TECHNICAL REPORT

IEC TR 62210

First edition
2003-05

Power system control and associated communications – Data and communication security

Reference number
IEC/TR 62210:2003(E)

Publication numbering

As from 1 January 1997 all IEC publications are issued with a designation in the 60000 series. For example, IEC 34-1 is now referred to as IEC 60034-1.

Consolidated editions

The IEC is now publishing consolidated versions of its publications. For example, edition numbers 1.0, 1.1 and 1.2 refer, respectively, to the base publication, the base publication incorporating amendment 1 and the base publication incorporating amendments 1 and 2.

Further information on IEC publications

The technical content of IEC publications is kept under constant review by the IEC, thus ensuring that the content reflects current technology. Information relating to this publication, including its validity, is available in the IEC Catalogue of publications (see below) in addition to new editions, amendments and corrigenda. Information on the subjects under consideration and work in progress undertaken by the technical committee which has prepared this publication, as well as the list of publications issued, is also available from the following:

- **IEC Web Site (www.iec.ch)**

- **Catalogue of IEC publications**

  The on-line catalogue on the IEC web site (http://www.iec.ch/searchpub/cur_fut.htm) enables you to search by a variety of criteria including text searches, technical committees and date of publication. On-line information is also available on recently issued publications, withdrawn and replaced publications, as well as corrigenda.

- **IEC Just Published**

  This summary of recently issued publications (http://www.iec.ch/online_news/justpub/jp_entry.htm) is also available by email. Please contact the Customer Service Centre (see below) for further information.

- **Customer Service Centre**

  If you have any questions regarding this publication or need further assistance, please contact the Customer Service Centre:

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

TECHNICAL
REPORT

IEC
TR 62210

First edition
2003-05

Power system control and associated communications – Data and communication security

International Electrotechnical Commission, 3, rue de Varembé, PO Box 131, CH-1211 Geneva 20, Switzerland
Telephone: +41 22 919 02 11 Telefax: +41 22 919 03 00 E-mail: inmail@iec.ch Web: www.iec.ch

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

PRICE CODE X

For price, see current catalogue

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

POWER SYSTEM CONTROL AND ASSOCIATED COMMUNICATIONS –

Data and communication security

FOREWORD

1) The IEC (International Electrotechnical Commission) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of the 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, the IEC publishes International Standards. 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. The 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 the 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 National Committees.
3) The documents produced have the form of recommendations for international use and are published in the form of standards, technical specifications, technical reports or guides and they are accepted by the National Committees in that sense.
4) In order to promote international unification, IEC National Committees undertake to apply IEC International Standards transparently to the maximum extent possible in their national and regional standards. Any divergence between the IEC Standard and the corresponding national or regional standard shall be clearly indicated in the latter.
5) The IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with one of its standards.
6) Attention is drawn to the possibility that some of the elements of this technical report may be the subject of patent rights. The 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. However, a technical committee may propose the publication of a technical report when it has collected data of a different kind from that which is normally published as an International Standard, for example “state of the art”.

IEC 62210, which is a technical report, has been prepared by IEC technical committee 57: Power system control and associated communications.

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

Enquiry draft	Report on voting
57/613/DTR	57/630/RVC

Full information on the voting for the approval of this technical report 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.

The committee has decided that the contents of this publication will remain unchanged until 2006. At this date, the publication will be

- reconfirmed;
- withdrawn;
- replaced by a revised edition, or
- amended.

A bilingual version of this technical report may be issued at a later date.

POWER SYSTEM CONTROL AND ASSOCIATED COMMUNICATIONS –

Data and communication security

1 Scope and object

This Technical Report applies to computerised supervision, control, metering, and protection systems in electrical utilities. It deals with security aspects related to communication protocols used within and between such systems, the access to, and use of the systems.

NOTE This report does not include recommendations or criteria development associated with physical security issues.

Realistic threats to the system and its operation are discussed. The vulnerability and the consequences of intrusion are exemplified. Actions and countermeasures to improve the current situation are discussed but solutions are to be considered issues for future work items.

2 Overview

Safety, security, and reliability have always been important issues in the design and operation of systems in electrical utilities. Supervision, protection, and control system have been designed with the highest possible level of safety, security, and reliability. The communication protocols have been developed with a residual error rate approaching zero. All these measures have been taken to minimise the risk of danger for personnel and equipment and to promote an efficient operation of the power network.

Physical threats on vulnerable objects have been handled in the classical ways by locked buildings, fences and guards but the quite possible terrorist threat of tripping a critical breaker by a faked SCADA command on a tapped communication link has been neglected. There is no function in the currently used protocols that ensure that the control command comes from an authorised source.

The deregulated electricity market has imposed new threats: knowledge of the assets of a competitor and the operation of his system can be beneficial and acquisition of such information is a possible reality.

The communication protocols and systems need protection from advertent and inadvertent intruders, the more the protocols are open and standardised and the more the communication system is integrated in the corporate and world-wide communication network.

This Technical Report discusses the security process of the electrical utility. The security process involves the corporate security policy, the communication network security, and the (end-to-end) application security.

The security of the total system depends on secure network devices, i.e. the security of any device that can communicate. A secure network device has to be capable of performing ‘safe’ communication and of authenticating the access level of the user. Intrusive attacks have to be efficiently detected, recorded and prosecuted as part of an active audit system.

The threats are analysed based on possible consequences to a system, i.e. what is the worst that could happen if an illicit intruder has ambition and resources? The vulnerability of a utility and its assets are analysed together with the threats.

Having shown that there exists threats to vulnerable points in the systems of electrical utilities the countermeasures are discussed with special focus on the communication protocols defined by IEC Technical Committee 57: the IEC 60870-5 series, the IEC 61334 series, the IEC 60870-6 series and the IEC 61850 series.

Proposals on new work items to include security aspects in these protocols are given.

3 Reference documents

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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*

IEC 61334 (all parts), *Distribution automation using distribution line carrier systems*

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

ISO/IEC 7498-1, *Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model*

ISO 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture*

ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*

ISO/IEC 10181-7:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Security audit and alarms framework*

ISO/IEC 15408-1, *Information technology – Security techniques – Evaluation criteria for IT Security – Part 1: Introduction and general model*

ISO/IEC 15408-2, *Information technology – Security techniques – Evaluation criteria for IT Security – Part 2: Security functional requirements*

ISO/IEC 15408-3, *Information technology – Security techniques – Evaluation criteria for IT Security – Part 3: Security assurance requirements*

4 Terms, definitions and abbreviations

4.1 Terms and definitions

4.1.1
accountability
property that ensures that the actions of an entity may be traced uniquely to the entity

4.1.2
asset
Anything that has value to the organisation

[ISO/IEC TR 13335-1:1997]

4.1.3
authenticity
property that ensures that the identity of a subject or resource is the one claimed. Authenticity applies to entities such as users, processes, systems and information

4.1.4
authorisation violation
entity authorised to use a system for one purpose uses it for another, unauthorised purpose

4.1.5
availability
property of being accessible and usable upon demand by an authorised entity

[ISO 7498-2: 1989]

4.1.6
baseline controls
minimum set of safeguards established for a system or organisation

[ISO/IEC TR 13335-1:1997]

4.1.7
confidentiality
property that information is not made available or disclosed to unauthorised individuals, entities, or processes

[ISO 7498-2:1989]

4.1.8
data integrity
property that data has not been altered or destroyed in an unauthorised manner

[ISO 7498-2:1989]

4.1.9
denial of service
authorised communications flow is intentionally impeded

4.1.10
eavesdropping
information is revealed to an unauthorised person monitoring communication traffic

4.1.11
hack
threat that may be a combination of one or more of the following threats: authorisation violation; information leakage; integrity violation; and masquerade

4.1.12
hash function
(mathematical) function that maps values from a (possibly very) large set of values into a smaller range of values

4.1.13
information leakage
unauthorised entity obtains secure/restricted information

4.1.14
integrity violation
information is created or modified by an unauthorised entity

4.1.15
intercept/alter
communication packet is intercepted, modified, and then forwarded as if it were the original packet

4.1.16
masquerade
unauthorised entity attempts to assume the identity of a trusted party

4.1.17
reliability
property of consistent intended behaviour and results

[ISO/IEC TR 13335-1:1997]

4.1.18
replay
communication packet is recorded and then retransmitted at an inopportune time

4.1.19
repudiation
exchange of information occurs and one of the two entities in the exchange later denies the exchange or contents of the exchange

4.1.20
residual risk
risk that remains after safeguards have been implemented

[ISO/IEC TR 13335-1:1997]

4.1.21
resource exhaustion
see denial of service

4.1.22
risk
potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets

[ISO/IEC TR 13335-1:1997]

4.1.23
security auditor
individual or a process allowed to have access to the security audit trail and to build audit reports

[ISO/IEC 10181-7:1996]

4.1.24
security authority
entity that is responsible for the definition, implementation or enforcement of security policy

4.1.25
security domain
set of elements, a security policy, a security authority, and a set of security-relevant activities in which the set of elements are subject to the security policy for the specified activities, and the security policy is administered by the security authority for the security domain

4.1.26
security domain authority
security authority that is responsible for the implementation of a security policy for a security domain

4.1.27
security token
set of data protected by one or more security services, together with security information used in the provision of those security services, that is transferred between communicating entities

4.1.28
security-related event
any event that has been defined by security policy to be a potential breach of security, or to have possible security relevance. Reaching a pre-defined threshold value is an example of a security-related event

4.1.29
spoof
combination of one or more of the following threats: eavesdropping; information leakage; integrity violation; intercept/alter; and masquerade

4.1.30
system integrity
property that a system performs its intended functions in an unimpaired manner, free from deliberate or accidental unauthorised manipulation of the system

[ISO/IEC TR 13335-1:1997]

4.1.31
threat
potential cause of an unwanted incident which may result in harm to a system or organisation

[ISO/IEC TR 13335-1:1997]

4.1.32
trust
entity X is said to trust entity Y for a set of activities if and only if entity X relies upon entity Y behaving in a particular way with respect to the activities

4.1.33
trusted entity
entity which is assumed to appropriately enforce security policies. Because of this assumption, the entity may cause other security policies to be obviated.

EXAMPLE A trusted authorisation entity declares a user to be authorised for control thereby challenges authentication procedures, that would normally be applied, are not invoked.

Entity that can violate a security policy, either by performing actions which it is not supposed to do, or by failing to perform actions which it is supposed to do

4.1.34
vulnerability
includes a weakness of an asset, or group of assets, which can be explained by a threat

[ISO/IEC TR 13335-1:1997]

4.1.35
developed technology
software code/algorithms that are developed within the configuration and guidelines for quality and security assurance set forth as EAL-5, or greater, as specified in ISO/IEC 15408-3

4.2 Abbreviations

AMR	Automatic Meter Reading
CC	Common Criteria
COTS	Commercial off the shelf software
DISCO	Distribution Company
DLC	Distribution Line Carrier
DLMS	Distribution Line Messaging System
DMS	Distribution Management System
EAL	Evaluation Assurance Level
EMS	Energy Management System
GENCO	Generation Company
HMI	Human – Machine Interface (for example: operator workstation)
HV	High Voltage
IED	Intelligent Electronic Device
IT	Information Technology
LAN	Local Area Network
LV	Low Voltage
MMS	Manufacturing Message Specification
MV	Medium Voltage
NT	Windows NT is a Microsoft Windows personal computer operating system designed for users and businesses needing advanced capabilities
OASIS	Open Access Same-Time Information System
PLC	(user) Programmable Logic Controller
POTS	Plain Old Telephone System
PP	Protection Profile
RTU	Remote Terminal Unit
SCADA	Supervisory Control And Data Acquisition
ST	Security Target
TASE	Telecontrol Application Service Element
TCP/IP	Transmission Control Protocol/ Internetworking Protocol
TOE	Target of Evaluation
TRANSCO	Transmission Company
VAA	Virtual Application Association
VDE	Virtual Distribution Equipment
WAN	Wide Area Network

5 Introduction to security

Communication and information security is becoming an essential requirement for information networks in the commercial/private sector. This is particularly true for communication and information technologies employed as part of critical service infrastructures/services. Disruption of these services (for example gas, water, and electric service deliveries) can have impact over a wide geographical area and upon a large number of individuals and companies.

Communication networking and information exchange, within and between companies, is becoming more prevalent within the electrical infrastructure. Whereas, in the past, utilities held their information tightly and controlled most of their communication infrastructure, this is no longer the case. Shared communication networks and information exchanges over public networks are becoming more prevalent. This trend allows for systemic attacks to be considered by non trusted parties (for example hackers, downsized employees, or terrorists). This trend, and the large amount of technology available to be employed in an attack, portends an increased probability for more numbers of attacks with several being successful.

NOTE There is little publicly available information on which to derive models of threats and attacks for the future. However, the lack of this information does not mean that attacks are not occurring but rather that the utilities either do not have the processes in place to detect the attack or that the information of such attacks are not publicly disclosed. Additionally, the trend towards increased probability of attacks can be projected due to increased financial motivation (for example due to deregulation) and the ease of conducting attacks (for example due to technology advances).

Unlike the military, most users of computer/utility information systems and protocols are largely unaware of the potential threats to their information and infrastructure. Worse yet, the users are sometimes aware but do not place importance on addressing the known security risks. Currently, the number of incidents (detected attacks) is relatively low. However, there is an increase in detected attacks and critical infrastructures (for example gas, water, and electric) have been proven to be extremely vulnerable.

There are several ways in which to view security issues, and this document deals with communication security only. It does not deal with aspects of security relating to informational security within a computer system, but rather with only informational security aspects when information is being transferred via a protocol specified within IEC Technical Committee 57.

5.1 How to use this report

This report is intended to present recommendations to IEC Technical Committee 57 and its working groups. The work should be viewed as the foundation upon which new work items may need to be commissioned. The work should not be viewed as complete.

Additional consideration should be given to establishing strong liaisons with other IEC Technical Committees so that the work and recommendations set forth in this report can be considered.

6 The security analysis process

The recommendations in this report will have a direct impact on the normal corporate security processes and must be constructed in a manner consistent with this process. Therefore it is important to understand the typical corporate security process requirements and their impact on the scope of this report.

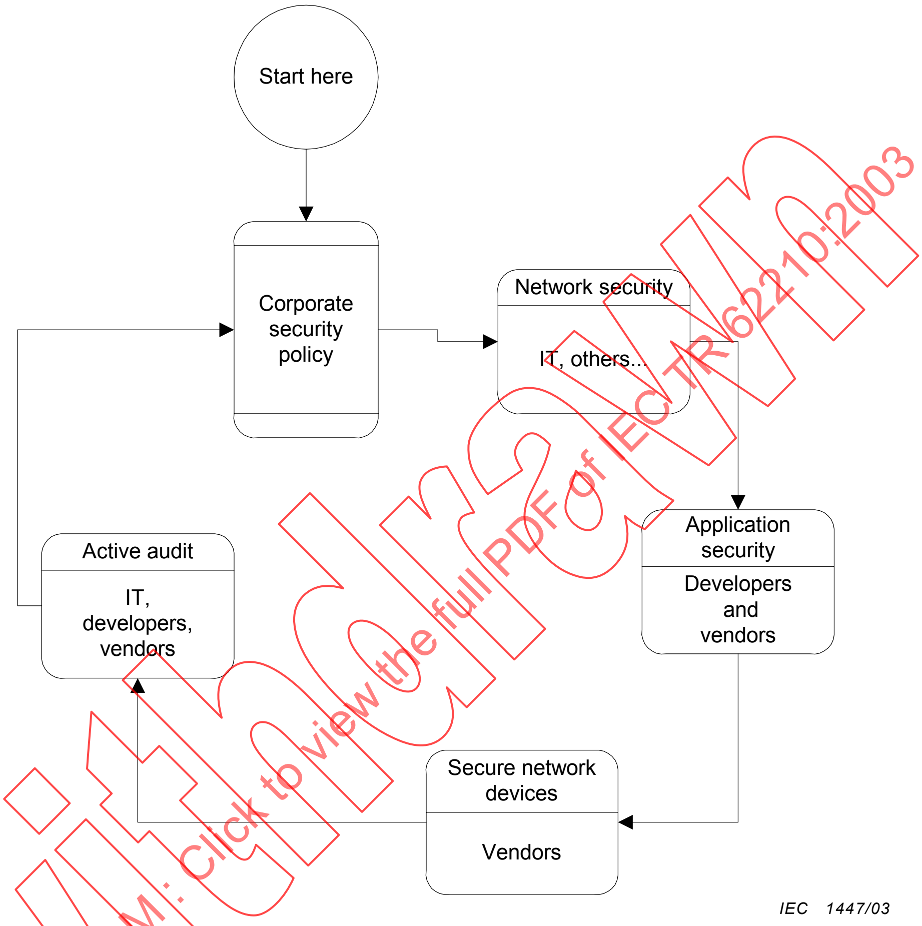

Figure 1 – Normal corporate security process

Figure 1 depicts what is typically considered to be the normal corporate security policy that should be implemented in order to create a relatively "secure" corporate infrastructure. The figure clearly shows that in order to create a secure corporate infrastructure, corporate security policy must be developed and adopted by the management of the corporation first.

The corporate security policy rules will deal with a definition and assignments of the security domains, security domain authority(s), security auditor, and accountability. Additionally, these policies typically dictate the acceptable residual risk once the corporate policies are translated into actions and implementation. It is clear that corporations will develop policies, which may or may not rely upon the recommendations within this report.

However, it is within the scope of this report to inform corporate management as to threats and consequences that are relevant to protocols being addressed by this report. Therefore, corporate security policy should review the following parts of this report:

a) Definitions (see 4.1): this will be useful in constructing a consistent vocabulary.

b) Specific threats to be considered in PP (see 7.2.3): this lists the set of threats, and their definitions, that are being addressed within the scope of this report.

c) Vulnerabilities (see Clause 8): this deals with the set of communication system vulnerabilities that are known to exist in the communication protocols addressed within the scope of this report.

d) The security analysis process (see Clause 6): this may prove of interest to the corporate policy writers; however it is more typically of interest to other parts of the corporate security policy team.

Corporate policies tend to be at an objective level and therefore the clauses of interest should be used to help formulate objectives and to inform corporate management. However, such corporate objectives are translated into implementation strategy and policies in the network security, application security, and secure network devices processes.

Application security deals with the end-to-end application level security issues. There needs to be strong and clear guidance on security procedures such that usage of host computer applications is appropriately restricted, maintained, and audited. This report is neutral in regards to the technologies and methodologies used to secure host based applications.

Network security, within the corporate security process, typically deals with firewalls and sub-network access. Security policies in this domain must address the issues of access privileges from one sub-network to another. This report has no direct impact on the network security corporate policy process.

However, there is a strong relationship between the user of applications and the privileges that are granted through remote communications to end devices/applications. Therefore it is important in developing security policies, to consider the following issues:

a) Certain applications may need to have security privileges determined based upon which host computer/terminal is being used for the execution of the application.

   EXAMPLE In the case of a SCADA master, it may be allowed that any authenticated terminal/user is able to view SCADA information. However, only terminals located within a physically secure (for example control centre) environment may have privileges to actually control remote devices/applications or change configurations.

   In the above example, even if the user of the application has appropriate privilege, the user's privileges are further restricted based upon the terminal/application execution host.

b) It is rare, but applications may need their own security policies established.

   This is particularly true for shared applications (for example such as NT services) which may or may not be able to determine the user of the application.

Therefore, the recommended hierarchy to be considered in constructing an application security policy is:

a) Can user authentication be achieved and translated into usable information by remote applications?

b) Can the location of the user authentication be determined?

c) Can the network location of the application execution be determined?

The most secure (from a communication perspective) is to have application security policies developed in which the remote device/application authenticates the application user and not only the node used for the connection.

Secure network devices: This Technical Report deals with issues, technologies, and recommendations that may allow increased security on utility "networked" devices. For the purposes of this report, "networked" is defined as any device that can communicate.

It is imperative that the reader of this report be advised that the overall security of the communication system will be determined by the degree of security in the networked device. This is in a large part due to the fact that the device is the source of most information and is the entity that can directly impact the utility business operations (for example opening a breaker causing a power outage). It is therefore important that these devices be capable of authenticating the access level of users. Additionally, it is even more important that these devices be able to be part of an audit process so that attacks can be detected, countered, and prosecuted in an expeditious manner.

This is also the area where most utilities will not desire to spend any additional money. However, education and this report will address many of the issues and make a compelling statement as to why the current implementations are not sufficient.

Active audit: any set of security policies and implementations must be continuously monitored and adapted as part of the continuous corporate security process. Without the ability to audit and analyse security attacks and system operations and weaknesses, a secure system will eventually become non-secure.

In order to have an active audit process and a continuous corporate security process, personnel must be dedicated to this task. Therefore, utilities will need to be educated as to the risks associated if such action is taken. It is difficult, if not impossible, to prove cost benefit of such a process until there has been a successful attack. Justifications will need to be based upon the potential "risked" costs if a security process is not implemented.

All parts of the process need to be closely looked at and tailored to a particular environment. But all aspects need to be analysed and addressed in some regards.

6.1 Network topologies

There are many different ways in which to view the communication topologies. From a high level, an analysis of the information flow between sources and consumers of information is needed.

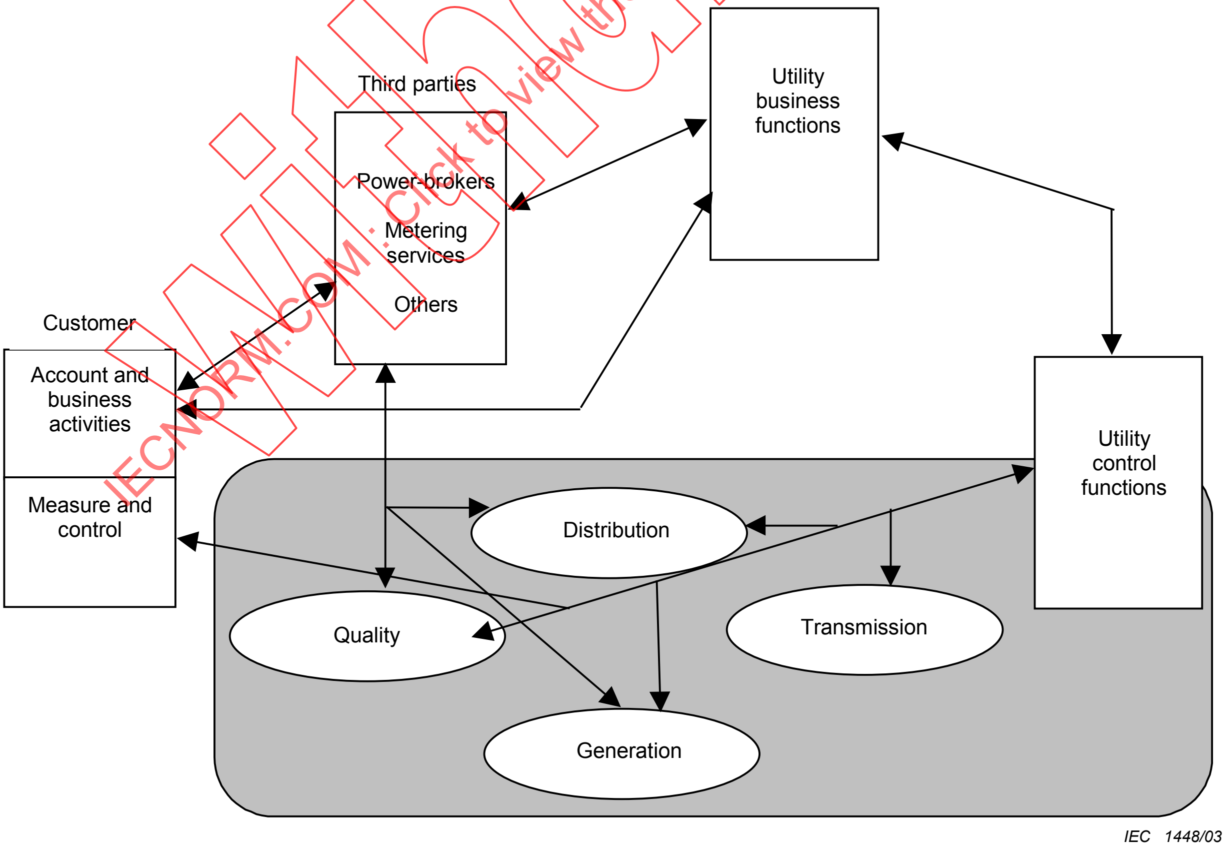

Figure 2 – Business information flow

There are several major business entities shown in Figure 2. These are:

a) **Customer** – this business entity represents the consumer of electrical power and services. There are several aspects to the types of services that the customer expects to have delivered as part of power delivery ranging from billing to power quality control. The customer typically expects the following services:

   1) *Account and business activities:* These include customer service, billing, and power procurement (brokering). The current method by which information is exchanged between these activities is typically by telephone, fax, or email. However, the trend in the industry is to provide these through the use of Internet technologies or other e-commerce type of mechanisms.

      Additionally, these are now not only provided by utility business functions but also may be provided by third parties. In many situations, these two competing organisations may be exchanging information with the same customer over the same information infrastructure.

   2) *Measurement and control activities:* these activities are mainly concerned with communication that allows control of the supply and quality of power delivered to the end customer. This activity is the responsibility of the local distribution utility even though third parties may be mandated to monitor revenue-metering information.

b) **Third parties** – the trend towards deregulation of the utility industry has given rise to business entities that broker power, perform third party meter reading and billing, and offer other services. These third parties exchange information with the customer, utility business functions, and potentially monitor revenue meters and power quality directly.

c) **Utility business functions** – these provide information to customers and to third parties (as required by law). In a deregulated environment, portions of these activities may need to be viewed as if they are the equivalent to third parties.

d) **Utility control functions** – these are the typical SCADA, EMS, and DMS functions that are provided today. The control functions encompass any activities that determine the generation, distribution, or quality of the power product. The communication activities span distribute automation, utility to utility, utility to substation, utility to generation, and others.

It is a subject of this report to determine the types of communications used (within the scope of IEC Technical Committee 57), and the impact of threats upon this technology. However, many of the threats deal with weaknesses in the communication architecture and topology. At the highest level, shown in Figure 2, any interface point directly or indirectly between business entities offers a high probability for a security-related event to occur. However, in order to protect the information available at such points, and in order to recommend appropriate security policy rules, the actual communication topologies of such interfaces needs to be discussed.

The customer, as shown in Figure 2, actually has two major interface points to potentially three different business entities. However, the topologies employed for the account and business activities function will typically be based upon e-commerce or Internet technologies/topologies. However, the measure and control function represents a topology that is similar to the quality, distribution, transmission, generation, and substation topologies used by utilities.

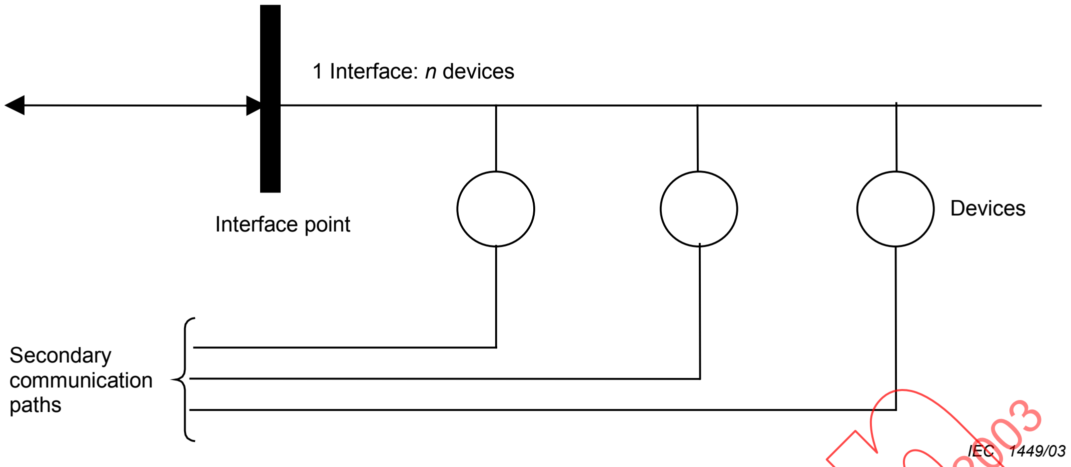

Figure 3 – General communication topology

Figure 3 shows a primary communication path to one or more devices/sources of data and optional secondary communication paths. Any of these paths may be interfaces where security threats may be introduced. Each interface point, even to the actual device, needs to be evaluated for its risk. As part of the security analysis, protocols and communication media also tend to impact the risk. It is the scope of this report to determine the exposure to major threats, based upon these factors, and to develop recommendations for baseline controls based upon this analysis.

6.2 User consequence based analysis

It is clear that the importance of the information, and thereby the amount of effort that a company is willing to expend to protect that information, is an extremely subjective view. The importance is determined by the entity or stakeholder based upon the consequences to the stakeholder's business or interests of a successful attack. Therefore, a methodology of security analysis based upon stakeholders and consequences has been developed.

6.2.1 Stakeholders

The definition of a stakeholder is any entity whose business processes can be impacted through a successful security attack. The stakeholder categories, for the purposes of this Technical Report[1], which can be identified in Figure 2, are:

a) *Generation company (GENCO)* – these are business entities whose end product is electric power. These stakeholders typically have large capital investments in generation facilities.

b) *Transmission company (TRANSCO)* – these are business entities whose end product is the delivery of electric energy, produced by a GENCO. The delivery of the energy is typically to a DISCO. A TRANSCO is typically a customer of a GENCO.

c) *Distribution company (DISCO)* – these are business entities whose end product is the delivery of electric energy to the customer. These stakeholders have assets and communication requirements that span large geographic areas and service multiple customers. A DISCO is a customer is a TRANSCO.

d) *Data aggregator* – these are business entities that process customer metering data in bulk by aggregating it for each supplier so that it may be used to calculate payments owed to each GenCo, TransCo, and DisCo for the use of their energy and transport facilities.

e) *Meter service provider* – these are business entities that provide services to install and maintain (meter operation) and also read (data collection) customer’s meters.

[1] The definition and delineation of stakeholders and business processes may be region specific. Check with the appropriate regional regulatory authority for details.

f) *Supplier* – these are business entities which purchase electricity on the wholesale market and sell it to end customers. They operate without the geographical restriction of owning a network and pay a use-of-system charge to distribution companies.

g) *Risk management market participant* – these are business entities that sell, trade, broker or otherwise participate in markets for derivative financial instruments. Examples of these are futures, options, hedging, options on futures, swaps, or other securities that are created and traded. The objective of these is to manage the risk of price fluctuation and other contingencies of electric energy associated with forward contracts for purchase and sale of electric energy.

h) *End customer* – is a business entity or individual that purchases energy or utility services and needs to verify that contractual commitments are being fulfilled.

Each stakeholder may require information from one or more business activities. Therefore, a matrix of such activities has been developed in order to determine the areas of analysis that this report should focus upon.

Table 1 shows the considered matrix of generic stakeholders and business processes. The ‘x’ indicates that a specific stakeholder requires or provides information relevant to a particular business process. Regional variations of stakeholders or business processes may be formed through a combination of these categories.

The fact that stakeholders do not map one-to-one to business organisations is critical to the understanding of Table 1. For example, it might appear that an ‘x’ should be placed in the box at the intersection of the tertiary asset leveraging row and the DISCO column, since a business organisation serving as a DISCO would be interested in leveraging its distribution lines (for example, by carrying message traffic). However, the activity of serving a message-transfer market is a supplier activity rather than a DISCO activity. Thus, the ‘x’ is placed in the supplier column rather than the DISCO column, even though the business organisation might be thought of as a DISCO rather than a supplier.

Table 1 – Matrix to determine business process importance

Business process	**Stakeholders**							
	GENCO	DISCO	TRANSCO	DATA	METER	SUPPLIER	RISK MNGT.	END CUST.
Buying and/or selling of energy	x					x	x	x
Generation of power (includes power quality)	x	x	x	x	x	x	x	x
Transmission of energy (includes power quality)	x	x	x	x	x	x		
Distribution of energy (includes power quality)		x	x	x	x	x		x
Measurement of trading (revenue metering)	x	x	x	x	x	x		x
Asset management	x	x	x		x			
Energy conservation	x	x	x			x		x
Information mining				x		x	x	
Tertiary asset leveraging[a]						x		x
Risk management	x					x	x	x

[a] An example of this is offering internet connectivity over the resources used for other business processes.

Based upon an analysis of stakeholder concerns and business processes, the most important business processes to secure are:

- generation of power,
- transmission of power,
- distribution of power,
- measurement of trading,
- asset management,
- energy conservation.

6.3 Consequences to be considered

In order to perform a consequence based security analysis, the major consequences of concern to the stakeholders and their respective business practices need to be determined. In regards to the set of business processes, which are recommended to be the focus of further security work within IEC Technical Committee 57, the major consequence categories which need to be considered are: financial; asset destruction/degradation; and the inability to restore service.

6.3.1 Financial

This category includes any activity that results in a financial loss to one stakeholder or a financial gain to another stakeholder. This financial consequence is also affected by loss or degradation of an asset (see 6.3.2). Activities, or events, which can cause financial consequences, are found in the following Subclauses.

6.3.1.1 Loss of revenue

Loss of revenue can be caused by a number of factors:

a) **Increased competition**

This arises from activities such as a competitor infringing a stakeholder's market (either licitly or illicitly) due to lack of security of the stakeholder's system. This may also come about as a result of information leakage from the stakeholder itself.

b) **Loss of customers**

A stakeholder may loose customers through events such as:

- contractual disputes,
- non-competitive pricing,
- lack of trust, caused for example through low consumer confidence,
- reduced reliability of service,
- the inability to deliver service,
- slow reaction to market fluctuations and trends,
- poor response to customer demands.

c) **Inability to gain customers**

A stakeholder may be unable to gain customers through reasons similar to those listed above such as slow reaction to the market fluctuations and trends, non-competitive pricing, etc. The inability to gain customers may also be caused by a damaged reputation through loss of customers.

6.3.1.2 Reduced profitability

Reduced profitability can be caused by:

- increased cost for resources of production,
- cash flow disturbances.

This can be caused by a number of events – for example predatory insider trading on power futures, an attack on the billing database resulting in an inability to bill, etc.

6.3.1.3 Manipulation of production and consumption data

This can be caused by:

- erroneous metering information – for example deliberate falsification of consumption or production data,
- erroneous demand forecasts,
- alteration of metered information during aggregation or billing,
- loss of information.

6.3.1.4 Artificial change of stock value

Any of the above may cause changes in stock value. However, there are other events (illicit) which may artificially change the stock value:

- rumours,
- analyst forecasts.

6.3.2 Asset destruction/degradation

This category includes activities that will result (deliberate or not) in the destruction or degradation of an asset in such a way that the required service or operation of that asset cannot be fulfilled. Activities or events that can cause these include:

- improper asset operation,
- improper asset maintenance,
- inadequate protection/security,
- inordinate expenditure of human assets.

Typical assets that may be attacked and should be part of an analysis include:

- power system resources (power lines, transformers, generators, bus-bars, etc.),
- control systems (SCADA, EMS, etc.),
- metering (data acquisition, meters, etc.),
- information systems (for example OASIS).

The relevance of these assets and their information to particular business processes is shown in Table 2. Additionally, the relevant IEC Technical Committees are indicated in the table (where known).

Table 2 – Asset to business process relationships

Asset business process	EMS (IEC TC 57)	SCADA (IEC TC 57)	Generators (IEC TC xx) (IEC TC 57)	Power lines (IEC TC 38) (IEC TC 57)	Transformers (IEC TC 14) (IEC TC 57)	Switch device (IEC TC 17) (IEC TC 57)	Metering (IEC TC 13) (IEC TC 57)	Info systems (TC xx)
Buying and selling of power	✔		✔				✔	✔
Generation of power (includes power quality)	✔	✔	✔		✔	✔	✔	✔
Transmission of power (includes power quality)	✔	✔		✔	✔	✔	✔	✔
Distribution of power (includes power quality)	✔	✔		✔	✔	✔	✔	✔
Measurement of trading (revenue metering)		✔	✔	✔			✔	✔
Asset Management	✔	✔	✔	✔	✔	✔	✔	✔
Energy Conservation	✔	✔	✔				✔	✔
Information mining		✔					✔	✔
Tertiary asset leveraging				✔	✔			✔
Risk management	✔	✔						✔

6.3.3 Inability to restore service

This category includes activities that result (deliberate or not) in the stakeholder being unable to maintain obligated services. Activities, or events, which can cause these include:

- loss of information that is necessary for the relevant services or operations,
- misinformation resulting from incorrect perception of the state of the power network,
- loss or degradation of an asset (see above),
- improper action (or no action) by personnel,
- inability to act upon receiving correct information (for example data deluge),
- communication capacity exhaustion,
- other resource exhaustion.

6.4 Consequences and security threats

The pre-requisites for performing a security analysis based upon potential business consequences have now been defined. These are:

a) Identify the stakeholders within the communication environment.

b) Identify business processes that are of concern to the stakeholders.

c) Identify consequences that can adversely affect the business processes.

d) Identify events that can cause the consequence(s) to be realised.

The next step is to determine the security threats that, if successful, can cause the consequences to be realised.

An example analysis of part of the “inability to restore service” consequence is presented in Figure 4.

Figure 4 shows that “Loss of asset” can lead to the inability to restore service (the consequence). The next step is to analyse what events, or sequences of events, can lead to “Loss of asset”.

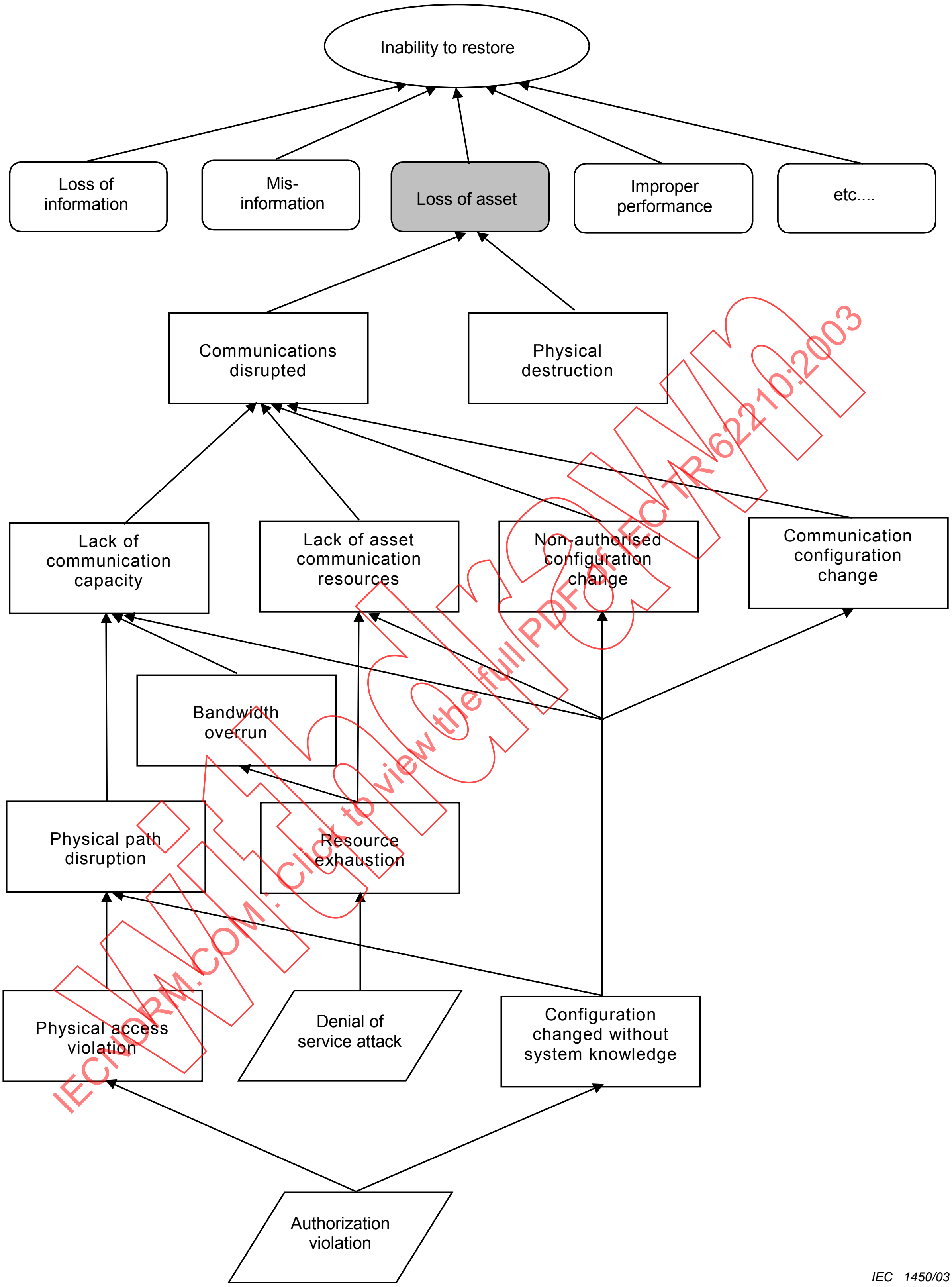

Figure 4 – Consequence diagram: inability to restore service

The sequence of events that can lead to “Loss of asset” can occur through several paths. However, all paths dealing with communications resolve to the consequence being achieved through the successful security attacks of either “Denial of service” or “Authorisation violation”.

NOTE More detail and complete consequence diagrams need to be created in order for a utility to determine which threats are of primary importance to be countered or at least detected. However, several general consequence diagrams may be found in Annex C of this Technical Report.

7 Focus of security work within this report

A comprehensive security analysis, and the resulting countermeasure recommendations, of all protocols within the auspices of IEC Technical Committee 57 would create a tomb of documentation. Likewise, the time constraint for this report's publication has forced a focussed analysis.

Therefore, the focus of this report has been in areas that are considered most vulnerable and whose countering will lead to the greatest decrease in security risk within the communication infrastructures using IEC Technical Committee 57 protocols. In order to determine the focus of this report, a short explanation follows as to the threats and risks that are typically considered relevant on a communication model basis. The communication reference model considered is the OSI 7-Layer Communication Reference Model (ISO/IEC 7498-1).

7.1 Justification of application level security focus

It should be noted that depending upon the consequence analysis, different attacks may need to be countered. However, general security/counter technology is typically applied to the following layers: physical, transport, and application. A close inspection of the communication model security matrix shows that application of appropriate security functions in the application/user domain can address a vast majority of the typical security threats that may occur. Additionally, only security countermeasures at the application layer can minimise the security risks of unauthorised access and illegitimate use.

Table 3 details the typical security risks that are known to be associated with the individual communication functions of the OSI layers. This report will focus on application layer security issues. It is recommended that future work at the lower layers, starting with the transport layer, should be considered.

Table 3 – Communication model security matrix

Layer	Communication function	Typical risks	Typical security attacks
Application	Responsible for conveying user/business information in a standard protocol.	Information leakage[a] Unauthorised access Illegitimate use Denial of service	Masquerade Bypassing controls Authorisation violation Service spoofing Message Intercept/alter/replay Denial of service Resource exhaustion
Presentation	Responsible for translating local representation to a standard/well known transfer representation.	Information leakage	
Session	Responsible for maintenance of connection oriented sessions.	Information leakage	
Transport	Responsible for maintenance of connection oriented sessions.	Information leakage Denial of service	Denial of service Resource exhaustion
Network	Responsible for routing between communications segments (for example LAN to WAN).	Information leakage Denial of service	Denial of service Masquerade Message Intercept/alter/replay
Link	Responsible for local addressing and media access algorithm implementation.	Information leakage Denial of service	Denial of service
Physical	Responsible physical interface to transmission media and any required modulation.	Information leakage Denial of service	Physical Disruption Eavesdropping Denial of Service

[a] Information leakage can occur via direct (for example packet decoding) or indirect (for example traffic analysis) means.

7.2 Security analysis technique

It is recommended that consequence based analysis (see 6.2) shall be used to develop a list of relevant threats to the system. These threats shall be used as input to the recommended formal documentation methodology.

After reviewing several different methodologies for documenting security issues, it is recommended that IEC Technical Committee 57 shall use ISO 15408 for this purpose. ISO 15408 details the development of Protection Profiles (PPs), Target of Evaluation (TOE), and Security Targets (STs).

As defined in ISO 15408, a protection profile states assumptions about a target of evaluation, identifies threats to that TOE based on the assumptions, gives security goals to counter the threats, and finally identifies security functions to satisfy the security goals. An implementation of a PP is defined as a security target against which security threats and attacks can be executed.

However, the work encompassed by IEC Technical Committee 57 requires the generation of multiple TOEs. Subclauses 7.2.1, 7.2.2 and 7.2.3 should be used by IEC Technical Committee 57 as a basis to generate the appropriate set of TOEs. It is recommended that IEC Technical Committee 57 develop TOEs for IEC Technical Committee 57 protocols that are in use within the industry. The first set of TOE developments, that are recommended as future IEC Technical Committee 57 work items, includes:

a) IEC 60870-6 TASE.2,

b) IEC 60870-5,

c) IEC 61334,

d) IEC 61850.

It is inconclusive, at the time of the publication of this report, if TOEs need to be generated for the output of IEC Technical Committee 57 Working Groups 13 and 14. Additional system/ application specific TOEs (for example key management, system level authentication, and enterprise system) will need to be considered in the future.

NOTE Further details and an example PP are included in annexes.

7.2.1 Security objectives

Security goals and functions include:

a) *Confidentiality* – ensuring that information is not disclosed to unauthorised persons.

b) *Integrity* – ensuring that information held in a system is a proper representation of the information intended and that it has not been modified, created, or deleted by an unauthorised person.

c) *Availability* – ensuring that information processing resources are not made unavailable by malicious action.

d) *Non-repudiation* – ensuring that agreements made electronically can be proven to have been made.

e) *Administration* – management of the security system.

f) *Prosecution* – performance of such functions as may be required to enable and facilitate legal action against perpetrators of malicious activity, under applicable law.

7.2.2 General threats

Threats are made against the assets or information used by business processes and/or stakeholders (as defined in 6.2.1). Sources of threats include:

a) act of nature,

b) equipment failure,

c) legitimate user inadvertently acting on an insufficiently protected system,

d) legitimate user violating the limits of authorisation for malicious reasons (insider threat),

e) intruder coherently and/or logically penetrating system,

f) intruder acting without coherent or logical penetration of system,

g) warfare,

h) human or computer error,

i) interaction of the above sources.

7.2.3 Specific threats to be considered in PP

The following list includes the possible threats anticipated against electric power telecontrol and teleprotection systems that might use IEC Technical Committee 57 protocols. The list of threats is intended to address the end systems as well as the telecommunications between them. For each instance considered, some subset of the threats would apply. Not all threats would apply in each case. For example, for a telecontrol or teleprotection system that is not interconnected to other systems, the threats involving use of the telecontrol or teleprotection system to attack other interconnected systems would not apply. Similarly, in a telecontrol or teleprotection system in which the making of electronic agreements is not a function, the repudiation threats would also not apply.

The format used for identifying threats here is intended to facilitate use of the threats in preparing protection profile documents under the common criteria. The intent is to simplify the eventual preparation of protection profiles for products to be used in protecting electric power telecontrol and teleprotection equipment/systems. A common criteria protection profile document represents the user requirement for protection. The offered product protection description is contained in a security target document. These and other documents also define the product tests and other assurance procedures to be followed. The common criteria standards are intended to facilitate the development of products that can be certified and listed as conforming to specified requirements, and to facilitate communication of requirements and offered capabilities between the acquirer of a system requiring security protection and the provider of that system.

Natural threats are beyond the scope of this technical report.

Subclauses 7.2.3.1 to 7.2.3.4 document a set of threat definitions. These Subclauses define threats as being generally applicable for system level TOEs (general). Additionally, these Subclauses define a set of threat definitions that may be applicable to protocols (protocols).

These threat definitions are a first step to defining an inclusive list of system threats that may occur as a result of constructing a system consisting of multiple TOEs.

In general, there is a hierarchy of threat definitions: general, protocol, and TOE specific (for example specific threats defined as part of the TOE development).

7.2.3.1 Confidentiality threats

7.2.3.1.1 General

T.CONF1	Authorised user improperly obtaining unauthorised information from TOE
T.NOAUT-VIEW	Unauthorised user viewing TOE data
T.CONF2	Authorised user improperly using access to TOE to obtain unauthorised information from other interconnected systems
T.CONF3	Intruder using penetration of TOE to facilitate obtaining unauthorised information from other interconnected systems
T.TRAFFIC-ANALYSIS	Intruder inferring unauthorised information by observing patterns or other characteristics of message traffic to which access is not authorised or to which access is authorised only in encrypted form, depending on the medium used for transmitting the traffic and the laws applicable to that medium in the relevant country

7.2.3.1.2 Protocol

T.NOAUT-VIEW	Unauthorised user viewing TOE data
T.TRAFFIC-ANALYSIS	Intruder inferring unauthorised information by observing patterns or other characteristics of message traffic to which access is not authorised or to which access is authorised only in encrypted form, depending on the medium used for transmitting the traffic and the laws applicable to that medium in the relevant country

7.2.3.2 Integrity threats

7.2.3.2.1 General

T.INTEG1	Authorised user maliciously commanding and mis-operating TOE without authorisation to command or operate that TOE
T.INTEG2	Intruder commanding and mis-operating equipment without authorisation to command or operate that equipment by impersonating the SCADA master or modifying and re-transmitting legitimate messages from the SCADA master
T.HIJACK	Intruder mis-operating TOE by hijacking authenticated association
T.REPLAY	Intruder causing mis-operation of TOE or transmission of old information by replaying old messages
T.IMPERSONATE	Unauthorised user assuming the identity of an authorised user
T.CHANGE	Adversary modifying or destroying TOE data
T.INTEG3	Authorised user maliciously loading false parameters into remote equipment without authorisation to access that equipment
T.INTEG4	Authorised user improperly using access to TOE to place false information in other interconnected systems to which access is not authorised
T.INTEG5	Intruder penetrating TOE to facilitate placement of false information into other interconnected systems to which access is not authorised

7.2.3.2.2 Protocol

T.INTEG2	Intruder commanding and mis-operating equipment without authorisation to command or operate that equipment by impersonating the SCADA master or modifying and re-transmitting legitimate messages from the SCADA master
T.HIJACK	Intruder mis-operating TOE by hijacking authenticated association
T.REPLAY	Intruder causing mis-operation of TOE or transmission of old information by replaying old messages
T.IMPERSONATE	Unauthorised user assuming the identity of an authorised user
T.CHANGE	Adversary modifying or destroying TOE data

7.2.3.3 Denial-of-service threats

7.2.3.3.1 General

T.AVAIL1	Authorised user maliciously denying access to TOE
T.AVAIL2	Intruder maliciously denying access to TOE
T.AVAIL3	Authorised user improperly accessing TOE to maliciously deny use of other interconnected systems to authorised, legitimate users
T.AVAIL4	Intruder accessing TOE to maliciously deny use of other interconnected systems to authorised, legitimate users

7.2.3.3.2 Protocol

T.DENIAL-OF-SERVICE	User maliciously denying access to TOE. This is a combination of T.AVAIL1 and T.AVAIL2.

7.2.3.4 Repudiation threats

7.2.3.4.1 General

T.REPUD1	Authorised user repudiating a TOE transaction

7.2.3.4.2 Protocol

None identified.

7.2.3.5 Administration threats

7.2.3.5.1 General

T.ADMIN1	Authorised user inadvertently operating TOE in a situation where such operation is not authorised by policy but does not violate any authorisation constraint of the system. (The authorisations in the system do not reflect the organisation's policy.)
T.ADMIN2	Authorised user improperly gaining unauthorised access to the security functions
T.ADMIN3	Intruder gaining access to the security functions
T.ADMIN4	Authorised user improperly disabling functions or changing parameters to avoid having unauthorised activity recorded
T.ADMIN5	Intruder disabling functions or changing parameters to avoid having unauthorised activity recorded
T.ADMIN6	Authorised user improperly using a denial-of-use attack on the recording system (such as forcing an overflow of storage capacity) to avoid having unauthorised activity recorded
T.ADMIN7	Intruder using a denial-of-use attack on the recording system (such as forcing an overflow of storage capacity) to avoid having unauthorised activity recorded
T.ADMIN8	Authorised user improperly deleting records of unauthorised activity
T.ADMIN9	Intruder deleting records of unauthorised activity

7.2.3.5.2 Protocol

T.ADMIN3	Intruder gaining access to the security functions
T.ADMIN7	Intruder using a denial-of-use attack on the recording system (such as forcing an overflow of storage capacity) to avoid having unauthorised activity recorded
T.ADMIN9	Intruder deleting records of unauthorised activity

8 Vulnerabilities

8.1 Threats to topologies

The generic model of the communications topology shown in Figure 3 can be described in terms of LANs and WANs by that shown in Figure 5.

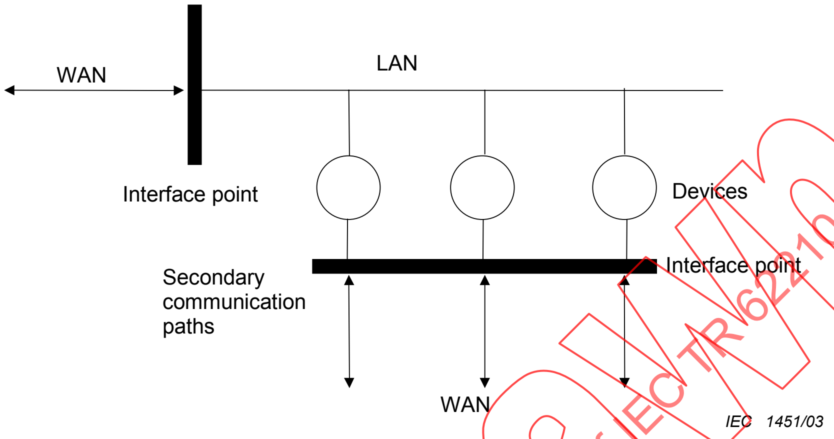

Figure 5 – WAN/LAN topology

Where the interface points is the vector of attack. The LAN is assumed to be within a physically secure environment.

Typical examples of this network topology are:

- EMS/SCADA applications, where examples of the devices are the operator workstations (HMI) and database server (both normally with no secondary WANs) and the telemetry front end processors with their WAN connections to the utility's substations.
- The LAN would typically be an Ethernet network – with an interface point to the high bandwidth corporate network or to the Internet to provide a connection to other applications.
- At the utility's substation, where examples of the devices are the substation IEDs (protection devices, metering equipment, local HMI etc) which may be connected using an Ethernet LAN, a field bus LAN, a serial LAN or similar.
- Some IEDs may have secondary (WAN) links to either local or remote devices with capabilities for informative interfaces, for configuration interfaces, for bulk data transfers.
- The main interface point into the substation, the WAN to LAN interface, is typically implemented by an RTU, a PLC, or a gateway/router.

Threats to a LAN differ from those to the WAN. Principally, without a WAN connection a would-be intruder requires physical access to the customer premises to penetrate it. LAN threats thus come from the disgruntled employee or the unauthorised employee rather than a third party intruder.

The interface points represent the key points of connections between the customer's LAN and the external communications infrastructure – and these points, together with the associated communications media at these points, are the principal focus for looking at threats. Different technologies that may be used to implement the WANs each offer different sets of security issues, the typical WAN technologies in use today being:

- radio (licensed or un-licensed),
- Distribution Line Carrier (DLC), power line carrier,

- private wire, fibre,
- leased lines,
- independent network provider (POTS, mobile telephone systems, packet radio, X.25 etc).

The vulnerabilities of the topologies based on these technologies with the protocol threats identified above are shown in Figure 6, for configurations with either a single WAN/LAN interface point and for configurations with a second, redundant, WAN/LAN interface point. The risks assessed below represent the likelihood of an attack being attempted based upon the ease of acquiring resources and knowledge required to perpetrate the attack. Motivations for attacks have not been factored into the risk levels nor have the likelihood of physical damage (accidental or malicious).

L = Low risk
M = Medium risk
H = High risk

	Radio	Power line carrier	Private wire, fibre	Leased line	POTS etc	Redundant WAN
Confidentiality						
T.NOAUTH-VIEW	**H**	**H**	**L**	**M**	**M**	**-**
T.TRAFFIC-ANALYSIS	**H**	**H**	**L**	**L**	**M**	**-**
Integrity						
T.INTEG2, T.CHANGE, T.REPLAY	**H**	**H**	**L**	**L**	**H**	**-**
T.IMPERSONATE	**H**	**H**	**M**	**M**	**H**	**-**
T.HIJACK	**H**	**H**	**L**	**M**	**L**	**-**
Denial of Service						
T.DENIAL-OF-SERVICE	**H**	**H**	**H**	**H**	**H**	**M**
Administration						
T.ADMIN3, T.ADMIN7, T.ADMIN9	**H**	**H**	**M**	**M**	**H**	**-**

IEC 1452/03

Figure 6 – Levels of vulnerability

Figure 6[2] is intended to highlight those areas that are most vulnerable, so as to identify where further security analysis is required to define counter measures. The IEC Technical Committee 57 protocols in use at these most vulnerable points then need to be analysed to determine if, and how, they can provide the relevant counter measures.

For the threats, Figure 6 highlights the following:

- **Confidentiality, integrity and administration**

  POTS and third party networks, radio and PLC solutions are at a medium to high risk of intruder attack. Information about the networks, protocols, etc. is readily available from a number of open sources. So it is not too difficult for the intruder to eavesdrop and hence gain access to confidential information, alter information, replay information exchanges, spoof or masquerade.

  The use of private or leased lines is at a less risk of intruder attack because of the increased difficulty for the intruder to gain physical access to the media.

[2] Figure 6 is intended to show the vulnerabilities of the identified media and threats and is not necessarily an exhaustive list of all media and threats.

- **Denial of service**

  POTS and third party networks are particularly susceptible to this attack. Intruders can often determine the “network address/number” very easily from public information and then establish a link to that interface point. Once established, the link is then unavailable to the legitimate user unless a secondary link is available.

  Radio networks are also particularly susceptible to this attack – being susceptible to frequency jamming. Again, the information about frequencies etc. that are in use is often easily obtained by an intruder from public sources.

  Other media are susceptible to denial of service attacks – but more in the form of resource exhaustion. Here the intruder prevents legitimate use of the media by generating large amounts of traffic to the interface point thus degrading response times and even saturating the device so as to make the device non-operational.

This shows us that there are substantial issues that need to be resolved in regards to communications security at the WAN interface points. Many of the issues, and the criticality of security threats, change depending on the communication architectures and media. However, certain conclusions can be drawn:

- Communications security starts with restricted/secure access to the communications channels.
- Denial of service attacks is potentially a high risk given single communications channels to devices. Counter measures must be implemented to these threats or multiple communications paths provided to minimise the risk of total denial of service.
- Devices need strong audit and repudiation capabilities to improve communications security.
- Where a topology is used for multiple applications (for example SCADA and enterprise applications) then risks may be higher than those shown above – with threats to one application affecting the other application.

8.2 Current IEC Technical Committee 57 protocols

Within the scope of IEC Technical Committee 57, the following protocols have been standardised or specified:

8.2.1 TASE.1

One of the activities of IEC Technical Committee 57 Working Group 07 has been the production of the IEC 60870-6 series of standards (telecontrol protocols compatible with ISO standards and ITU-T recommendations). Parts of this series concern Telecontrol Application Service Element No. 1 (TASE.1):

- IEC 60870-6-502: TASE.1 protocol definitions,
- IEC 60870-6-504: TASE.1 user conventions,
- IEC 60870-6-701: functional profile for providing TASE.1 application service in end systems.

The technical content of this series evolved from work being carried out in Europe, under the umbrella of a protocol known as ELCOM (initially described as ELCOM-83 and later updated with ELCOM-90). TASE.1 and ELCOM-90 are not identical and whilst there are a large number of ELCOM-90 implementations there are, as yet, no vendors offering TASE.1 in their products. This perceived lack of support for TASE.1 leads us to the conclusion that efforts should not be spent on performing a security assessment of TASE.1.

8.2.2 TASE.2

Another of the activities of IEC Technical Committee 57 Working Group 07 has been the production of the series concerning Telecontrol Application Service Element No. 2 (TASE.2) – based on work originating in the USA under the umbrella of the Utilities Communications Architecture (UCA). One of the deliverables from UCA was a protocol for use when transferring information from one control centre to another – the Inter Control centre Communications Protocol (ICCP). Working Group 07 standardised ICCP:

- IEC 60870-6-503: TASE.2 services and protocol,
- IEC 60870-6-702: functional profile for providing TASE.2 application service in end systems,
- IEC 60870-6-802: TASE.2 object models.

This ad-hoc working group has started the security analysis for TASE.2 – the results of the analysis are shown in annex B. This ad-hoc working group believes that a work item to complete the security analysis for TASE.2 is the highest priority for future work. This conclusion is based upon the wide scale deployment of TASE.2, the control aspects, and the financial implications of a successful attack on a TASE.2 system.

This proposed work item should be undertaken in conjunction with similar work items for IEC 61334 and IEC 61850 due to similar architectures and technologies. It is the expectation of the ad-hoc working group that a consistent security methodology can be developed for all three protocols.

8.2.3 IEC 60870-5

IEC Technical Committee 57 Working Group 03 has produced the IEC 60870-5 series of standards, defining recommendations for building a protocol suited to a specific application (or profile). Using these recommendations IEC Technical Committee 57 Working Group 03 has defined a number of protocol profiles:

- IEC 60870-5-101: companion standard for basic telecontrol tasks,
- IEC 60870-5-102: companion standard for the transmission of integrated totals in electric power systems,
- IEC 60870-5-103: companion standard for the informative interface of protection equipment,
- IEC 60870-5-104: network access for IEC 60870-5-101 using standard transport profiles.

The IEC 60870-5 series basic recommendations do not address the issues of a mechanism for access control, encryption, or an authentication method. The companion standards IEC 60870-5-101, IEC 60870-5-102 and IEC 60870-5-103 thus have no current capability of implementing additional security measures. IEC Technical Committee 57 Working Group 03 should analyse the security requirements of these companion standards (producing protection profiles) and use the results to propose any necessary enhancements to the standards. It must be recognised that adding security enhancements to these protocols will be difficult and almost definitely mean the protocols will not be backward compatible with existing implementations.

8.2.4 IEC 61334

IEC Technical Committee 57 Working Group 09 has the title ‘distribution automation using distribution line carrier systems’ and has produced the IEC 61334 series of standards. The scope covers communications protocols for both distribution and customer automation for the LV and MV-Networks. The key documents are:

- IEC 61334-4-41
- IEC 61334-4-42

Most of the interest shown in this these standards has been for remote metering rather than distribution automation. However, metering communication is also covered by IEC Technical Committee 13 Working Group 14. IEC has therefore divided the scope such that the protocol and DLC medium is covered by IEC Technical Committee 57 Working Group 09 but the metering application (and hence metering objects) and other media are covered by IEC Technical Committee 13 Working Group 14. Although the IEC standards refer to DLMS as Distribution Line Message Specification', the commercial promotion of DLMS now refers to it as 'Device Language Message Specification' in order to acknowledge its applicability to other communications media.

DLMS was originally a subset of MMS, ISO/IEC 9506, but its support for low cost devices and for channels with limited transmission capacity (such as DLC) was found to be lacking. In particular it was found necessary to introduce the extension, 'unacknowledged broadcast' for operations such as the synchronisation of time clocks. Subsequently, other variations were introduced so that MMS and DLMS are now non-interoperable. More recently IEC Technical Committee 57 Working Group 09 has sought to address these incompatibilities, but as yet there has been no resolution.

DLMS (IEC 61334-4-41) and the application layer described in IEC 61334-4-42 has a mechanism for access control and some 'hooks' to allow encryption, but there is no explicit authentication method.

DLMS defines a Virtual Distribution Equipment (VDE) object. For example, a named variable with a VDE specific scope of access is freely accessible. For access control, it also defines a Virtual Application Association (VAA). The VAA-specific scope of access restricts access to certain named variables that are only open to the DLMS user that previously created the VAA object.

The application ciphering/deciphering function is provided to ensure security and confidentiality of transmitted data. The algorithm is said to be application dependent and therefore definition is deferred to a companion standard. Two types of key are defined: the global ciphering key and the dedicated ciphering key. The intent of the global ciphering key is to allow ciphered broadcasting. The dedicated ciphering key is contained in the DLMS context and is specific to that instance of application-association.

A one-time copy-check field, avoiding the unauthorised replay of previously sent messages, is foreseen as part of the encryption algorithm.

Key management is not covered in the documents.

IEC Technical Committee 57 Working Group 09 has attempted to initiate further work on security, but this has not made progress due to lack of resources.

It is the expectation of the ad-hoc working group that a consistent security methodology can be developed for the IEC 61334 series, the IEC 61850 series and TASE.2.

8.2.5 IEC 61850

The activities of IEC Technical Committee 57 Working Groups 10, 11 and 12 cover the production of the IEC 61850 series of standards (communication networks and systems in substations). This series of standards defines models for:

- the basic structure of information elements,
- the substation and feeder devices,
- service models such as "time", "reporting", "control", "association" etc.,

and then shows how these can be mapped to a standard protocol stack such as MMS with TCP/IP, the IEC 60870-5 series, Profibus, etc.

The association model defined in IEC 61850 (and its mapping to MMS) is designed to cater for the security requirements of the communications system in question – modelling capabilities for authentication, encryption and data access control (secure views). The IEC Technical Committee 57 Working Groups 10, 11 and 12 should demonstrate the suitability of the IEC 61850 series association model by performing a security analysis – i.e. produce a protection profile for the IEC 61850 series.

It is the expectation of the ad-hoc working group that a consistent security methodology can be developed for the IEC 61850 series, the IEC 61334 series and TASE.2.

9 Recommendations for future IEC Technical Committee 57 security work

a) It is recommended that IEC Technical Committee 57 ad-hoc Working Group 06 becomes a Working Group so that:

1) Comments on this document can be resolved.

2) The Working Group can continue with the completion of the original charter of the ad-hoc Working Group: co-ordination of security work and solutions within IEC Technical Committee 57.

3) The working group can assist in the performance of the work items as recommended for other standards within IEC Technical Committee 57.

4) It is recommended that the working group be responsible for generating work items relating to specific protocol security for individual working group security work items (standard or report) that have not gained support (for example the ballot of the work item failed).

b) It is recommended to make use of consequence based security analysis techniques, for IEC Technical Committee 57 security related activities.

1) Refine the set of business processes upon which consequences should be considered.

The current list of business processes recommended to be considered are:

- generation of power,
- transmission of power,
- distribution of power,
- measurement of trading,
- asset management,
- energy conservation.

2) Refine and further define the set of consequence categories which need to be considered as part of the consequence based security analysis.

The current consequences recommended to be considered are:

- financial,
- asset destruction/degradation,
- inability to restore service.

c) It is recommended that security countermeasures at other OSI communication layers, besides the Application Layer, be considered for future work items on a per protocol/standard basis.

d) It is recommended that work items for the following standards be considered in the areas of security in liaison with the transitioned IEC Technical Committee 57 ad-hoc Working Group 06.

1) It is recommended that the working groups, responsible for the following standards generate work items structured as a joint task force so that consistent security mechanisms can be used by all standards:

NOTE In large part, this recommendation is based upon the commonality of underlying protocols used by these standards.

- IEC 60870-6 TASE.2. It is recommended that resolution of TASE.2 issues be the highest priority.
- IEC 61850 series.
- IEC 61334-4-41 (DLMS).
- IEC 61334-4-42 (application layer).
- It is also recommended that the joint task force establish a liaison with IEC Technical Committee 13 Working Group 14 and IEC Technical Committee 95.

2) It is recommended that the IEC Technical Committee 57 Working Group 03 generate a work item for the IEC 60870-5 series.

3) It is recommended that a transitioned IEC Technical Committee 57 ad-hoc Working Group 06 (for example as a working group) be responsible for generating work items relating to specific protocol security for protocols that individual working group security work items have not gained support (for example the ballot of the work item failed).

e) Security enhancements/work items are not recommended for the following standards.

NOTE In large part this recommendation is based upon usage patterns of the standard.

1) IEC 60870-6 TASE.1.

f) It is recommended that the work items undertaken concentrate on A-Profile security applied as part of application and presentation layer functionality.

1) It is recommended that encryption be considered a Presentation Layer function consistent with ISO definitions (Generic Upper Layer Security – GULS).

2) It is recommended that application layer authentication mechanisms be addressed as part of the work items.

It is recommended that a minimum of three (3) levels of Authentication mechanisms be provided:

- none,
- password,
- strong.

3) It is recommended that the work items address minimum security levels (for example defaults in the instance where no security authentication is provided).

g) It is recommended that the work items undertaken develop protection profiles as part of the work items.

h) It is recommended that the work items include the development of consequence diagrams associated with the specific use of the communication protocol(s).

i) It is recommended that the transitioned IEC Technical Committee 57 ad-hoc Working Group 06 undertake a future work item in regards to encryption key management.

j) Securing a communications channel over which a protocol operates using modern cryptography amounts to performing a presentation transformation of an application protocol data unit to transfer syntax through the use of encryption and its associated secret key(s). The keys that are used by the presentation transformation are maintained on systems that are outside the scope of IEC Technical Committee 57. The security of IEC Technical Committee 57 protocols will only be as good as the security of the systems that maintain the keys. The system(s) that initiates and manages the communications channels needs to be secured and this task should become a work item for IEC Technical Committee 57. The security formalisms should take the form of Common Criteria protection profiles.

k) It is recommended that the transitioned ad-hoc Working Group 06 undertake a future work item in regards to generating system level TOE(s).

l) An important consideration is that protection profiles be created for not only the protocols, but also the systems that support the protocols. These profiles can be used as the basis for creating metrics for component, subsystem, and system level security.

m) This work item will need to analyse the interface boundaries of the TOEs developed as output of other work items.

n) It is recommended that the transitioned IEC Technical Committee 57 ad-hoc Working Group 06 undertake a future work item to identify the architectural patterns used by the systems within IEC Technical Committee 57, (for example a substation LAN pattern) and then perform a consequence analysis on the patterns.

o) The result will be a basis for the set of system architectures and protocols that operate on these architectures. These patterns can be used as templates for initiating a consequence analysis on the architecture of a particular system. This can be used to understand the threats to the specific system. Developing such sets of consequence analyses is an important step towards identifying and mitigating the system threats for architectures used within IEC Technical Committee 57.

p) It is recommended that the transitional IEC Technical Committee 57 ad-hoc Working Group 06 undertake a future work item to define the boundary between physical and information security.

q) Once information security measures are developed, with certain assurance level(s), then there is a need to ensure that corresponding physical security assurance levels are developed. An important problem is to precisely define the boundary between the information security and physical security problems (TOEs).

r) It is recommended that IEC Technical Committee 57 consider a process through which issues of insider threats can be resolved.

s) Specific attention should be given to the insider threat, since this is the most difficult to protect against and has the potential to deliver the most damage for the least amount of resources.