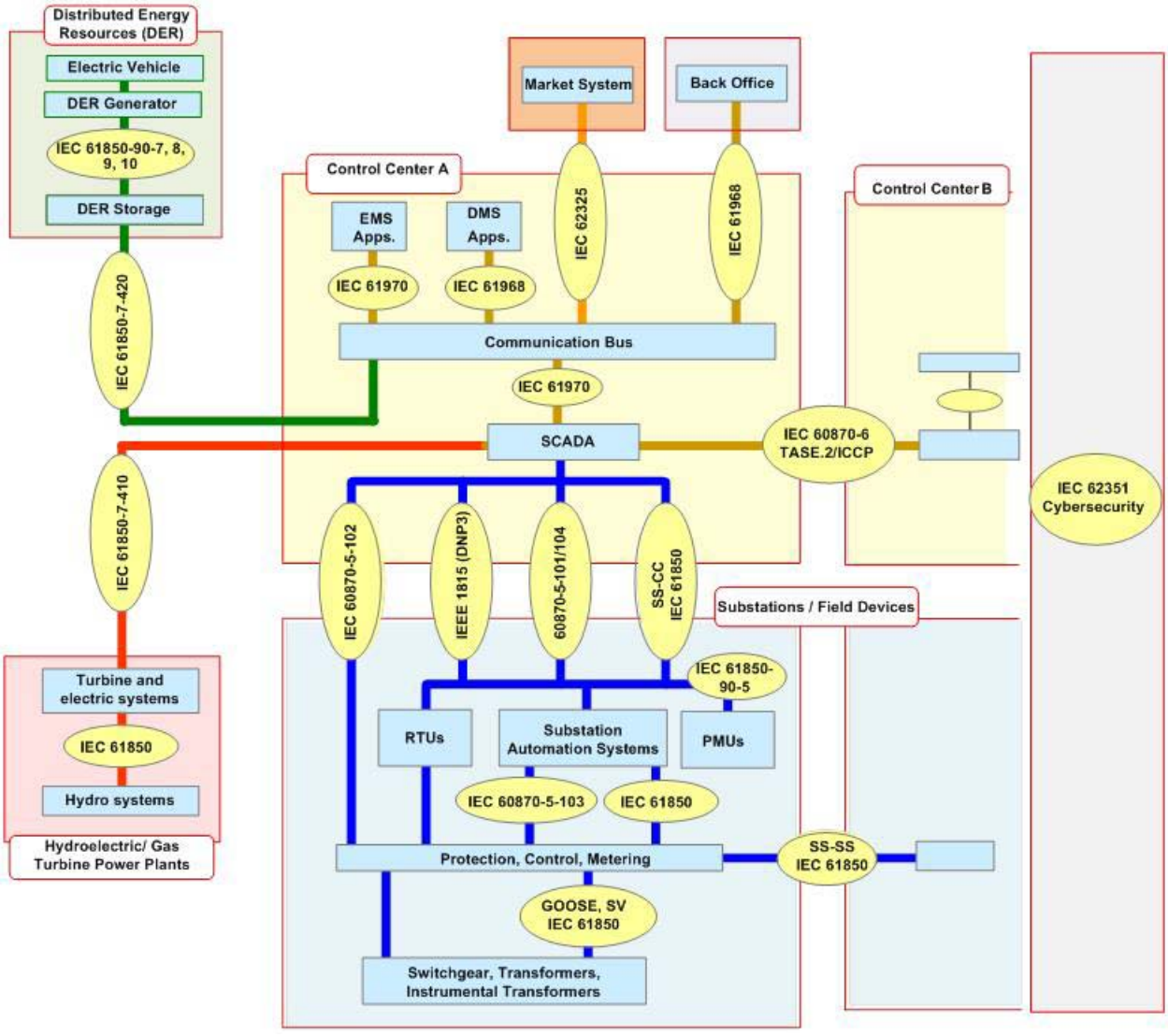


Figure 14: Architecture of IEC TC57 Information Exchange Standards

6.2 IEC TC57 WG15: Data and communication security

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 cybersecurity 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.

WG15 therefore undertook the development of the IEC 62351 series of security standards.

6.3 IEC 62351 Standards

The status of each of the current (June 2012) parts of the IEC 62351 standards is shown in Table 1.

Table 1: Status of IEC 62351 standards

IEC 62351 Part	Release Date	Activities (June 2012)	Next Release
IEC/TS 62351-1: Introduction	2007		
IEC/TS 62351-2: Glossary	2008	Review Report pending	Amendment by mid 2013
IEC/TS 62351-3: Security for profiles including TCP/IP	2007	Updated document being finalized June 2012	CDV by June 2012 IS by June 2013
IEC/TS 62351-4: Security for profiles including MMS	2007		
IEC/TS 62351-5: Security for IEC 60870-5 and derivatives	2009	DTS as Ed. 2	TS by Q3 2012
IEC/TS 62351-6: Security for IEC 61850 profiles	2007	Updates planned but not started	
IEC/TS 62351-7: Objects for Network Management	2010		
IEC/TS 62351-8: Role-Based Access Control	2011		
IEC/TS 62351-9: Key Management		CD to be submitted June 2012	
IEC/TS 62351-10: Security Architecture		DTS sent to IEC – voting date 6-22-12	TS by Q3 2012
IEC/TS 62351-11: Security for XML Files		NWIP – closing date 7-27-12	

6.4 Interrelationships of IEC TC57 Standards and the IEC 62351 Security Standards

There is not a one-to-one correlation between the IEC TC57 communication standards and the IEC 62351 security standards. This is because many of the communication standards rely on the same underlying standards at different layers.

The interrelationships between the IEC TC57 standards and the IEC 62351 security standards are illustrated in Figure 15.

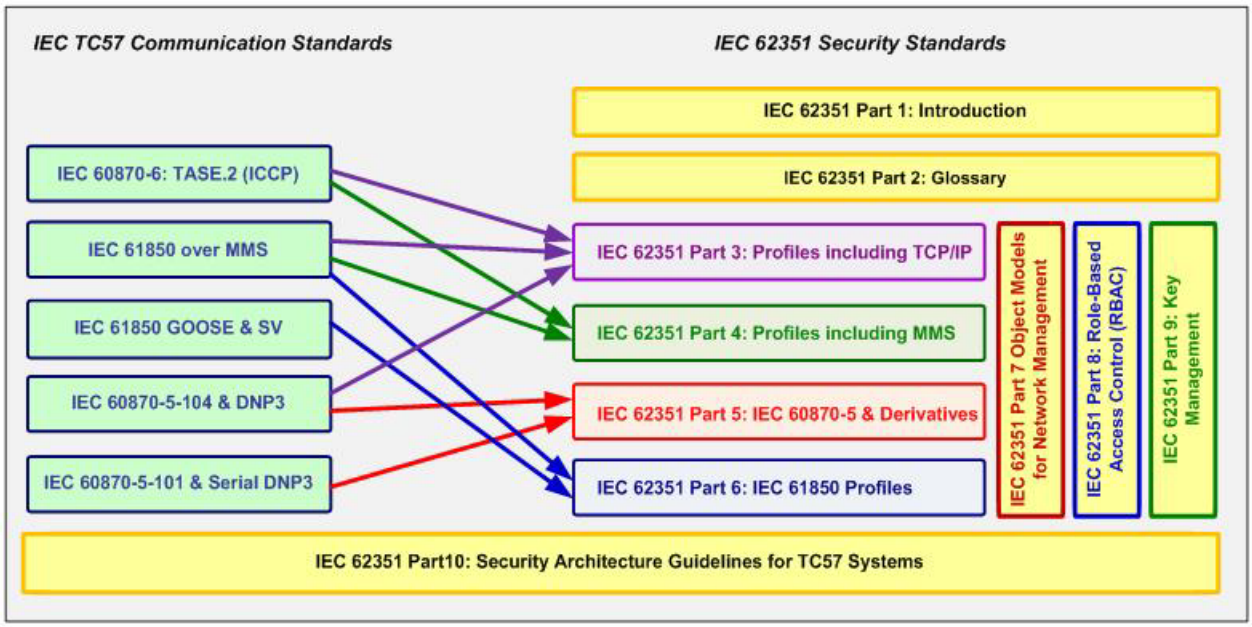


Figure 15: Interrelationships between the IEC TC57 Standards and the IEC 62351 Security Standards

6.5 IEC 62351 Parts 1-2 – Introduction and Glossary

6.5.1 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.

6.5.2 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

6.6 IEC 62351 Parts 3-6 – Security Standards for IEC TC57 Communication Standards

6.6.1 Overview

Since it was formed, WG15 has undertaken the development of security standards for the four communication standards 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 was 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:
  - IEC 60870-6 (TASE.2 / ICCP)
  - IEC 60870-5 Part 104
  - IEEE 1815 (DNP 3) over TCP/IP
  - IEC 61850 over TCP/IP
- **IEC 62351-4: Data and Communication Security – Profiles Including MMS.** These security standards cover those profiles used by:
  - IEC 60870-6 (TASE.2 / ICCP)
  - IEC 61850 using the MMS profile
- **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, all parts
  - IEEE 1815 (DNP 3)
- **IEC 62351-6: Data and Communication Security – Security for IEC 61850 Peer-to-Peer Profiles.** These security standards cover profiles in:
  - IEC 61850 that are not based on TCP/IP – GOOSE and SV

The interrelationship of these security standards and the protocols are illustrated in Figure 15.

6.6.2 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 62351-3 is being updated (June 2012).

6.6.3 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.

6.6.4 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-intense and/or communications-intense 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.

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.

6.6.5 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.

6.7 IEC 62351 Parts 7-11 – End-to-End Security Requirements

WG15 undertook a fifth task in addition to the security standards for the communication standards 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.

6.7.1 IEC 62351-7: Security through Network and System Management

6.7.1.1 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 16).

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 itself 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.

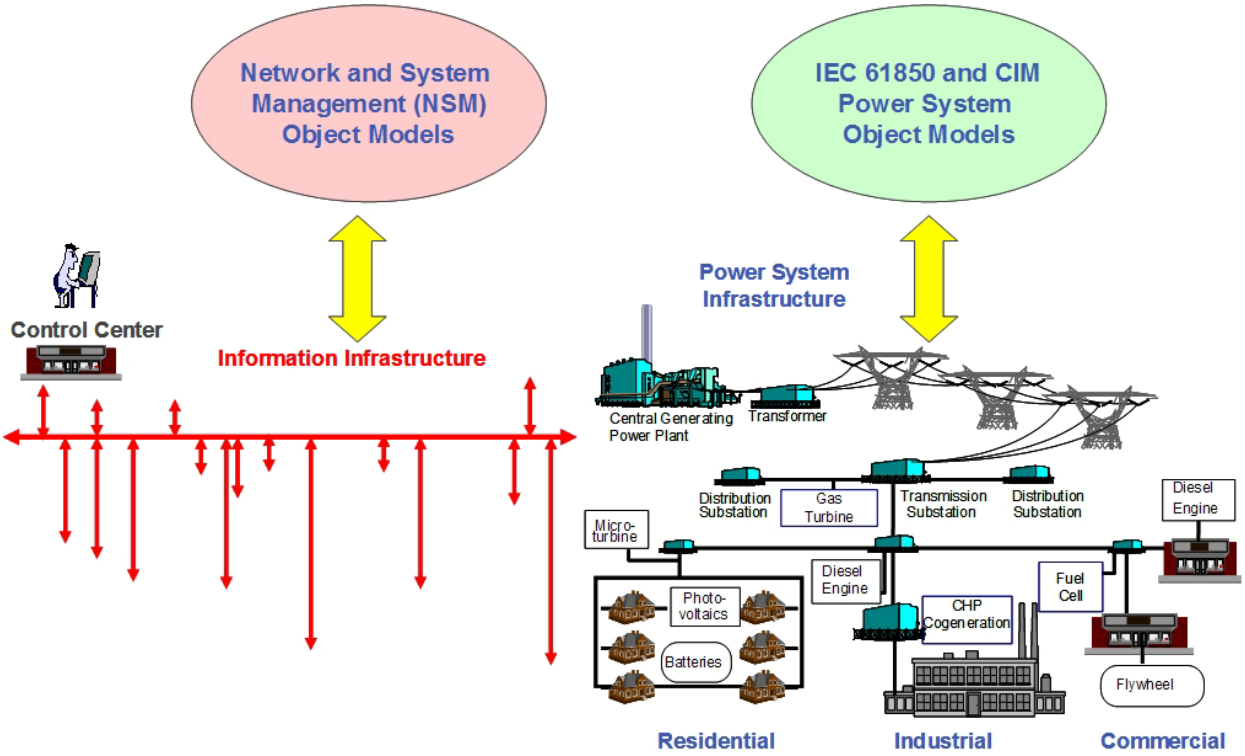


Figure 16: NSM object models are the Information Infrastructure equivalent to the CIM and IEC 61850 object models of the Power System Infrastructure

6.7.1.2 Purpose of Network Management: 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.

6.7.2 IEC 62351-8: 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 person's job. RBAC enables an organization to separate super-user capabilities and package them into special user accounts termed *roles* for assignment to specific individuals according to their job needs. This enables a variety of security policies, networking, firewall, back-ups, and system operation. A site that prefers a single strong administrator but wants to let more sophisticated users fix portions of their own system can set up an advanced-user role. RBAC is not confined to users though, it applies equally well to automated computer agents, i.e., software parts operating independent of user interactions.

As in many aspects of security, RBAC is not just a technology; it is a way of running a business. RBAC provides a means of reallocating system controls, but it is the organization that decides the implementation.

Figure 17 gives a survey of an infrastructure for implementing RBAC. First, the management of for instance a power corporation decides to implement a set of security policies, e.g., NERC **Error! Reference source not found.**. It also assigns permissions for local execution to specific substations (thereby realizing network segregation).

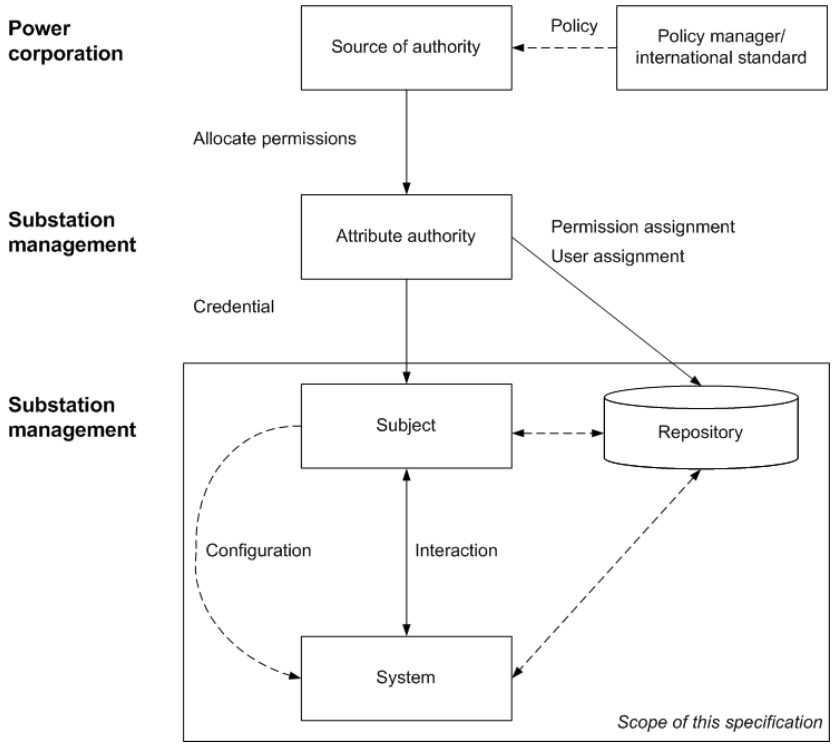


Figure 17: Survey of an RBAC infrastructure

For instance, if RBAC is applied to substations, a particular substation then may define additional roles and assign permissions to them according to their needs, level of expertise or area of knowledge of their employees. The role-permission mapping cannot be arbitrary, as the security policies imposed by the power corporation must be met by that specific substation. The role-permission mapping is used for configuring the devices of the substation. The substation management also assigns users to the roles and issues the credentials with the roles to the users. The role-permission mapping is stored along with the user-role mapping in a repository.

The scope of this specification is the lower part of Figure 17, 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.

6.7.3 IEC 62351-9: Key Management

This part 9 of the IEC 62351 series specifies how to generate, distribute, revoke and handle digital certificates, cryptographic keys to protect digital data and communication. Included in the scope is the handling of asymmetric keys (private keys and X.509 certificates), as well as symmetric keys (pre-shared keys and session keys).

This standard is still under development. (June 2012)

6.7.4 IEC 62351-10: Security Architecture

This document targets the description of security architecture guidelines for power systems based on essential security controls, i.e., on security-related components and functions and their interaction. Furthermore, the relation and mapping of these security controls to the general system architecture of power systems is provided as guideline to support system integrators to securely deploy power generation, transmission, and distribution systems applying available standards.

Figure 18 illustrates the IEC TC57 architecture used as a base for applying cybersecurity.

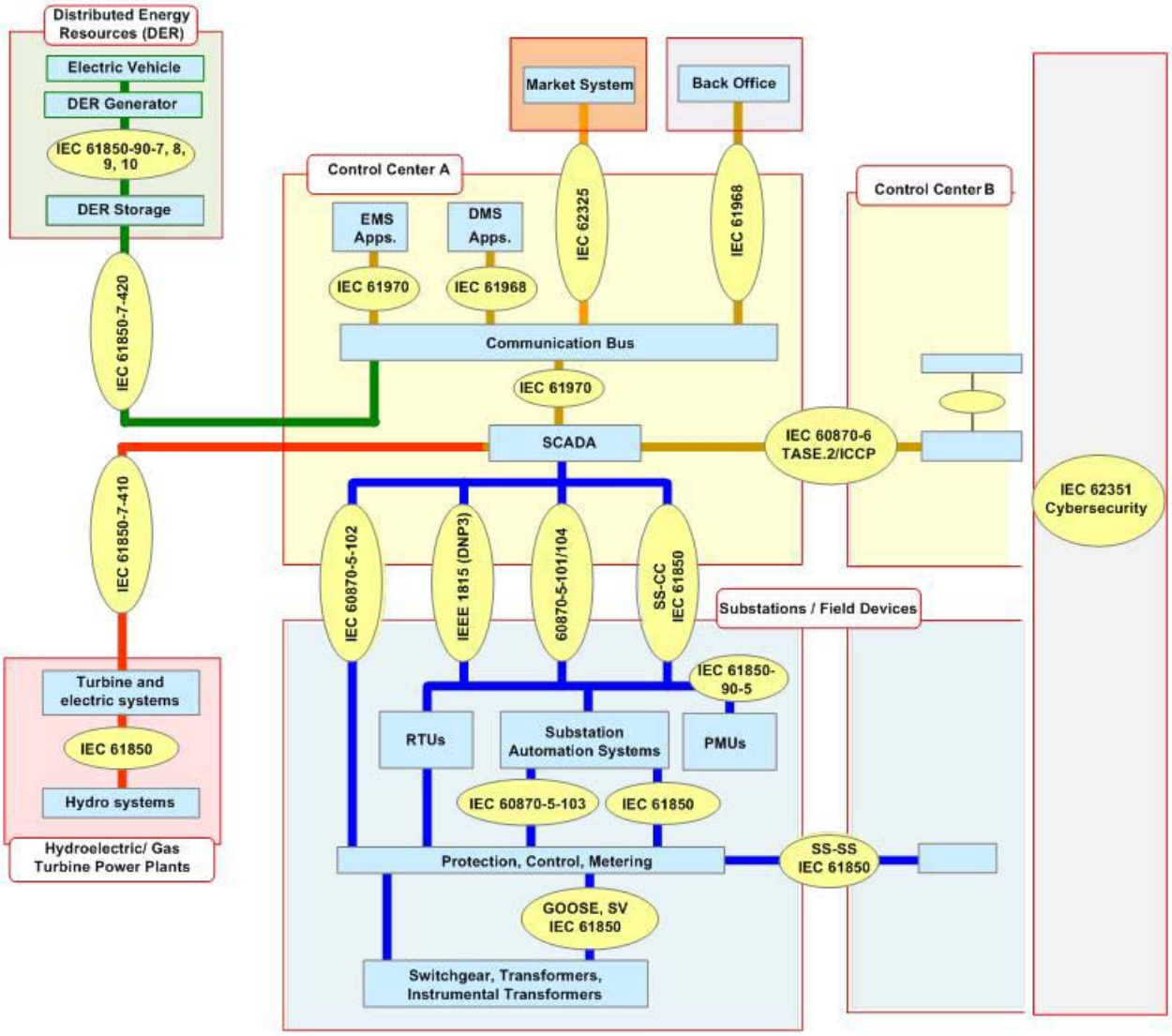


Figure 18: IEC TC57 Communication Standards Architecture

6.7.5 IEC 62351-11: Security for XML Files

This standard which is just starting development (June 2012) defines the security for XML-based files. Currently, XML files, such as those created by CIM and by IEC 61850 SCL, are transferred electronically/manually without any security signature that indicates the authenticity of the document or that provides an indication that the file's contents may have been tampered with. Therefore, the key primary objectives are:

- Provide a mechanism to authenticate the source of the file.
- Provide a mechanism for tamper detection.
- Provide these security mechanisms in a manner that maintains as much compatibility with the current CIM, SCL, and other XML formats as possible.

An additional security issue requires the development of a use case to analyze how a source of data can identify what data may or may not be made available to other entities in addition to the initial receiving entity.

7. Example of Security for IEC 61850 using IEC 62351

An example of security for Distributed Energy Resources (DER) using the IEC 61850 information models mapped to different protocols is shown in Figure 19.

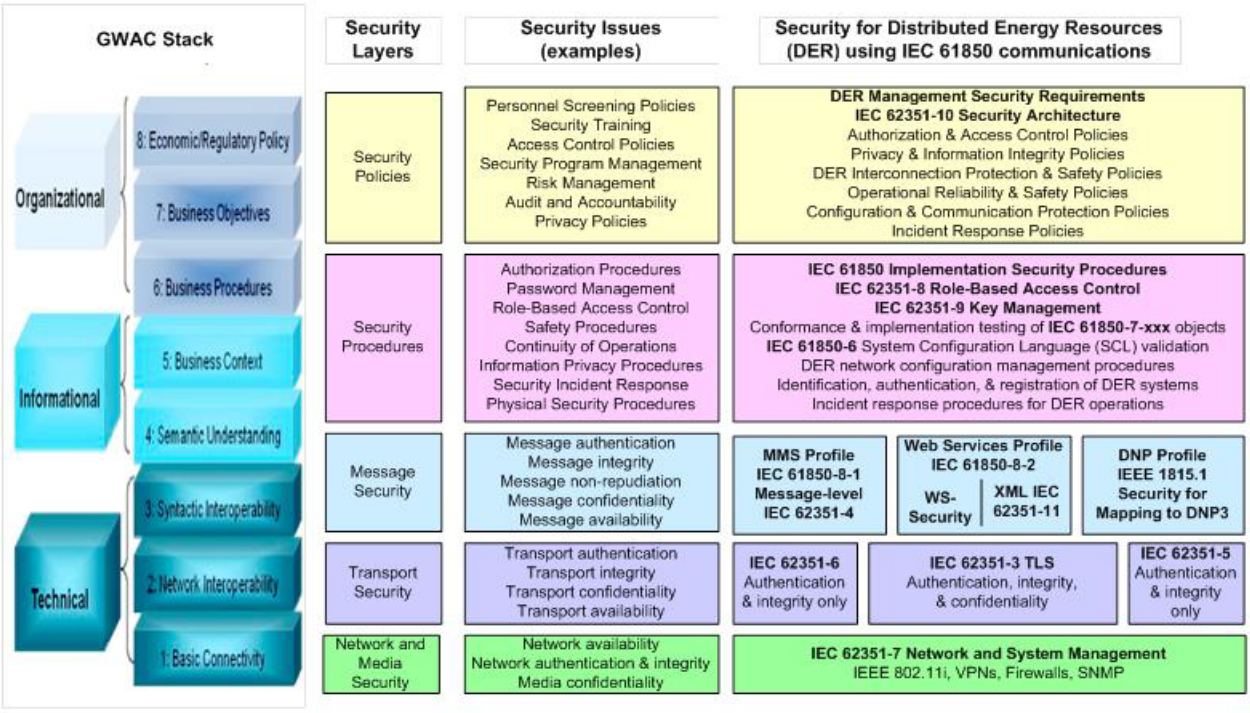


Figure 19: Security for Distributed Energy Resources (DER) using IEC 61850 communications and IEC 62351