TECHNICAL SPECIFICATION

IEC TS 62351-1

First edition
2007-05

Power systems management and associated information exchange – Data and communications security

Part 1: Communication network and system security – Introduction to security issues

Reference number
IEC/TS 62351-1:2007(E)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

- Catalogue of IEC publications: www.iec.ch/searchpub

The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub

Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.

- Customer Service Centre: www.iec.ch/webstore/custserv

If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:

Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

TECHNICAL SPECIFICATION

IEC TS 62351-1

First edition
2007-05

Power systems management and associated information exchange – Data and communications security

Part 1: Communication network and system security – Introduction to security issues

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

PRICE CODE V

For price, see current catalogue

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE – DATA AND COMMUNICATIONS SECURITY

Part 1: Communication network and system security – Introduction to security issues

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as “IEC Publication(s)”). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.

2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.

3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.

4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.

5) IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.

6) All users should ensure that they have the latest edition of this publication.

7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.

8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

The main task of IEC technical committees is to prepare International Standards. In exceptional circumstances, a technical committee may propose the publication of a technical specification when

- the required support cannot be obtained for the publication of an International Standard, despite repeated efforts, or
- The subject is still under technical development or where, for any other reason, there is the future but no immediate possibility of an agreement on an International Standard.

Technical specifications are subject to review within three years of publication to decide whether they can be transformed into International Standards.

IEC 62351-1, which is a technical specification, has been prepared by IEC technical committee 57: Power systems management and associated information exchange.

The text of this technical specification is based on the following documents:

Enquiry draft	Report on voting
57/802/DTS	57/850/RVC

Full information on the voting for the approval of this technical specification can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all parts of the IEC 62351 series, under the general title *Power systems management and associated information exchange – Data and communications security*, can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the maintenance result date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- transformed into an International standard,
- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

A bilingual edition of this document may be issued at a later date.

POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE – DATA AND COMMUNICATIONS SECURITY

Part 1: Communication network and system security – Introduction to security issues

1 Scope and object

1.1 Scope

The scope of the IEC 62351 series is information security for power system control operations. The primary objective is to "*Undertake the development of standards for security of the communication protocols defined by 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*."

1.2 Object

Specific objectives include:

- IEC 62351-1 provides an introduction to the remaining parts of the standard, primarily to introduce the reader to various aspects of information security as applied to power system operations.
- IEC 62351-3 to IEC 62351-6 specify security standards for the IEC TC 57 communication protocols. These can be used to provide various levels of protocol security, depending upon the protocol and the parameters selected for a specific implementation. They have also been design for backward compatibility and phased implementations.
- IEC 62351-7 addresses one area among many possible areas of end-to-end information security, namely the enhancement of overall management of the communications networks supporting power system operations.
- Other parts are expected to follow to address more areas of information security.

The justification for developing these information security standards is that safety, security, and reliability have always been important issues in the design and operation of systems in the power industry, and information 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. In addition, inadvertent actions (e.g. carelessness and natural disasters) can be as damaging as deliberate actions. Recently, the additional threat of terrorism has become more visible.

Although many definitions of "end-to-end" security exist, one (multi-statement) standard definition is "*1. Safeguarding information in a secure telecommunication system by cryptographic or protected distribution system means from point of origin to point of destination. 2. Safeguarding information in an information system from point of origin to point of destination*"[1]. Using this definition as a basis, the first four standards address the security enhancements for IEC TC 57 communication profiles, since these were identified as the obvious first steps in securing power system control operations. However, these security enhancements can only address the security requirements between two systems, but does not address true "end-to-end" security that covers internal security requirements, including

[1] ATIS: an expansion of FS-1037C which is the US Federal Government standard glossary for telecommunications terms.

security policies, security enforcement, intrusion detection, internal system and application health, and all the broader security needs.

Therefore, the final sentence in the scope/purpose statement is very important: it is recognized that the addition of firewalls or just the simple use of encryption in 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, authorized access to sensitive market data, reliable and timely information on equipment functioning and failures, backup of critical systems, and audit capabilities that permit detection and reconstruction of crucial events.

2 Normative references

The following documents contain provisions which, through reference in this text, constitute provisions of this part of the IEC 62351 standard series.

IEC 60870-5 (all parts), *Telecontrol equipment and systems – Part 5: Transmission protocols*

IEC 60870-6 (all parts), *Telecontrol equipment and systems – Part 6: Telecontrol protocols compatible with ISO standards and ITU-T recommendations* [2]

IEC 61850 (all parts), *Communication networks and systems in substations*[3]

3 Terms, definitions and abbreviations

For the purposes of this part of IEC 62351, the terms and definitions given in IEC 62351-2 apply.

4 Background for information security standards

4.1 Rationale for addressing information security in power system operations

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 centres. Who could possibly care about the megawatts on a line, or have the knowledge of how to read the idiosyncratic bits and bytes of 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

[2] Also known as Inter-Control Centre Communications Protocol (ICCP) allows for data exchange over Wide Area Networks (WANs) between a utility control centre and other control centres, other utilities, power pools, regional control centres, and Non-Utility Generators.

[3] IEC 61850 which is used for protective relaying, substation automation, distribution automation, power quality, distributed energy resources, substation to control centre, 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.

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 now have to 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. Therefore, the reliability of the power system is increasingly affected by any problems that the information infrastructure might suffer.

4.2 IEC TC 57 data communications protocols

The International Electrotechnical Commission (IEC) Technical Committee (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 TC 57 has developed three widely accepted protocol standards, and has been the source of a fourth protocol. The three 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 (IEC 60870-5-101) and over networks (IEC 60870-5-104). **DNP3** was derived from IEC 60870-5 for use in the USA 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 ICCP)** which is used internationally for communications between control centres and often for communications between SCADA systems and other engineering systems within control centres.
- **IEC 61850** which is used for protective relaying, substation automation, distribution automation, power quality, distributed energy resources, substation to control centre, 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.

These protocols are now widely used in the electric power industry. However, they were developed before information security became a major issue for the industry, so no security measures were included in the original standards.

4.3 History of the Development of these Security Standards

By 1997, IEC TC 57 recognized that security would be necessary for these protocols. It therefore first established a temporary group to study the issues of security. This group published a IEC/TR 62210 on the security requirements. One of the recommendations of

IEC/TR 62210 was to form a Working Group to develop security standards for the IEC TC 57 protocols and their derivatives.

The International Standards Organization (ISO) Common Criteria were originally selected as the method for determining the security requirements. This approach uses the concept of a Target of Evaluation (TOE) as the focus of a security analysis. However, determining what the characteristics of the TOE to protect became very cumbersome, given the multiplicity of different power system environments and the varying security needs, so ultimately it was not used. Threat-mitigation analysis (determining the most common threats and then developing security countermeasures for those threats) was used instead.

Therefore, IEC TC 57 WG 15 was formed in 1999, and has undertaken this work. The WG 15 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 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. Recently, 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 data, 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.

5 Security issues for the IEC 62351 series

5.1 General information on security

This informative clause provides additional information on security issues that are not explicitly covered by these normative standards, but may be useful for understanding the context and scope of the normative standards.

5.2 Types of security threats

5.2.1 General

Security threats are generally viewed as the potential for attacks against assets. These assets can be physical equipment, computer hardware, buildings, and even people. However, in the cyber world, assets also include information, databases, and software applications. Therefore countermeasures to security threats should include protection against both physical attacks as well as cyber attacks.

Security threats to assets can result from inadvertent events as well as deliberate attacks. In fact, often more actual damage can result from safety breakdowns, equipment failures, carelessness, and natural disasters than from deliberate attacks. However, the reactions to successful deliberate attacks can have tremendous legal, social, and financial consequences that could far exceed the physical damage.

Utilities are accustomed to worrying about equipment failures and safety-related carelessness. Natural disasters are taken into consideration, particularly for utilities that commonly experience hurricanes, earthquakes, cyclones, ice storms, etc., even though these are looked upon as beyond the control of the utility. What is changing is the importance of protecting information which is becoming an increasingly important aspect of safe, reliable, and efficient power system operations.

Security risk assessment is vital in determining exactly what needs to be secured against what threats and to which degree of security. The key is determining the cost-benefit: "one size does not fit all"[4] (substations), layers of security are better than a single solution, and ultimately no protection against attacks can ever be completely absolute. Nonetheless, there is a significant space between the extremes from doing nothing to doing everything, to provide the level of security needed for modern utility operations.

The benefits also can flow the other way. If additional security is implemented against possible deliberate attacks, this monitoring can be used to improve safety, minimize carelessness, and improve the efficiency of equipment maintenance.

The following Subclauses discuss some of the most important threats to understand and to protect against. Most of these are covered by the IEC 62351 series, at least at the monitoring level.

5.2.2 Inadvertent threats

5.2.2.1 Safety failures

Safety has always been a primary concern for electric power utilities, particularly for those field crews working in the high voltage environments of substations. Meticulous procedures have been developed and refined over and over again to improve safety. Although these procedures are the most important component of a safety program, monitoring of the status of key equipment and the logging/alarming of compliance to the safety procedures through electronic means can enhance safety to a significant degree, and can benefit other purposes as well.

In particular, although access measures which permit only authorized personnel into substations have been implemented primarily for safety reasons, electronic monitoring of these safety measures can also help to prevent some deliberate attacks, such as vandalism and theft.

5.2.2.2 Equipment failures

Equipment failures are the most common and expected threats to the reliable operation of the power system. Significant work has been undertaken over the years to monitor the status of substation equipment, such as oil temperature, cooling systems, frequency deviations, voltage levels, and current overloads. This part of IEC 62351 does not focus on these types of monitoring except where the additional information can provide additional physical security.

However, often the monitoring of the physical status of equipment can also benefit maintenance efficiency, possible prevention of certain types of equipment failures, real-time detection of failures not previously monitored, and forensic analysis of equipment failure processes and impacts. Therefore, the total cost-benefit of some monitoring of physical security can be improved by taking these additional consequences into account.

[4] In the sense that one single solution cannot be used for all situations, so multiple solutions should be allowed.

5.2.2.3 Carelessness

Carelessness is one of the "threats" to protecting assets in substations, whether it is permitting tailgating into a substation or not locking doors or inadvertently allowing unauthorized personnel to access passwords, keys, and other security safeguards. Often this carelessness is due to complacency ("no one has ever harmed any equipment in a substation yet") or laziness ("why bother to lock this door for the few moments I am going into the other area") or irritation ("these security measures are impacting my ability to do my job").

5.2.2.4 Natural disasters

Natural disasters, such as storms, hurricanes, and earthquakes, can lead to widespread power system failures, safety breaches, and opportunities for theft, vandalism, and terrorism. Monitoring of the physical and informational status of field facilities and equipment in real-time can provide utilities with the "eyes and ears" to understand what is taking place and to take ameliorating actions to minimize the impact of these natural disasters on power system operations.

5.2.3 Deliberate threats

5.2.3.1 General

Deliberate threats can cause more focused damage to facilities and equipment in substations than the inadvertent threats. The incentives for these deliberate threats are increasing as the results from successful attacks can have increasingly economic and/or "socio/political" benefits to the attackers. Sophisticated monitoring of facilities and equipment can help prevent some of these threats, while ameliorating the impact of successful attacks through real-time notifications and forensic trails.

5.2.3.2 Disgruntled employee

Disgruntled employees are one of the primary threats for attacks on power system assets. Unhappy employees who have the knowledge to do harm can cause significantly more damage than a non-employee, particularly in the power system industry where many of the systems and equipment are very unique to the industry.

5.2.3.3 Industrial espionage

Industrial espionage in the power system industry is becoming more of a threat as deregulation and competition involving millions of dollars provide growing incentives for unauthorized access to information – and the possible damaging of equipment for nefarious purposes. In addition to financial gains, some attackers could gain "socio/political" benefits through "exposing" the incompetence or unreliability of competitors.

5.2.3.4 Vandalism

Vandalism can damage facilities and equipment with no specific gain to the attackers other than the act of doing it, and the proof to themselves and others that they can do it. Often, the vandals are unaware of or do not care about the possible consequences of their actions.

Monitoring the access to locked facilities and alarming any access anomalies in real-time can help prevent most vandalism. However, some vandalism, such as shooting equipment in the yard from outside the substation, or turning off equipment and software applications, would require additional types of monitoring.

5.2.3.5 Cyber hackers

Hackers are people who seek to breach cyber security for gain. This gain may be directly monetary, industrial knowledge, political, social, or just an individual challenge to see if the hacker can gain access. Most hackers use the Internet as their primary gateway to entry, and therefore most utilities use a variety of firewalls, isolation techniques, and other countermeasures to separate power system operation systems from the Internet.

In the public's eye, cyber security is often seen only as protection against hackers and their associated problems, computer viruses and worms. With the computer systems for power operations presumably kept isolated from the Internet, many utility personnel do not see any reason for adding security measures to these systems. However, as clearly seen from these Subclauses, this may not be true anymore as networking becomes more prevalent and additional information access requirements grow (e.g. vendor remote access, maintenance laptop access, protective relay engineer access for retrieving special data, etc.).

5.2.3.6 Viruses and worms

Like hackers, viruses and worms typically attack via the Internet. However, some viruses and worms can be embedded in software that is loaded into systems that have been isolated from the Internet, or could possibly be transmitted over secure communications from some insecure laptop or other system. They could include man-in-the-middle viruses, spyware for capturing power system data, and other Trojan horses.

5.2.3.7 Theft

Theft has a straightforward purpose – the attackers take something (equipment, data, or knowledge) that they are not authorized to take. Generally, the purpose has financial gain as the motive, although other motives are possible as well.

Again, monitoring access to locked facilities and alarming anomalies in the physical status and health of equipment (e.g. not responding or disconnected) are the primary methods for alerting personnel that theft is possibly being committed.

5.2.3.8 Terrorism

Terrorism is the least likely threat but the one with possibly the largest consequences since the primary purpose of terrorism is to inflict the greatest degree of physical, financial, and socio/political damage.

Monitoring and alarming anomalies to access (including physical proximity) to substation facilities is possibly the most effective means to alert personnel to potential terrorist acts, such as physically blowing up a substation or other facility. However, terrorists could become more sophisticated in their actions, and seek to damage specific equipment or render critical equipment inoperative in ways that could potentially do more harm to the power system at large than just blowing up one substation. Therefore, additional types of monitoring are critical, including the status and health of equipment.

5.3 Security requirements, threats, vulnerabilities, attacks, and countermeasures

5.3.1 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. In each case, authorization requires authentication of the users as a basic premise:

- **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 or accountability** – preventing the denial of an action that took place or the claim of an action that did not take place.

5.3.2 Security threats

In general, there are four types of cyber security threats:

- Unauthorized access to information.
- Unauthorized modification or theft of information.
- Denial of service.
- Repudiation/unaccountability.

There are, however, many different types of vulnerabilities and methods of attacks against these vulnerabilities by which these threats might be successful. Security countermeasures shall take into account these different types of vulnerabilities and attack methods.

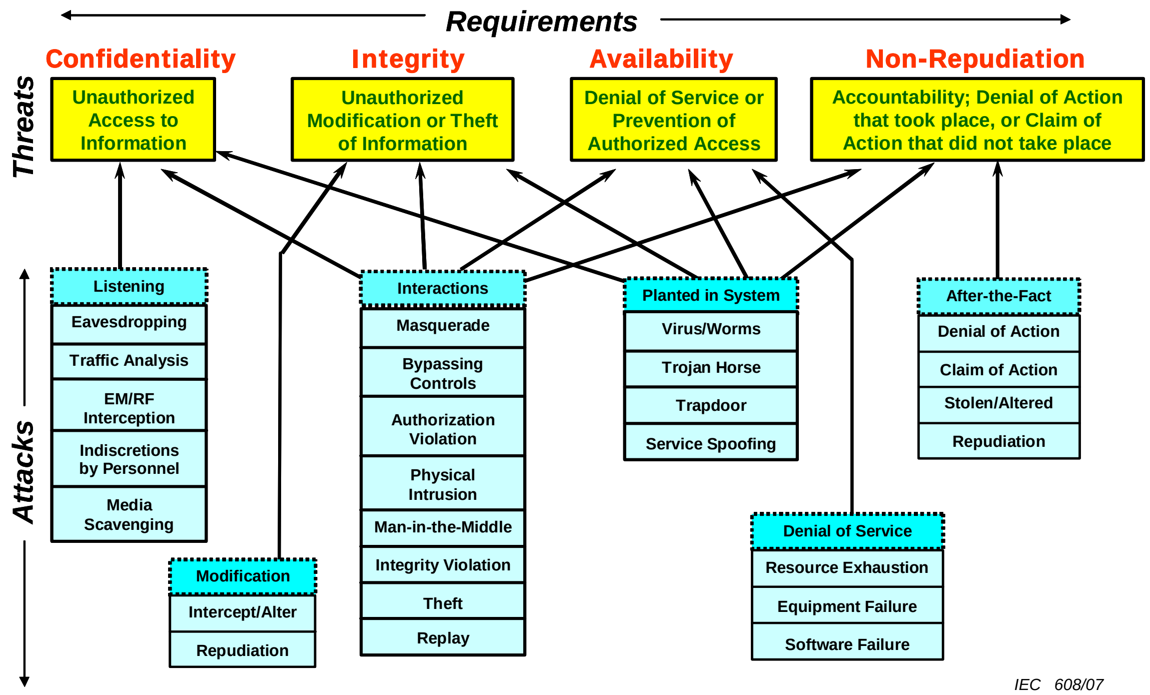
5.3.3 Security vulnerabilities

Cyber security vulnerabilities refer to weaknesses or other opening in a system that could permit deliberate or inadvertent unauthorized actions to realize a threat. Vulnerabilities may result from bugs or design flaws in the system, but can also result from equipment failures and physical actions. A vulnerability can exist either only in theory, or could have a known exploit.

5.3.4 Security attacks

The threats can be realized by many different types of attacks, some of which are illustrated in Figure 1. 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.

In addition, a “chain of attacks” in which a sequence of attacks, possibly involving different assets and possibly taking place over time, can also realize a given threat.

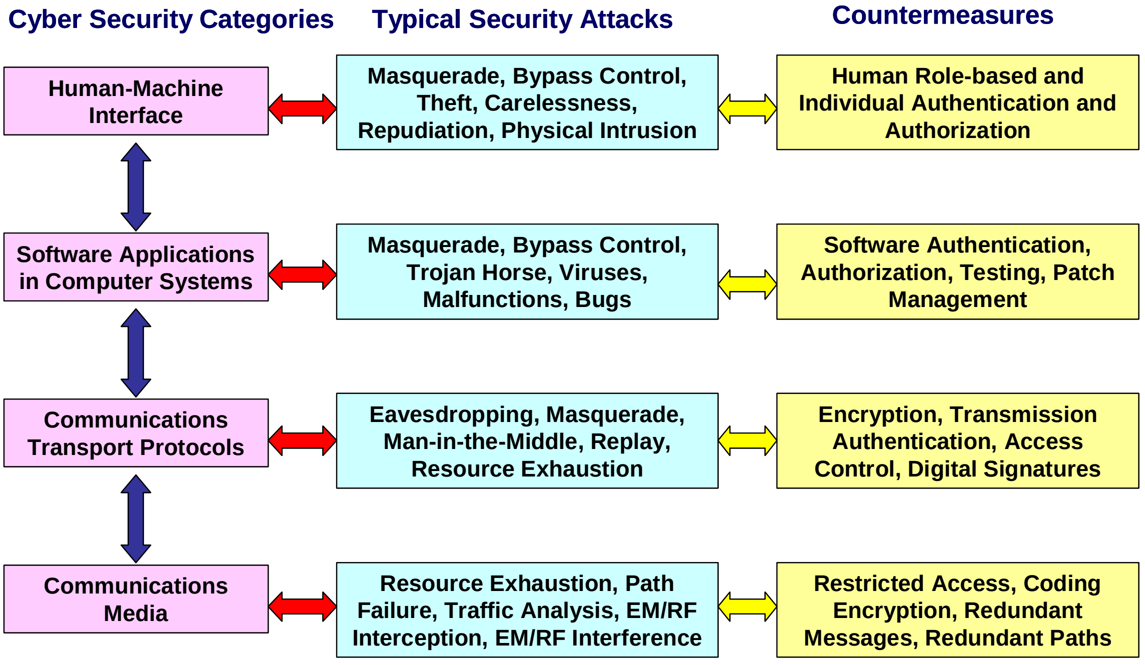


IEC 608/07

Figure 1 – Security requirements, threats, and possible attacks

5.3.5 Security Categories

From one perspective on security, cyber security can be categorized into four areas (see Figure 2). These categories are illustrated below:


Cyber Security Categories
Typical Security Attacks
Countermeasures
Human-Machine Interface
Masquerade, Bypass Control, Theft, Carelessness, Repudiation, Physical Intrusion
Human Role-based and Individual Authentication and Authorization
Software Applications in Computer Systems
Masquerade, Bypass Control, Trojan Horse, Viruses, Malfunctions, Bugs
Software Authentication, Authorization, Testing, Patch Management
Communications Transport Protocols
Eavesdropping, Masquerade, Man-in-the-Middle, Replay, Resource Exhaustion
Encryption, Transmission Authentication, Access Control, Digital Signatures
Communications Media
Resource Exhaustion, Path Failure, Traffic Analysis, EM/RF Interception, EM/RF Interference
Restricted Access, Coding Encryption, Redundant Messages, Redundant Paths

IEC 609/07

Figure 2 – Security categories, typical attacks, and common countermeasures

Usually all four of these categories need to have security measures applied in order to achieve "end-to-end" security. Just securing one category will typically not be adequate. For instance, just implementing a Virtual Private Network (VPN) only handles threats to the communications transport protocols, and does not prevent one person masquerading as another person, nor does it prevent a malicious software application in the host computer from communicating over the VPN to the device in the field.

These security measures should be carefully integrated with each other so that inadvertent problems do not occur.

5.3.6 Security Countermeasures

Security countermeasures, as illustrated in Figures 3 to 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. An overview of all countermeasures is illustrated in Figure 7.

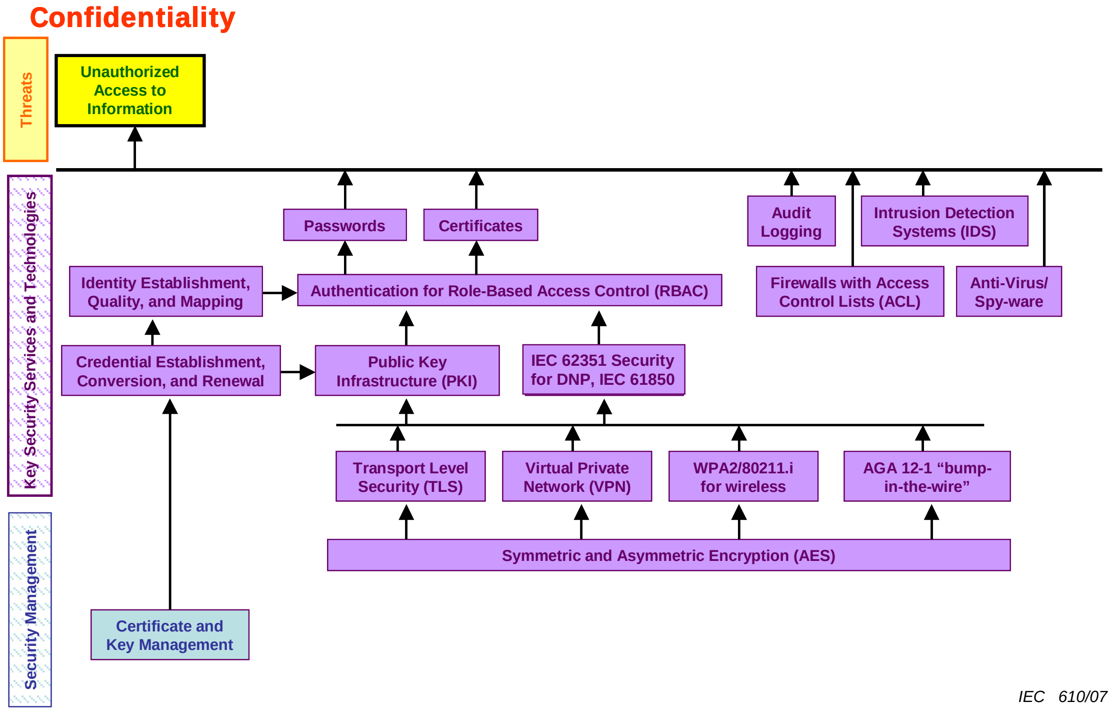

Confidentiality
Threats
Unauthorized Access to Information
Key Security Services and Technologies
Security Management
Passwords
Certificates
Audit Logging
Intrusion Detection Systems (IDS)
Identity Establishment, Quality, and Mapping
Authentication for Role-Based Access Control (RBAC)
Firewalls with Access Control Lists (ACL)
Anti-Virus/ Spy-ware
Credential Establishment, Conversion, and Renewal
Public Key Infrastructure (PKI)
IEC 62351 Security for DNP, IEC 61850
Transport Level Security (TLS)
Virtual Private Network (VPN)
WPA2/80211.i for wireless
AGA 12-1 "bump-in-the-wire"
Symmetric and Asymmetric Encryption (AES)
Certificate and Key Management
IEC 610/07

Figure 3 – Confidentiality security countermeasures

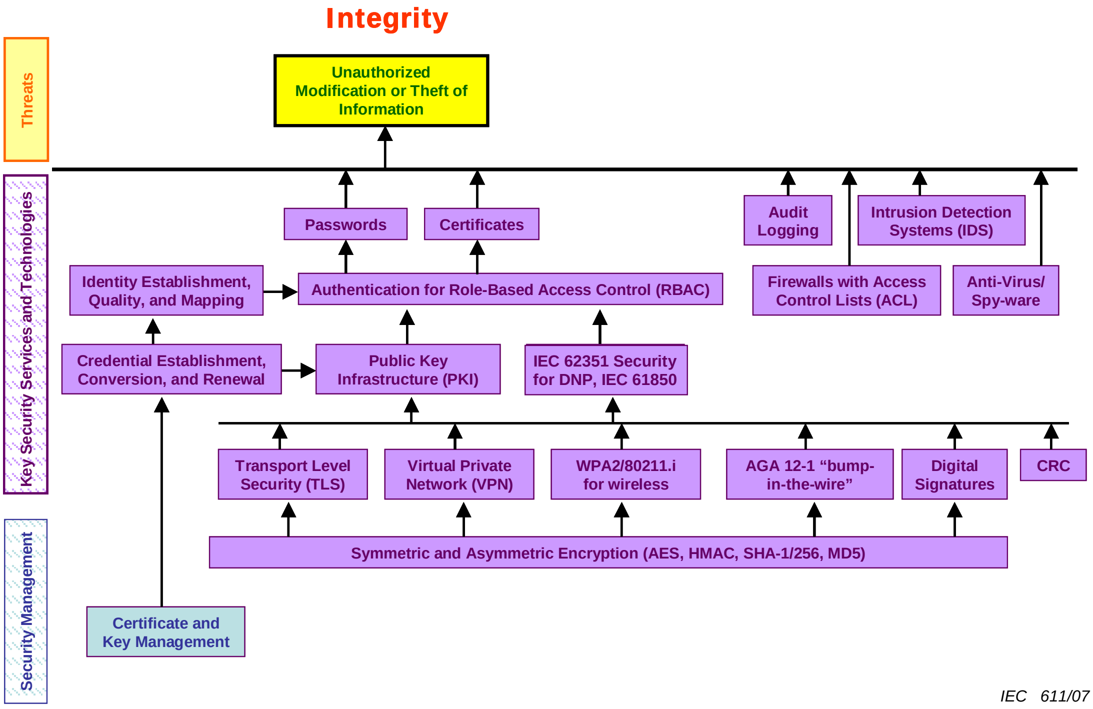

Integrity
Threats
Unauthorized Modification or Theft of Information
Key Security Services and Technologies
Security Management
Passwords
Certificates
Audit Logging
Intrusion Detection Systems (IDS)
Identity Establishment, Quality, and Mapping
Authentication for Role-Based Access Control (RBAC)
Firewalls with Access Control Lists (ACL)
Anti-Virus/ Spy-ware
Credential Establishment, Conversion, and Renewal
Public Key Infrastructure (PKI)
IEC 62351 Security for DNP, IEC 61850
Transport Level Security (TLS)
Virtual Private Network (VPN)
WPA2/80211.i for wireless
AGA 12-1 "bump-in-the-wire"
Digital Signatures
CRC
Symmetric and Asymmetric Encryption (AES, HMAC, SHA-1/256, MD5)
Certificate and Key Management
IEC 611/07

Figure 4 – Integrity security countermeasures

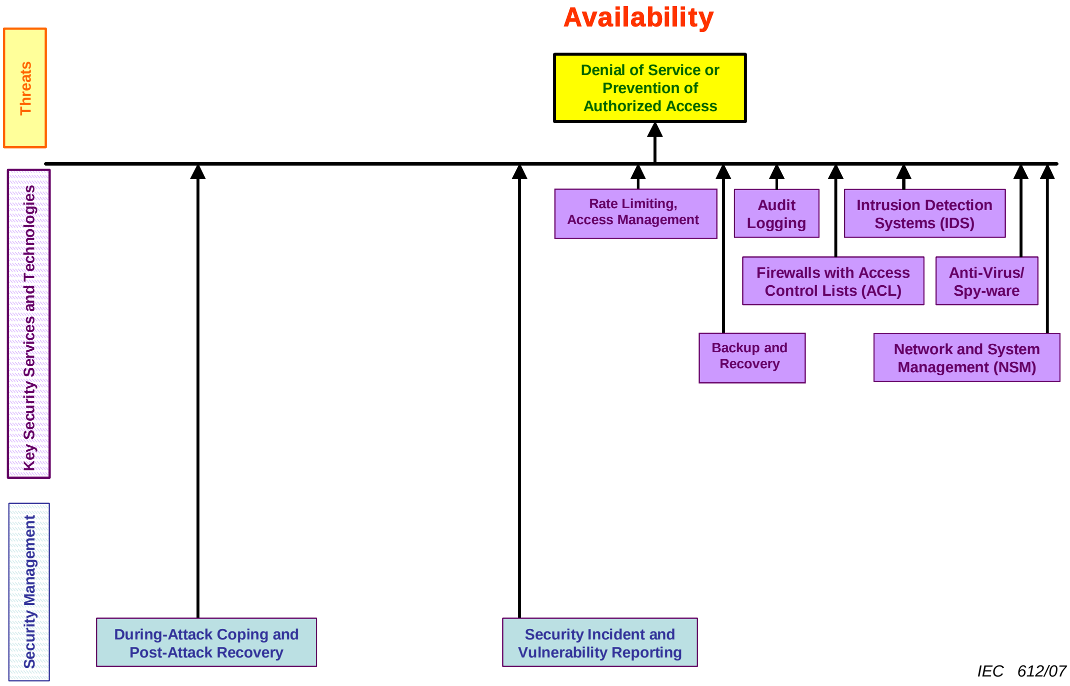

Availability
Threats
Key Security Services and Technologies
Security Management
Denial of Service or Prevention of Authorized Access
Rate Limiting, Access Management
Audit Logging
Intrusion Detection Systems (IDS)
Firewalls with Access Control Lists (ACL)
Anti-Virus/ Spy-ware
Backup and Recovery
Network and System Management (NSM)
During-Attack Coping and Post-Attack Recovery
Security Incident and Vulnerability Reporting
IEC 612/07

Figure 5 – Availability security countermeasures

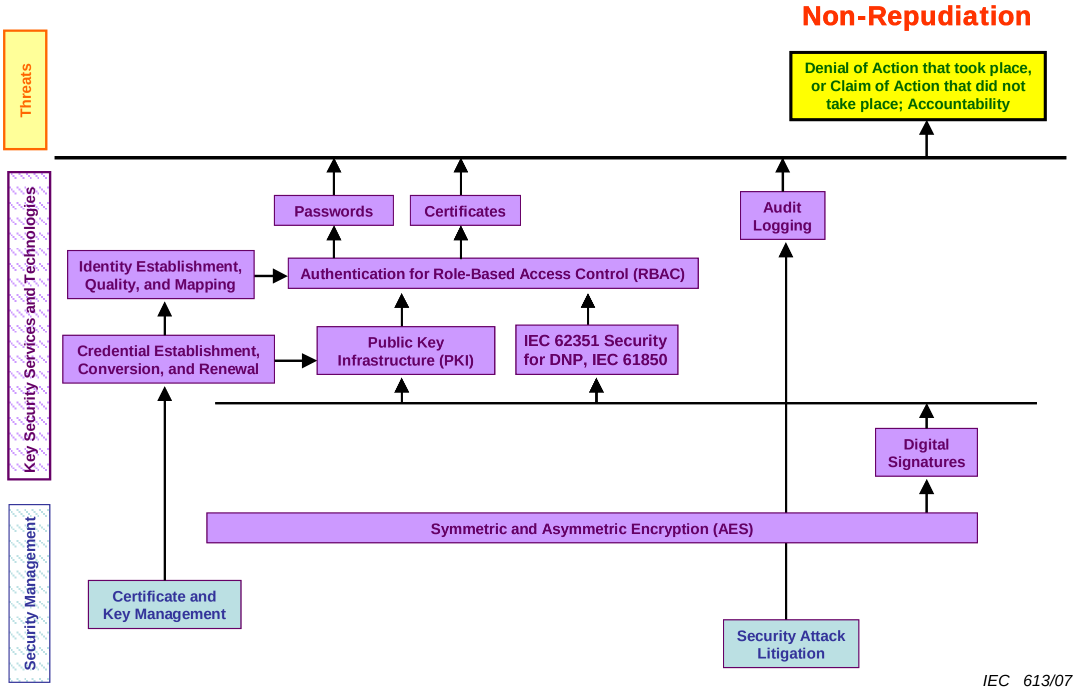
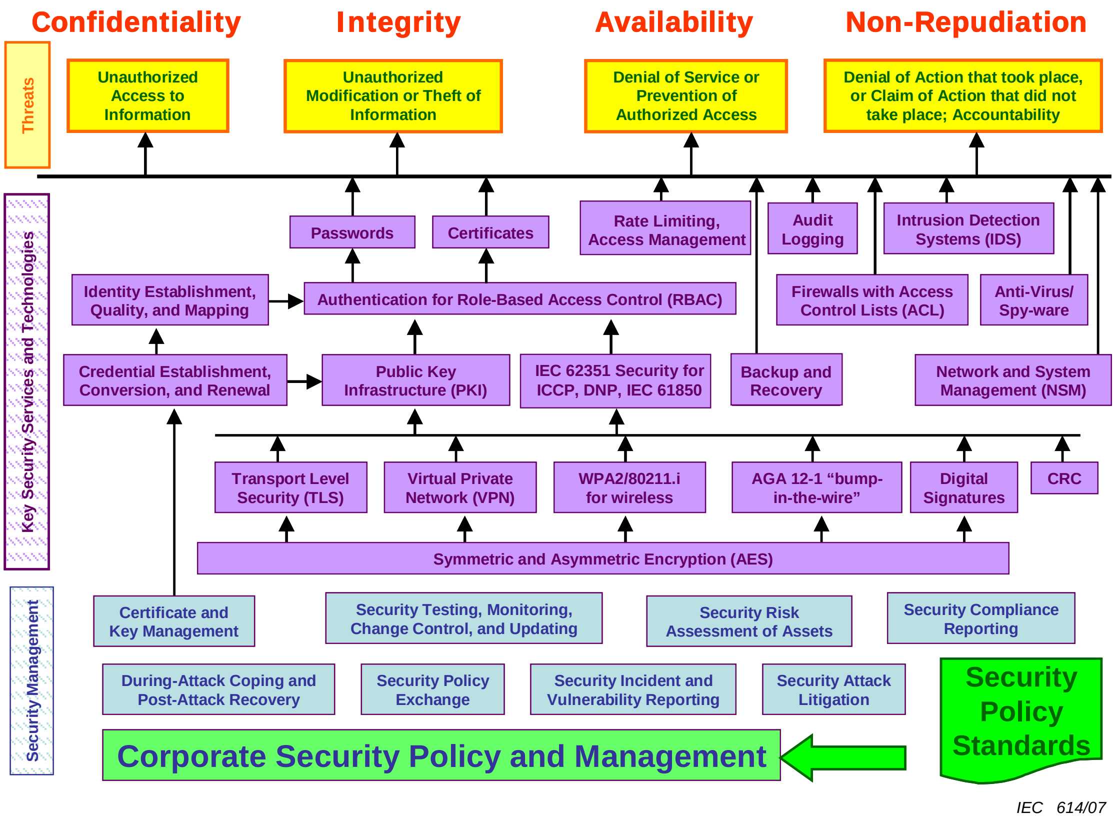

Non-Repudiation
Threats
Key Security Services and Technologies
Security Management
Denial of Action that took place, or Claim of Action that did not take place; Accountability
Passwords
Certificates
Audit Logging
Identity Establishment, Quality, and Mapping
Authentication for Role-Based Access Control (RBAC)
Credential Establishment, Conversion, and Renewal
Public Key Infrastructure (PKI)
IEC 62351 Security for DNP, IEC 61850
Digital Signatures
Symmetric and Asymmetric Encryption (AES)
Certificate and Key Management
Security Attack Litigation
IEC 613/07

Figure 6 – Non-repudiation security countermeasures


Confidentiality
Integrity
Availability
Non-Repudiation
Threats
Unauthorized Access to Information
Unauthorized Modification or Theft of Information
Denial of Service or Prevention of Authorized Access
Denial of Action that took place, or Claim of Action that did not take place; Accountability
Key Security Services and Technologies
Passwords
Certificates
Rate Limiting, Access Management
Audit Logging
Intrusion Detection Systems (IDS)
Identity Establishment, Quality, and Mapping
Authentication for Role-Based Access Control (RBAC)
Firewalls with Access Control Lists (ACL)
Anti-Virus/ Spy-ware
Credential Establishment, Conversion, and Renewal
Public Key Infrastructure (PKI)
IEC 62351 Security for ICCP, DNP, IEC 61850
Backup and Recovery
Network and System Management (NSM)
Transport Level Security (TLS)
Virtual Private Network (VPN)
WPA2/80211.i for wireless
AGA 12-1 "bump-in-the-wire"
Digital Signatures
CRC
Symmetric and Asymmetric Encryption (AES)
Security Management
Certificate and Key Management
Security Testing, Monitoring, Change Control, and Updating
Security Risk Assessment of Assets
Security Compliance Reporting
During-Attack Coping and Post-Attack Recovery
Security Policy Exchange
Security Incident and Vulnerability Reporting
Security Attack Litigation
Security Policy Standards
Corporate Security Policy and Management

IEC 614/07

Figure 7 – Overall security: security requirements, threats, countermeasures, and management

These figures are informative only; not all items illustrated in them are addressed in the IEC 62351 series.

In Figures 3 to 7, the four security requirements (confidentiality, integrity, availability, and non-repudiation) are shown at the top of each picture. The basic security threats are shown below each requirement. The key security services and technologies used to counter these threats are shown in the boxes immediately below the threats. These are just examples of commonly used security measures, with arrows indicating which technologies and services participate in the supporting the security measures above them. For instance, encryption is used in many security measures, including TLS, VPNs, wireless security, and "bump-in-the-wire" technologies. These in turn support IEC 62351 security standards and PKI, which are commonly used for authentication so that passwords and certificates can be assigned. At the bottom of each figure, below the security services and technologies, are the security management and security policies which provide the underpinning for all security measures.

5.3.7 Decomposing the security problem space

Security encompasses an enormously complex and multi-dimensional set of issues. There are no standardized or clearly defined mechanisms to decompose the security problem space, and therefore the analysis and deployment of appropriate and complete security measures in a cost-effective manner are often perceived to be impossible tasks.

For instance, two major discussion/analysis methods have been used in the past for analyzing security requirements: Enterprise-based analysis (one set of security measures are applied to an entire enterprise) and Technology/Threat-based analysis (one set of technologies, such as passwords and VPNs, is applied to all systems. Both approaches involve obvious pitfalls. Trying to develop a single set of security measures for an entire enterprise can cause either exaggerated or inadequate security for some areas of the enterprise. In addition, an enterprise is continuously evolving and changing, and may encompass more than one business entity where a single set of security policies and technologies cannot be enforced. The Technology/Threat-based analysis assumes security measures will not change, and that one solution is adequate for all situations. However, this is particularly not true in the power systems operations environment. One size simply does not fit all. In addition, 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. Thus any security decisions require a large amount of coordination and tend to make the security process frustrating if not totally impossible.

However, the security problem can be decomposed into smaller regions of security analysis/management. Three different approaches have been used, depending upon the issues involved. These are:

- **Physical security perimeter:** The physical six-wall border surrounding computer rooms, telecommunications rooms, operations centres, and other locations in which critical cyber assets are housed and for which access is controlled. This perimeter can be used for physically protecting assets.
- **Electronic security perimeter:** The logical border surrounding a network to which critical cyber assets are connected and for which access is controlled. This perimeter can be used for applying cyber security measures.
- **Security domain**: The area that organizationally belongs to one section, department, company, or other grouping where the security requirements are the same or at least under the control of the same entity. The security domain concept in particular allows a set of resources to be managed (from a security perspective) independently, since all assets within one Security Domain belongs to one organization.

This partitioning of the security problem space into manageable pieces can go a long way toward helping an organization develop appropriate and cost-effective security measures. However, this raises the issue of how to provide a security mechanism for inter-domain exchanges or across security perimeters. To solve this issue, special inter-domain security services are needed to cross these boundaries.

5.4 Importance of security policies

Security policy documents describe the primary threats to the company's facilities, explain the reasons for involving the employees in maintaining the security of company information, and define the rights and responsibilities of company employees, including the users and the IT staff.

As adjunct documents to the security policy, detailed security requirements should be developed to address specific security issues related to specific technologies and applications, including IT network configuration considerations, network performance issues, firewall locations and settings, data security classifications, protocol security requirements, and password/certificate assignments.

One of the primary functions of this document is as a training tool. Employees will support security measures more willingly and more completely if they understand the real-world threats, the security risks associated with everyday functions, and the validity of the security measures they are being asked to take in order to minimize these risks. The security policy should also be clear on the disciplinary actions which could be taken if the policy is not followed.

A security policy document should be a living document to reflect new technologies and new security requirements. As such, it should be reviewed and updated at least once a year, or whenever new developments take place in the security industry or in IT facilities.

5.5 Security risk assessment

Another issue, and typically the most daunting, is how to decide what needs to be secured and to what degree it needs to be secured. Some may contend that every asset needs to be 100 % secured, but this is usually impractical. In addition, this approach makes security deployment/adoption extremely costly and could prevent entities from even attempting to deploy minimal security.

Again, one size does not fit all: all assets do not need to be completely and invincibly secured, although all assets *could* be secured. However, all assets should be assessed with regard to the need and degree of security.

Security risk assessment identifies the degree of damage that a security breach might cause, and analyzes this damage (financial, safety, and social) against the costs of implementing and maintaining security countermeasures. Therefore, security risk assessment is a key security function that should be performed in advance of any security deployment.

5.6 Understanding the security requirements and impact of security measures on power system operations

5.6.1 Security challenges in 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, the threat of denial-of-service is far more important than in many typical Internet transactions.
- Many communication channels used in the power industry are narrowband and often, the end equipment is constrained in memory and computer power, 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, certificate revocation, and some other security measures difficult to implement.
- Many systems are connected by multi-drop communication channels, so network security measures typical in industry cannot work.
- Although wireless communications are becoming widely used for many applications, utilities will need to be very careful where and for what functions they implement these wireless technologies, partly because of the noisy electrical environment of substations (potential impacts to availability), and partly because of the very rapid and extremely reliable response required by some applications (throughput). Although security measures are available for many wireless systems, these can increase the overhead (albeit in a similar manner to wired media).

5.6.2 Key management and certificate revocation

Given the large territories, the narrowband communications, the limited capabilities of some end equipment, and the remoteness of much equipment from easy access by personnel, the management of cryptographic secret keys is an issue that most other industries, including the manufacturing industry, do not really face. Secret keys, whether part of a public-private key system or symmetric secret key system or used for “bump-in-the-wire” encryption devices, should be placed into the end equipment in a secure manner.

One option is for technicians to physically travel to the location of the equipment and download each secret key into each piece of equipment. This option is appropriate for initial installations, but could become a serious burden if the key needs to be updated regularly. Another option is for a “key server” to be co-located with the end equipment and interconnected with that equipment via a local network. The key server could then use some separate, wideband, secure communications to download new secret keys, which it can then issue to the different pieces of equipment.

Certificate revocation has a similar problem to key management, except that the constraint is not the narrow bandwidth of the communications, but the fact that no operational equipment can be connected to the internet. Normally certificate revocation is handled by a trusted certificate manager who issues revocations over the internet the moment it determines there is a problem with a certificate. With power system operations, some method should be developed to securely receive a revocation announcement over the Internet, and then pass this revocation securely to the appropriate end equipment, all in a timely manner.

5.6.3 System and network management

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 of the Northeast Coast of the United States showed, the primary reason behind the blackout itself was the lack of critical information made available to the right user at the right time.

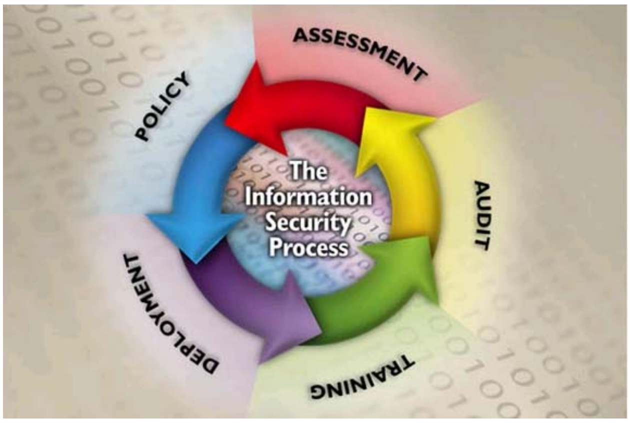
Every utility is different in what information is available to its maintenance staff. Telecommunication technicians are generally responsible for tracking down any microwave or fibre cable problems; telecommunication service providers should track their networks; database administrators should determine if data is being retrieved correctly from substation automation systems or from GIS databases; protocol engineers should correct protocol errors; application engineers should determine if applications have crashed, have not converged, or are in an endless loop; and operators should 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. Software applications which are critical to power system reliability will execute within Intelligent Electronic Devices (IEDs), and will themselves need to be monitored and managed in order to avoid software “crashes” and system failures. 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.

5.7 Five-step security process

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.



IEC 615/07

Figure 8 – General security process – continuous cycle

Security should 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 8, 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 always be residual risks that should 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. The security policy should be elaborated in a security plan that defines the detailed security measures to be implemented, the schedule for implementing these measures, and the review process for measuring the results and updating the plan.

Security deployment – Security deployment is a combination of purchasing, installing, and testing 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 should be implemented that allow intrusion detection and audit capabilities, to name a few.

Security training – Continuous training is necessary on security threats, security technologies, and corporate and legal policies that impact security. Security threats and technologies are continuously evolving, and require on-going analysis and training of personnel to implement and maintain the necessary security infrastructure.

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 regard to Security Domains.

5.8 Applying security to power system operations

Because of the large variety of communication methods and performance characteristics, as well as the fact that 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 3 to 7 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. It is crucial that only authorized control actions are allowed to take place.

Also because connection to the Internet should not be a major 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 in power system operations 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. Or a vendor backdoor link is used inappropriately.
- Disgruntled employee – an unhappy employee (or even one trying to play an innocent trick on another employee) has the knowledge to perform actions that may deliberately or inadvertently do harm to power system operations.
- 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.

6 Overview of the IEC 62351 series

6.1 Scope of the IEC 62351 series

Security standards have been developed for different profiles of the three communication protocols: IEC 60870-5 and its derivatives, IEC 60870-6 (TASE.2), and IEC 61850. In addition, security through network and system management has been addressed. These security standards should 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.

6.2 Authentication as key security requirement

One of the main focus areas of the IEC 62351 series is authentication, which is key to three of the four primary security threats: confidentiality, integrity, and non-repudiation. The IEC 62351 series can only address the security of communications, but it attempts to provide a mechanism by which Role Based Access Control (RBAC) can be supported within an implementation. RBAC can provide security against these three threats up to the user and/or software application level. In order to provide this basis for RBAC, communication application layer authentication is required as a minimum.

6.3 Objectives of the IEC 62351 series

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.

Some security requirements described in other Clauses are beyond the scope of the IEC 62351 series, since they involve security policies, employee training, and system design and implementation decisions. In addition, logging and reporting of events and alarms, which are already inherent in the IEC protocols standards are expected to be used to provide an audit trail.

Therefore, the IEC 62351 series have focused on providing the following types of security measures:

- Authentication to minimize the threat of man-in-the-middle attacks.
- Authentication to minimize some types of bypassing control.
- Authentication to minimize carelessness and disgruntled employee actions.
- Authentication of entities through digital signatures:
  - ensuring only authorized access to information,
  - communication access control.
- Confidentiality of authentication keys via encryption.
- Confidentiality of messages via encryption for those communications that have the resources to handle the additional burden.
- Integrity: tamper detection.
- Prevention of playback and spoofing.
- Both secure and non-secure devices should be allowed to co-exist on the same network, even though this might open some backdoor security issues.
- Monitoring of the communications infrastructure itself, which can provide:
  - a degree of intrusion detection,
  - resource load monitoring,
  - availability of components within the information system.
- One set of identity management policies required (e.g. same mechanism for all profiles).
- Desire to use mainstream IT methodologies.

6.4 Relationships between the IEC 62351 parts and IEC protocols

In each Part of the IEC 62351 series, the security requirements being addressed are stated (e.g. authentication, confidentiality, etc.). In addition, a Proforma Implementation Conformance Statement (PICS) is included that identifies mandatory and optional conformance for different security levels.

This series is published by the IEC as IEC 62351, Parts 1 to7, as follows:

- IEC 62351-1: Introduction and overview
- IEC 62351-2: Glossary of terms
- IEC 62351-3: Profiles including TCP/IP (*this part covers those profiles used by ICCP, IEC 60870-5-104, DNP 3.0 over TCP/IP, and IEC 61850 over TCP/IP*)
- IEC 62351-4: Profiles Including MMS (*this part covers those profiles used by ICCP and IEC 61850*)
- IEC 62351-5: Security for IEC 60870-5 and Derivatives (i.e. DNP 3.0) (*this part covers both serial and networked profiles used by IEC 60870-5 and DNP*)
- IEC 62351-6: Security for IEC 61850 Profiles (*this part covers those profiles in IEC 61850 that are not based on TCP/IP – GOOSE, GSSE, and SMV*)
- IEC 62351-7: Management Information Base (MIB) Requirements for End-to-End Network Management (*this part involve the development of Management Information Base (MIBs) for the power system operational environment*)

The correlation between the IEC 62351 series and the IEC TC 57 standards is shown in Figure 9.

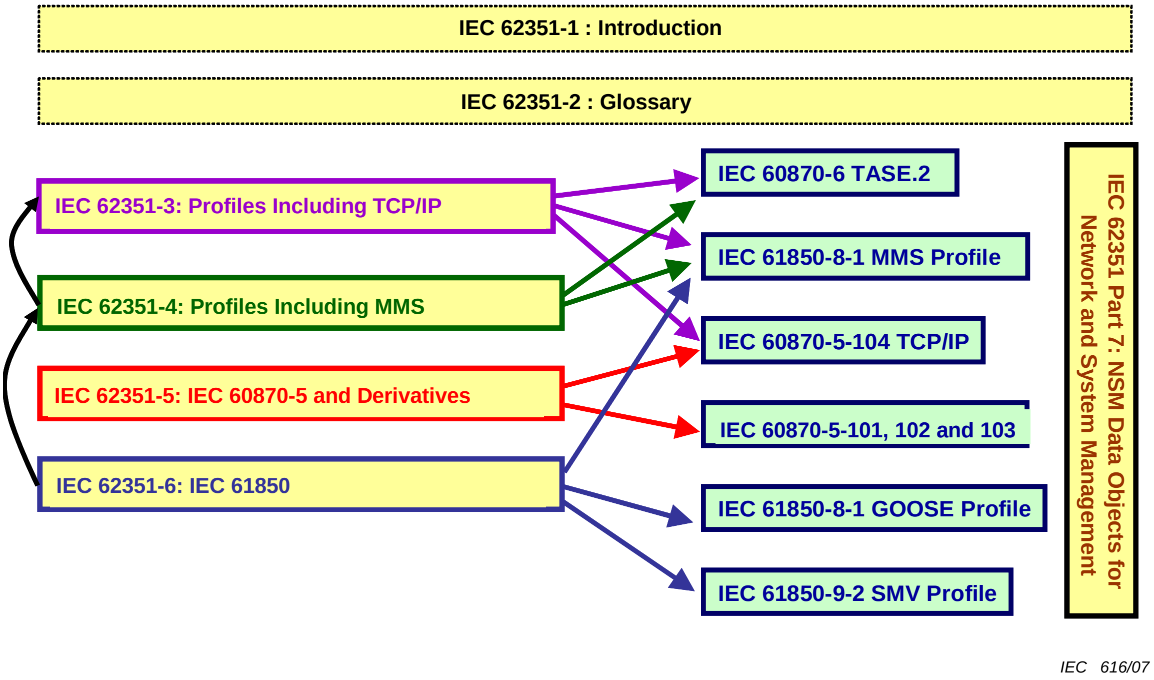

IEC 62351-1 : Introduction
IEC 62351-2 : Glossary
IEC 62351-3: Profiles Including TCP/IP
IEC 62351-4: Profiles Including MMS
IEC 62351-5: IEC 60870-5 and Derivatives
IEC 62351-6: IEC 61850
IEC 60870-6 TASE.2
IEC 61850-8-1 MMS Profile
IEC 60870-5-104 TCP/IP
IEC 60870-5-101, 102 and 103
IEC 61850-8-1 GOOSE Profile
IEC 61850-9-2 SMV Profile
IEC 62351 Part 7: NSM Data Objects for Network and System Management
IEC 616/07

Figure 9 – Correlation between the IEC 62351 series and IEC TC 57 profile standards

6.5 IEC 62351-1: Introduction

IEC 62351-1 (this document) is an informative introduction which covers the background of security for power system operations, and provides overview information on the IEC 62351 series.

6.6 IEC 62351-2: Glossary of terms

IEC 62351-2 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. When industry standard definitions are used, these are attributed to the source.

6.7 IEC 62351-3: Profiles including TCP/IP

6.7.1 Threats and types of attacks being countered

IEC 62351-3 provides security for any profile that includes TCP/IP. 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. IEC 62351-3 describes the mandatory and optional parameters and settings for TLS that should be used for utility operations.

The purpose of IEC 62351-3 is to provide end-to-end transport security for the communications between software applications. In determining the best approach to meet this purpose, both IPSec and TLS were analyzed. IPSec is typically used to protect all traffic that is exchanged between two LAN segments, whereas TLS provides encryption and man-in-the-middle protection on an end-to-end basis. Therefore, TLS was selected rather than IPSec to meet this purpose. It is understood and acceptable that IPSec may be used to protect other traffic or even be used in conjunction with TLS.

IEC 62351-3 protects against:

- Eavesdropping through Transport Layer Security (TLS) encryption.
- Man-in-the-middle security risk through message authentication.
- Spoofing through Security Certificates (Node Authentication).
- Replay, again through TLS encryption.

However, TLS does not protect against denial of service. This type of security attack needs to be guarded against through implementation-specific measures.

TLS security for TCP/IP provides security for the transport-layers of the communication profiles. TLS does not provide application-layer security, so this should be provided by other security measures.

6.7.2 Security requirements and measures

To support different levels of security, IEC 62351-3 specifies that products claiming conformance shall support the following capabilities:

- Interoperability with other devices that have not implemented either TLS or application authentication. This provides the necessary backward compatibility with existing implementations, and for the gradual updating of systems towards using security.
- Interoperability with other devices that have not implemented TLS, but do support application authentication. This can be used for implementations over VPN connections or internal to control centers.
- Interoperability with other devices that have implemented TLS, but not application authentication. This permits encryption and node level authentication only.
- Interoperability with other devices that have implemented both TLS and application authentication. This provides full security.

Some of the key elements of the security measures for TCP/IP are:

- Depreciation of SSL 1.0 and 2.0 due to known security vulnerabilities.
- Use TLS 1.0 or higher (which is equivalent to Secure Sockets Layer (SSL) 3.1).
- Deprecate cipher suites that do not provide encryption.
- Transparent key re-negotiation based upon time and number of packets, so that lightly loaded networks do not lose certification over long time periods, since most connections are long term. Both time and number are configurable, but the recommended parameters are time (10 min) and number of packets (5 000).
- The entity that was connected to is responsible for key negotiation. This avoids protocol deadlocking.
- Standardization for support for at least one common cipher suite, AES.
- Specification of TLS message authentication to avoid spoof and replay.
- Can request small certificates to minimize the burden.

6.7.3 Usage of VPN tunnels and bump-in-the-wire technology

The use of VPN tunnels and/or “bump-in-the-wire” (e.g. AGA 12-2) solutions is beyond the scope of the IEC 62351 standards. This does not exclude their use as part of an overall security solution, so long as it is recognized that they can protect only one of the security categories.

6.8 IEC 62351-4: Security for profiles that include MMS

6.8.1 Threats and types of attacks being countered

IEC 62351-4 provides security for profiles that include MMS, including TASE.2 (ICCP) and IEC 61850.

Security for the Manufacturing Message Specification (MMS) (ISO 9506) provides application-layer security. It requires TLS to configure and makes use of TLS security measures, in particular, authentication: the two entities interacting with each other are who they say they are.

If encryption is not employed, then the specific threats countered in IEC 62351-4 include:

- Unauthorized access to information

If IEC 62351-3 is employed, then the specific threats countered in IEC 62351-4 include:

- Unauthorized access to information through message level authentication and encryption of the messages
- Unauthorized modification (tampering) or theft of information through message level authentication and encryption of the messages

The following security attack methods are intended to be countered by IEC 62351-4. The following list is exclusive of the attack methods countered through IEC 62351-3. In the case that IEC 62351-3 is not employed, the threats countered are restricted to protection during association establishment:

- Man-in-the-middle: This threat will be countered through the use of a Message Authentication Code mechanism specified within this document
- Tamper Detection/Message Integrity: These threats will be countered through the algorithm used to create the Authentication mechanism as specified within this document.
- Replay: This threat will be countered through the use of specialized processing state machines specified within IEC 62351-3 and IEC 62351-4.

6.8.2 Security requirements and measures

Therefore, the combination of IEC 62351-3 and IEC 62351-4 provide end-to-end security up through the communications application layer, including the following types of security:

- authentication,
- confidentiality,
- data integrity,
- non-repudiation.

IEC 62351-4 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.

6.9 IEC 62351-5: Security for IEC 60870-5 and derivatives

6.9.1 Threats and types of attacks being countered

IEC 62351-5 provides different solutions for the serial version (primarily IEC 60870-5-101, as well as IEC 60870-5-102 and IEC 60870-5-103) and for the networked versions (IEC 60870-5-104 and derivates such as DNP3 over TCP).

Specifically, IEC 62351-5 provides application layer authentication which protects against spoofing, replay, modification, and some denial of service attacks. It does not include encryption, so it does not protect against eavesdropping, traffic analysis, or repudiation.

Application layer authentication is necessary because site-to-site security and, in some cases, transport layer security, do not address the following:

- Security within each local site.
- Security of serial protocols (such as IEC 60870-5) over unencrypted radios.
- Security of serial protocols that have been forwarded over IP networks through terminal servers.
- Protection from "rogue applications" or attacks from within hosts that may be infected by malware.
- Linking role-based authentication to the remote site. Today, the security chain for role-based authentication for users typically stops within the host. Application layer authentication can ensure that only those users authorized to see a particular set of data can access it by preventing it from being transmitted from the remote site until the user is authenticated.

6.9.2 Security requirements and measures

The networked versions of IEC 60870-5-104 and derivates 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 the authentication services provided by IEC 62351-5.

The serial version is usually used with communications media that can only support low bit rates or with field equipment that is compute-constrained. 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 simple authentication mechanisms.

6.9.3 Possible additional security measures to IEC 62351-5

If encryption is required, other encryption-based security measures could be added, such as VPNs or "bump-in-the-wire" technologies, depending upon the capabilities of the communications and equipment involved. These encryption measures act at the transport layer.

6.10 IEC 62351-6: Security for IEC 61850 Profiles

6.10.1 Threats and types of attacks being countered

IEC 62351-6 covers the IEC 61850 profile using MMS over TCP/IP uses IEC 62351-3 and IEC 62351-4.

The security threats that are countered include man-in-the-middle, unauthorized modification of data, unauthorized modification of messages, tamper detection, and replay. For those functions where the performance requirements are not as stringent and where confidentiality is required, encryption could be added by other security measures such as "bump-in-the-wire" or VPNs.

6.10.2 Security requirements and measures

The IEC 61850 profile using MMS 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. The possible use of these externally developed security measures are out-of-scope for the IEC 62351 series.

IEC 61850 also contains three protocols (GOOSE, GSE, and SMV) that are multicast datagrams and not routable, designed to run on a substation LAN or other non-routed network. In this environment, the messages need to be transmitted within 4 milliseconds; therefore most encryption techniques or other security measures which affect transmission rates are not acceptable. Therefore, authentication through a digital signature is the only security measure included.

The characteristics of these three protocols are shown in Table 1 below:

Table 1 – Characteristics of the three multicast IEC 61850 protocols

	SMV	GOOSE	MMS
PDU size	~1 500	~1 500	>30 000
Performance	Stream	4 ms	No requirement
Type	Multicast	Multicast	Connection oriented

Based on these characteristics, the following security measures were determined, as shown in Table 2:

Table 2 – Security measures for the three multicast IEC 61850 protocols

	SMV	GOOSE	MMS
X.509 certificates (identity)	No	No	Yes
Encryption (confidentiality)	Not necessary	Only if > 4 ms	Yes
Tamper detection (intrusion detection)	Yes	Yes	Yes

Some of the key elements of the security measures for GOOSE and SMV are:

- Authentication is the primary security measure.
- Encryption is not included because this adds too many bytes to the messages, and is not considered that important. (In the future, some hardware encryption might be added.)
- Key renegotiation is not supported “in-band” because it could disrupt the highly critical, high speed flow of information.
- Since security may be implemented over time, and because security may or may not be needed for different devices, a non-secure GOOSE client could ignore a secure GOOSE message.
- For backward compatibility, a reserved field is now used for length, so that an extension can be added to the end of the GOOSE/SMV message. This extension contains the authentication value (Digital Signature – HMAC). Non-secure clients would simply ignore this extension. This adds about 20 bytes.
- The IEC 61850 Substation Configuration Language (SCL) is extended in order to support the exchange of certificates.

The following diagram, Figure 10, illustrates the authentication security measure in GOOSE/SMV:

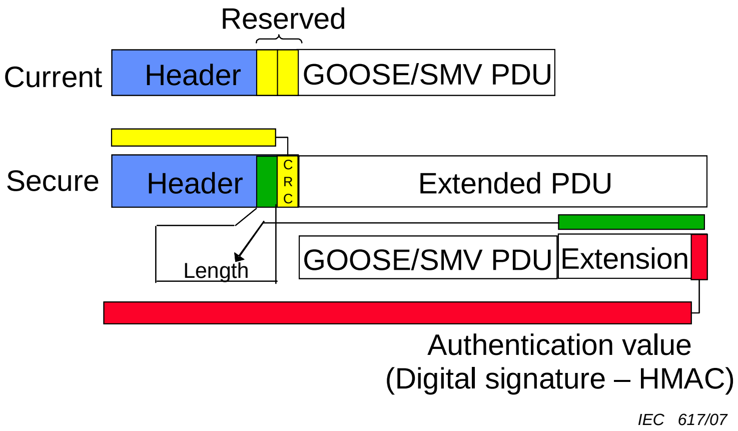


Figure 10 – Authentication security measure in GOOSE/SMV

6.11 IEC 62351-7: Security through network and system management

6.11.1 Purpose and scope of IEC 62351-7

IEC 62351-7 addresses security through network and system management 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.

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. IEC 62351-7 has therefore developed abstract Network and System Management (NSM) data objects for the power system operational environment 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 shall 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 NSM data objects 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 NSM data objects use the naming conventions developed for IEC 61850, expanded to address NSM issues.

The abstract SNMP client/agent model is assumed within the standard, but SNMP is not presumed to be the protocol of choice. Instead, the abstract NSM data objects defined in IEC 62351-7 may be mapped to any appropriate protocol, including IEC 61850, IEC 60870-5, IEC 60870-6, SNMP, web services, or any other appropriate protocol.

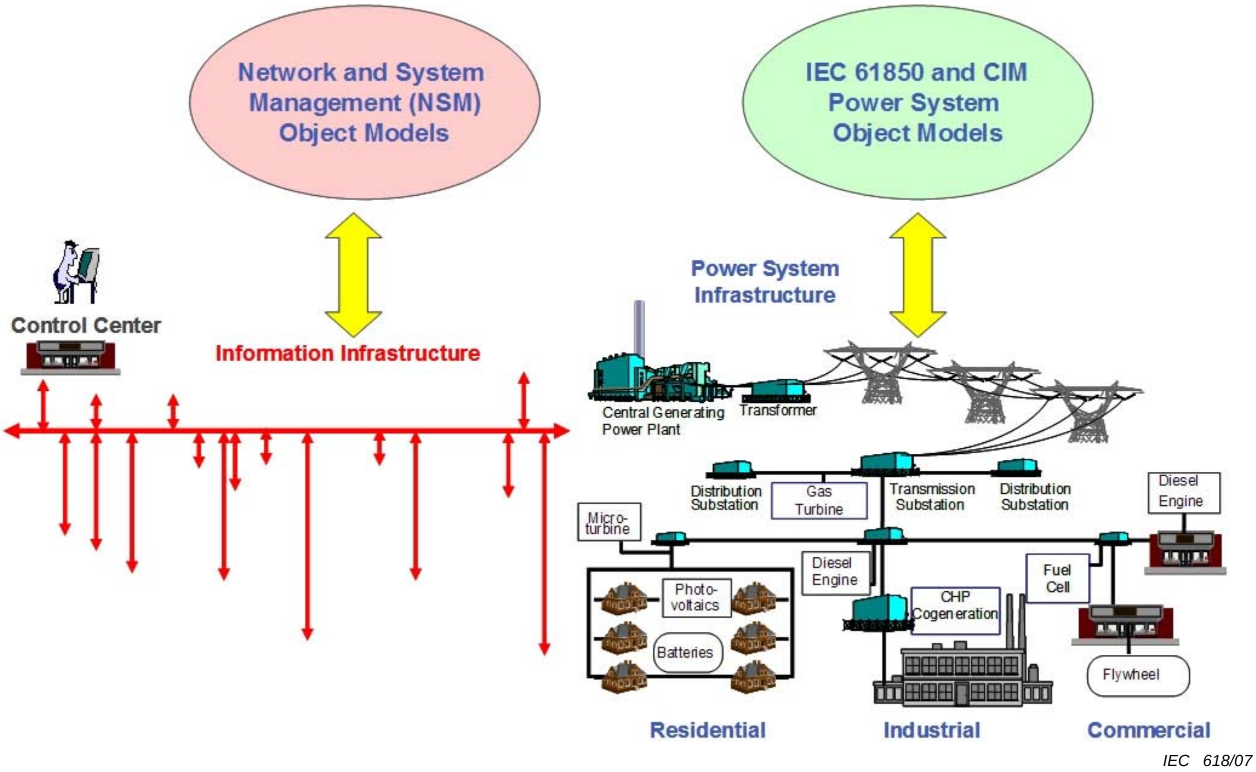


Figure 11 – NSM object models are the information infrastructure equivalent to the CIM and IEC 61850 object models of the power system infrastructure

6.11.2 NSM Requirements

Security and reliability NSM data object requirements that are specific for the power industry need to be defined. 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.

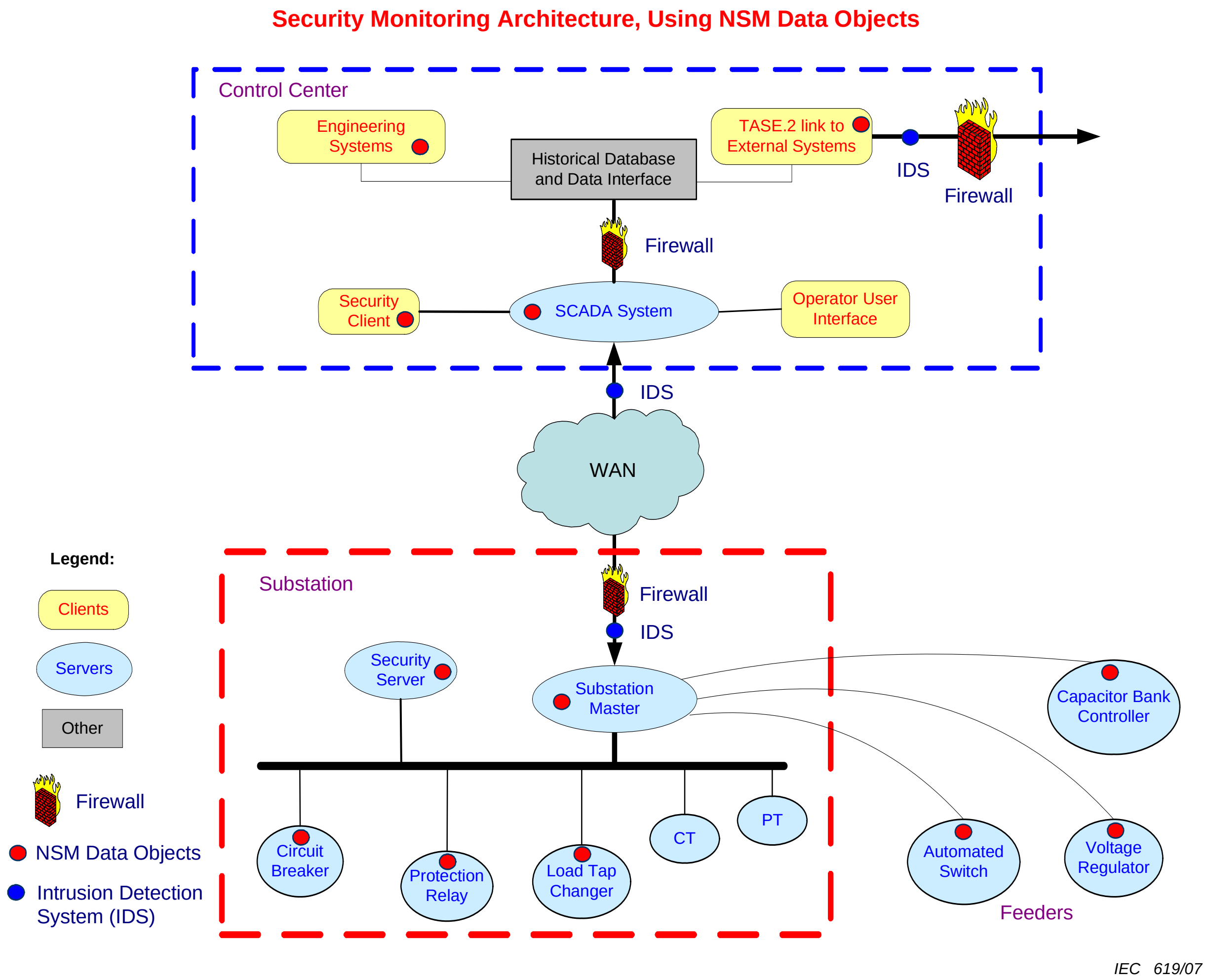


Figure 12 – Power system operations systems, illustrating the security monitoring architecture

6.11.3 Examples of NSM data objects

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

a) Communications network management: monitoring the networks and protocols

1) Detecting network equipment permanent failures
2) Detecting network equipment temporary failures and/or resets
3) Detecting network equipment failovers to backup equipment or communication paths
4) Detecting the status of backup or spare equipment
5) Detecting communication protocol version and status
6) Detecting mis-matches of differing protocol versions and capabilities
7) Detecting tampered/malformed protocol messages
8) Detecting inadequately synchronized time clocks across networks
9) Detecting resource exhaustion forms of Denial of Service (DOS) attacks
10) Detecting buffer overflow DOS attacks
11) Detecting physical access disruption

12) Detecting invalid network access
13) Detecting invalid application object access/operation
14) Ability to detect coordinated attacks across multiple systems
15) Collecting statistical information from network equipment
    - Determining average message delivery times, slowest, fastest, etc.
    - Counting number of messages, size of messages
16) Providing audit logs and records

b) Communications network management: controlling the networks
   1) Manual issuing of on/off commands to network equipment
   2) Manual issuing of switching commands to network equipment
   3) Setting parameters and sequences for automated network actions
   4) Automated actions in response to events, such as reconfiguration of the communications network upon equipment failure

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

d) System management: control actions within Intelligent Electronic Devices (IEDs)
   1) Start or stop reporting
   2) Restart IED
   3) Kill and/or restart application
   4) Re-establish connection to another IED
   5) Shut down another IED
   6) Provide event log of information events
   7) Change password
   8) Change backup or failover options
   9) Providing audit logs and records

7 Conclusions

Security measures should be built into every system from the moment they are conceived. Security includes not only firewalls or the “encryption” that most people 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.

Bibliography

North American Electric Reliability Council (NERC) Cyber Security Standard, CIP 002-009, 2006

ISBN 2-8318-9138-8

9 782831 891385

ICS 33.200

Typeset and printed by the IEC Central Office
GENEVA, SWITZERLAND