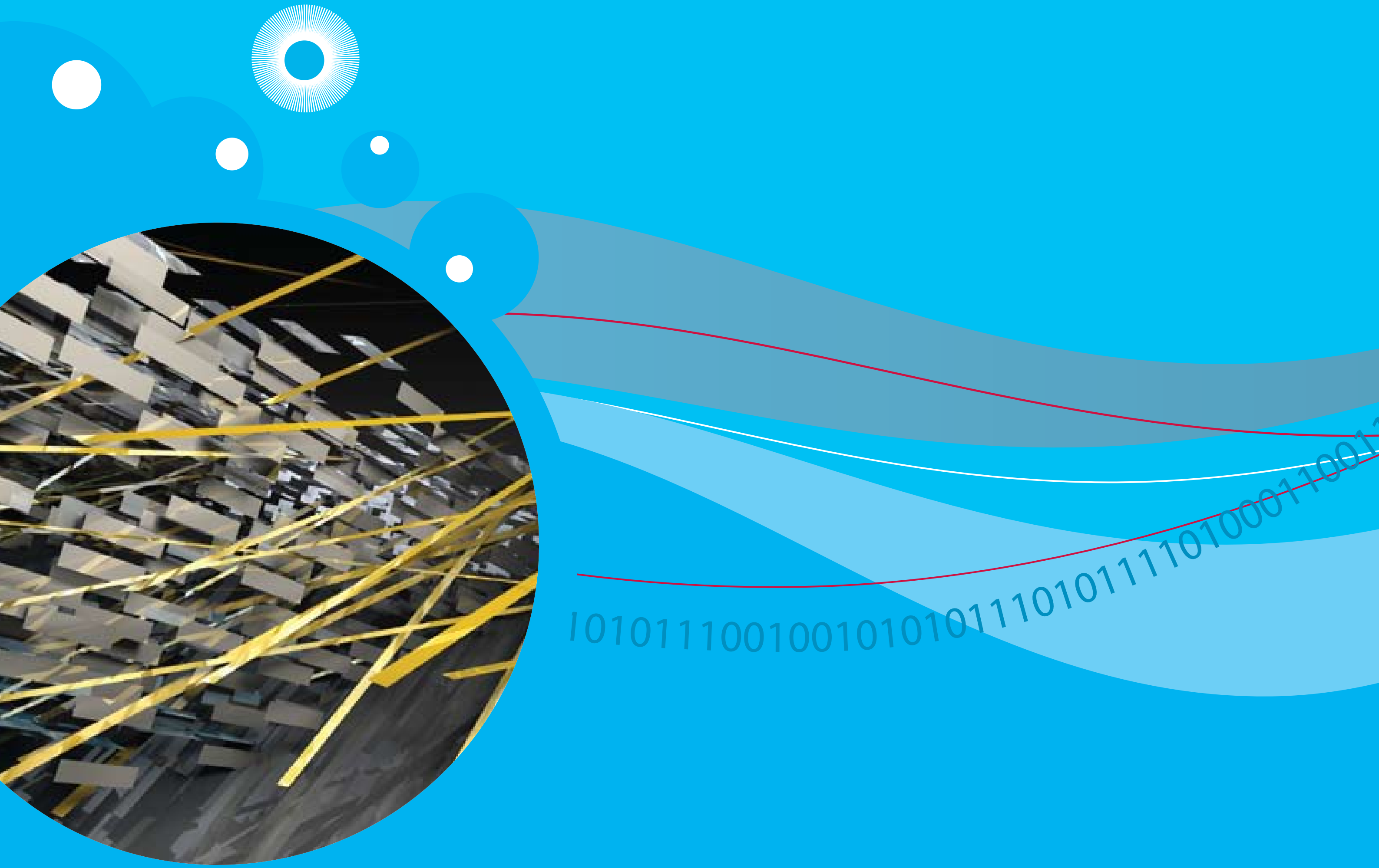


enisa
European Network
and Information
Security Agency

GAPS IN STANDARDISATION

related to resilience of communication networks

enisa
European Network
and Information
Security Agency

About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the agency facilitates contacts between the European institutions, the Member States and private business and industry actors.

Contact details:

For contacting ENISA or for enquiries on this study, please use the following details:
Slawomir Gorniak, Demosthenes Ikonomou, Panagiotis Saragiotis
Email: sta@enisa.europa.eu
Web: http://www.enisa.europa.eu/act/res/technologies/std

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004. This publication does not necessarily represent state-of the-art and it might be updated from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for educational and information purposes only. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Executive summary

Resilience of communications networks is not currently being addressed by the key standards developing organizations (SDOs) other than as guidance for management processes. This report summarises and presents the following key elements:

- the definition applied to resilience in the context of standardisation (section 1 and section 4);
- the identification and presentation of the major activities undertaken in the SDOs in either security or architecture that have a focus on resilience (section 7, section 8 and annex A);
- the identification where should work be undertaken in standardisation activity in either security or architecture, there will be a positive impact on the resilience of networks (section 10 and, in summary form, in each of sections 5, 6, 7, 8 and 9), in light of. the current lack of specific activity on resilience as identified in the SDOs.

The report makes the following recommendations for future standardisation activities:

#1 Work items should be actively promoted in the SDOs (eg, through a mandate) to support the specification of metrics and supporting test and validation criteria to be used in the assessment of resilience (derived, where possible, from existing metrics used in the assessment of reliability and failure analysis).

#2 Work items should be actively promoted in the SDOs (eg, through the means of a mandate) to support the development of a taxonomy for resilience.

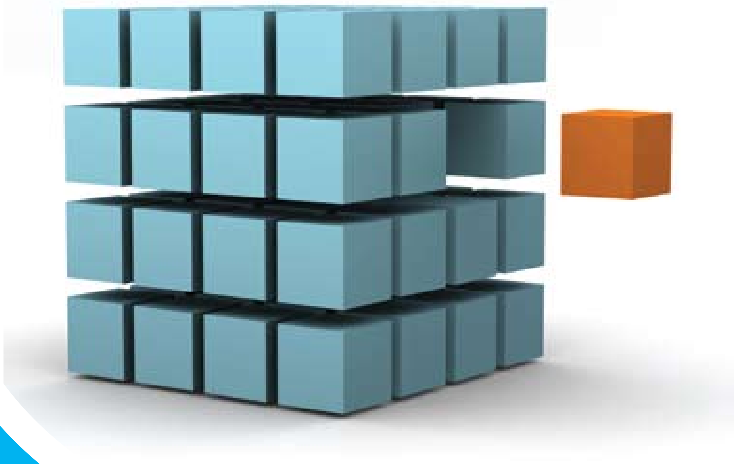
#3 As a very large part of system resilience is enabled by features and capabilities not covered by the conventional telecommunications SDOs, those SDOs should be encouraged to build links from their work to the output of bodies dealing with those ancillary features (eg, power, heat, light, flood control, environmental control, and access, ie, transport links to get maintenance staff to site for repairs).

#4 Add 'resilience' as a 'keyword' in classifying standards in the SDOs.

#5 Update the procedures of SDOs in approving work items to address how resilience will be achieved, eg, if a system implemented using the present document fails, how will the system be maintained (ie, what measures are offered in support of resilience by this standardisation effort).

In addition, the report identifies a number of detailed areas where the SDOs are expected to work in order to facilitate greater assurance of resilience in networks.

Contents



1 Structure of report

1 Structure of report

Resilience is addressed from the point of view of three layers which are the layers of the core network, of the services, and of the content provided. This approach guarantees the consideration of all aspects of the resilient delivery of content over a network using resilient networks where *resilient networks* are defined as:

> Resilient networks are characterised as providing and maintaining an acceptable level of service in the face of faults (unintentional, intentional, or naturally caused) that affect their normal operation. The main aim of the features of resilience is that faults are invisible to users. [2]

The report is structured to discuss resilience against two models of networks:

- one derived from Directive 2002/21/EC of 7 March 2002 *Common Regulatory Framework for Electronic Communications Networks (ECN) and Services (ECS)* (also known as the Framework Directive), in section 2 and section 7;
- the other derived from the security analysis of systems under attack, in section 3 and section 8.

In addition, the report gives a detailed overview of resilience technology in section 4, and identifies the requirements for a taxonomy covering metrics and risk categorisation to be applied to resilience in section 5. The economics of providing resilience are described in section 9.

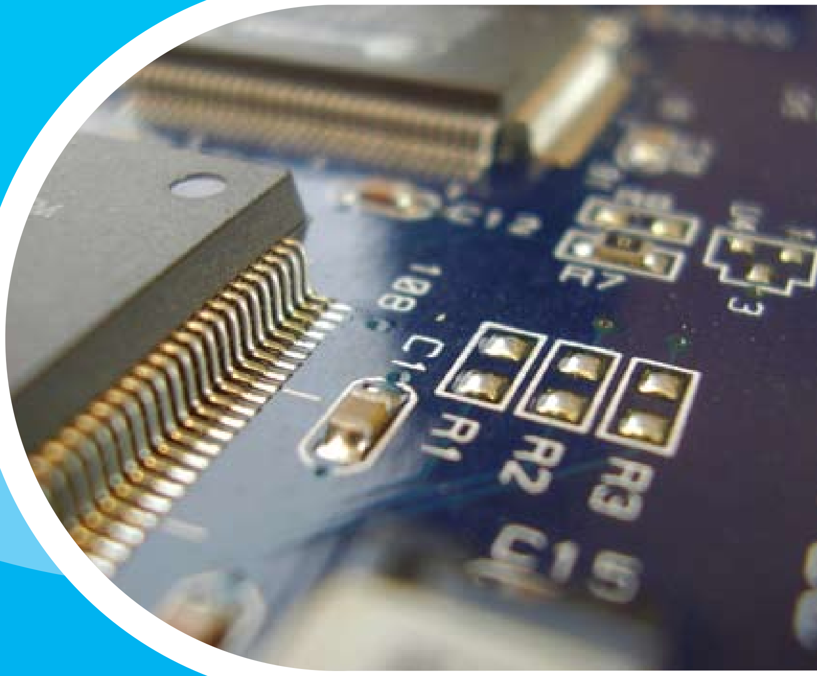
The study was initiated and supported by the members of the Security Tools and Architectures Section of the European Network and Information Security Agency[1]:

- Slawomir Gorniak
- Panagiotis Saragiotis
- Demosthenes Ikonomou.

The work was carried out in close collaboration with a group of leading experts in the field of ICT standardisation. In this light, the contribution of the experts below is gratefully acknowledged.

- Scott Cadzow, Cadzow Communications Consulting Ltd
- Charles de Couessin, ID PARTNERS
- Adrian Mueller, ID Cyber-Identity Ltd
- Salvatore D'Antonio, University of Naples 'Parthenope'.

[1] http://www.enisa.europa.eu/act/res/technologies/inf



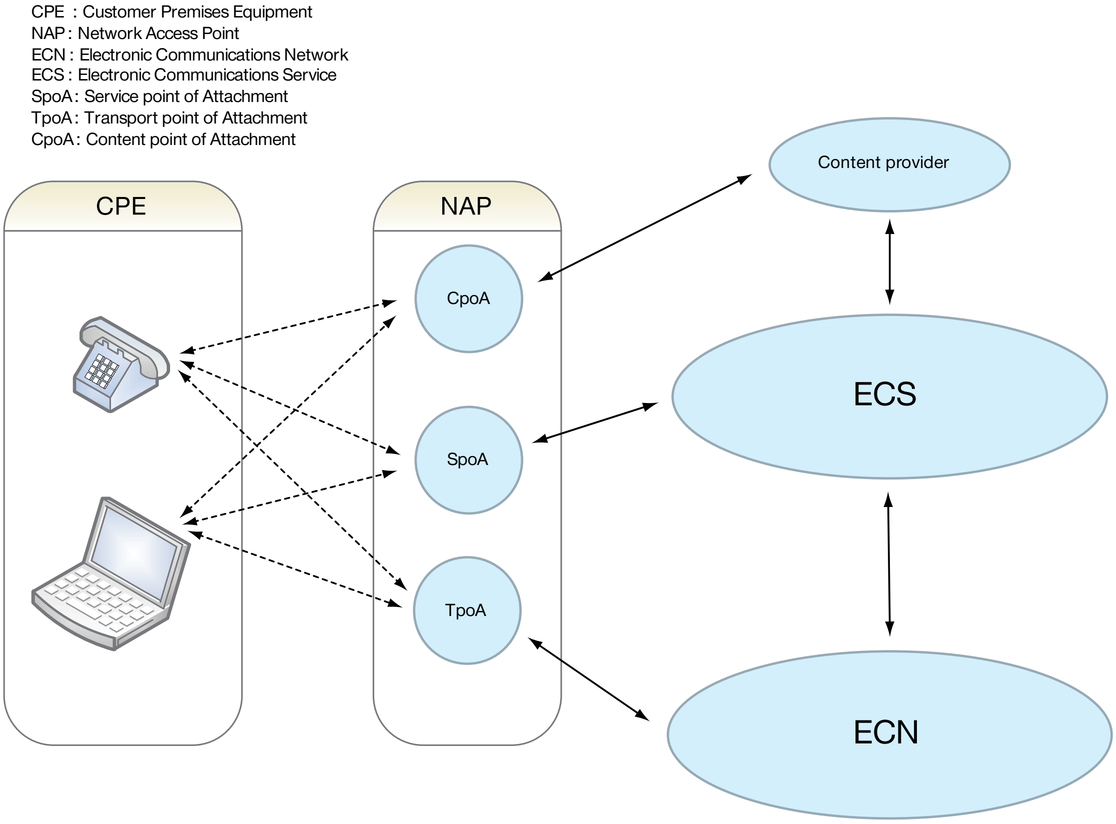
2 Resilience model derived from regulation

2 Resilience model derived from regulation

NOTE: In the bulk of the report, this model is referred to as the regulatory model of networks.

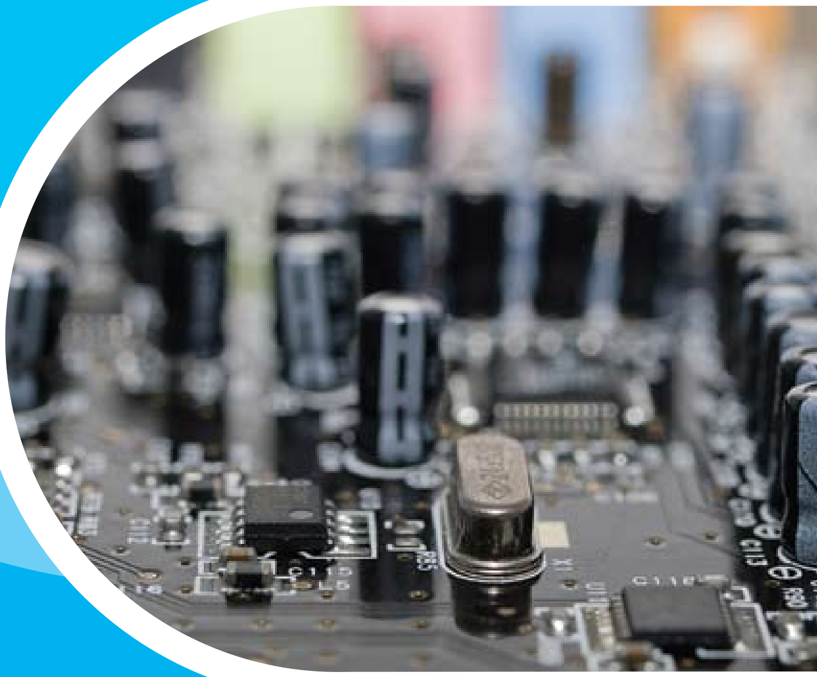
The first model is one drawn from the EU regulatory framework in which telecommunications is expected to operate, which is widely referred to as the Framework Directive [17] and which results in a model referred to as Electronic Communications Networks and Services (ECN&S). It has been extended for the purpose of this report to also consider content providers. This model is illustrated in figure 2.1.

Figure 2.1 – **Extended ECN&S model for resilience analysis**


CPE : Customer Premises Equipment
NAP : Network Access Point
ECN : Electronic Communications Network
ECS : Electronic Communications Service
SpoA : Service point of Attachment
TpoA : Transport point of Attachment
CpoA : Content point of Attachment
CPE
NAP
CpoA
SpoA
TpoA
Content provider
ECS
ECN

This ECN&S derived base model considers a user accessing services of the following types: transport, service, and content. They can be distinguished as follows:

- The network represented by the ECN provides bit pipes and will mostly consist of IP over Ethernet or IP over ATM connections with the possibility of QoS provided by MPLS or similar.
- The network represented by the ECS provides stateful control of services and will support protocols such as SIP.
- The content provider offers end-user content and may offer end-user directed interactive communication (eg, online games, or TV content that is provided using IPTV sessions managed in the ECS over QoS controlled connections in the ECN).



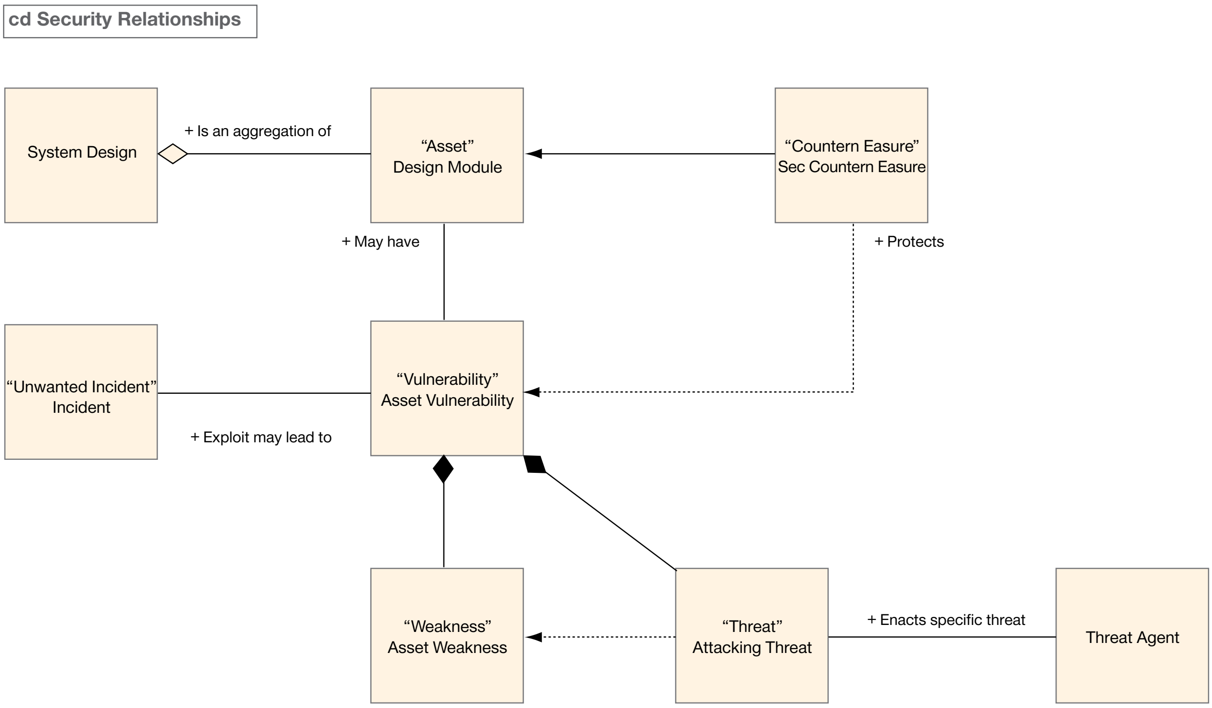
3 Resilience model derived from security analysis

3 Resilience model derived from security analysis

NOTE: In the bulk of the report, this model is referred to as the security model of networks.

The ECN&S model is considered alongside the model of systems under attack shown in figure 3.1, which models a system as an aggregation of assets which may be attacked in isolation or in combination with the aim of defeating the system objectives. An asset may be physical, human or logical. **Assets** in the model may have **weaknesses** that may be attacked by **threats**. A **threat** is enacted by a **threat agent**, and may lead to an **unwanted incident** breaking certain pre-defined security objectives. A **vulnerability**, consistent with the definition given in ISO/IEC 13335 *Information technology - Security techniques - Guidelines for the management of IT security* [45], is modelled as the combination of a **weakness** that can be exploited by one or more **threats**. When applied, **countermeasures** protect against **threats** to **vulnerabilities** and reduce the **risk**.

Figure 3.1 – **Generic system security and attack model**

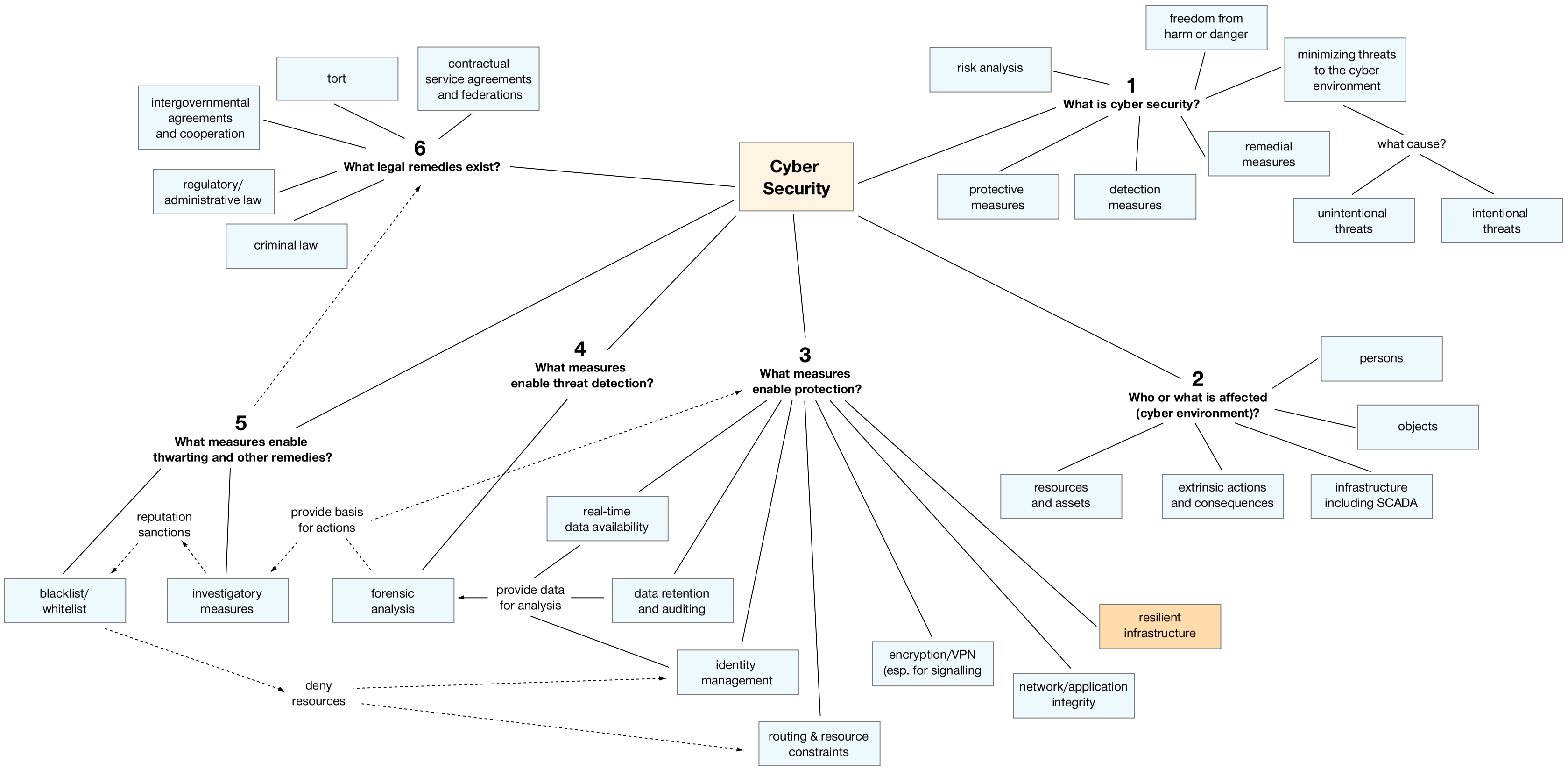


One of the purposes of security design is to minimize the probability of any instance of the class 'unwanted incident' being instantiated. For the purpose of the present report, the incident being explored is 'reduction in system resilience' and thus the report seeks to identify those assets whose vulnerabilities, when exploited, lead to this form of incident.

Whilst traditionally threats can be classified as one of four types (interception, manipulation, repudiation of sending, and repudiation of receiving), and whilst traditionally security objectives can be classified as one of four types (confidentiality, integrity, accountability, and availability), it is the purpose of this report to explicitly consider only those aspects that impact resilience as a composite of the typical security objectives. This is shown in figure 3.2 where a resilient infrastructure is one of the protection measures in the cyber security model.

This report addresses this purpose by examining the roles and work programmes of the main standards bodies that have a direct impact in the field of resilience, with a view both to presenting the standards from these bodies that, when implemented, have a positive impact on the mitigation of attacks that lead to a ‘reduction in system resilience’ and to identifying where further standardisation activity may have a similar positive impact.

Figure 3.2 – **ITU-T ontological model of cyber security stressing resilience**


Cyber Security
1
What is cyber security?
risk analysis
freedom from harm or danger
minimizing threats to the cyber environment
what cause?
unintentional threats
intentional threats
remedial measures
detection measures
protective measures
2
Who or what is affected (cyber environment)?
persons
objects
infrastructure including SCADA
extrinsic actions and consequences
resources and assets
3
What measures enable protection?
resilient infrastructure
network/application integrity
encryption/VPN (esp. for signalling
routing & resource constraints
identity management
data retention and auditing
real-time data availability
4
What measures enable threat detection?
provide data for analysis
forensic analysis
5
What measures enable thwarting and other remedies?
provide basis for actions
investigatory measures
reputation sanctions
blacklist/ whitelist
deny resources
6
What legal remedies exist?
contractual service agreements and federations
tort
intergovernmental agreements and cooperation
regulatory/ administrative law
criminal law

4 Resilience

4 Resilience

NOTE: this section is directly based on ETSI-TR-102445.

4.1 Overview

ETSI TR 102 445 *Emergency Communications (EMTEL): Overview of Emergency Communications Network Resilience and Preparedness* [6] addresses the resilience of networks in the context of an emergency across a broad spectrum of aspects related to the provisioning of telecommunications services in emergency situations. In particular, when emergency situations arise, efficient and effective communications are critical. This statement may be considered as being applicable to social and business operations in general and, as such, the enabling telecommunications technology needs to perform in a robust and reliable manner, providing the requisite functionality to be able to maintain guaranteed service levels. Network resilience and preparedness are critical. TR 102 445 gives an overview of several key technical concepts that can be employed to enhance network resilience and which are considered, in the context of the present report, as essential.

Resilience is a concept associated with optimizing the availability and quality of service of telecommunications systems and support resources. Amongst other objectives, two that are key are to maximize the mean time between failure (MTBF) and to minimize the mean time to repair (MTTR) (see section 5 for an evaluation of these metrics).

Resilience applies at all levels in the system hierarchy: at component level and at system level, and within switching systems, transmission systems and end devices.

Whereas resilient networks are characterised as providing and maintaining an acceptable level of service in the face of faults (unintentional, intentional, or naturally caused) that affect their normal operation [1], much of the mitigation of problems that impact resilience are related to the aims of **business continuity** and **disaster recovery planning** which are themselves governed by specific activities in both response and recovery plans, and in restoration activities.

Resilience is considered in the context of e-commerce continuity in ISO/IEC 17799 [48] and in BS 25999 [55], the standard for business continuity management (BCM) that has been developed to help minimize the impact of any disruption and thus ensure the protection of staff, the preservation of reputation and, in addition, maintenance of the ability to operate and trade. BS 25999 comprises two parts:

- Part 1, the Code of Practice
  - provides BCM recommendations for best practices.
- Part 2, the Specification
  - provides the requirements for a business continuity management system (BCMS) based on BCM best practices. This is the part of the standard that demonstrates compliance through an auditing and certification process.

In addition, the US standard ASIS SPC.1-2009 *Organizational Resilience: Security, Preparedness and Continuity Management Systems—Requirements with Guidance for Use* [53] covers a number of key tasks.

4.1.1 Resilience versus redundancy

Redundancy may be used to offer resilience, and often the terms are used as synonyms although, strictly speaking, they are not. A system offering redundancy that allows, for example, hot switching to alternative transmission media may result in a system that is more resilient. Redundancy is therefore considered in this report as a mechanism to achieve resilience, and standards for both protocols and architectures that support redundancy are identified in this report.

4.2 Component level resilience concept

NOTE: ETSI TR 102 445 [6] identifies a number of key concepts that may be used to address resilience and these concepts are illustrated here and in the remainder of this section using TR 102 445 as a key source extended for the general case (ie, not only emergency telecommunication) as indicative of approaches that may be taken in design and standardisation.

Component level resilience is the concept of incorporating features into the design of an individual component of equipment to enhance its overall availability.

Its features include:

- incorporation of multiple redundant modules within the component, such as power supplies, processor units and data storage modules;
- localized storage of information within the component to enable continued operation in the event of failure of higher-level information sources.

4.3 Multiple component operation concept

Multiple component operation describes the concept of deploying several components to fulfil a particular aspect of system functionality. Components are typically arranged in parallel and can be realised in several modes, of which the dominant modes are:

- Redundant Mode:
  - In the event of failure of the active component, operation is switched to the standby component. The switchover operation can range from manual intervention to fully automatic.
- Active Parallel Mode:
  - In the event of failure, operation continues but with reduced capacity.

The different modes have differing advantages and disadvantages. Regarding redundant mode, design of the application and design of the clustering is simpler and there should be little performance loss in the event of a failure. However the total cost of the system is likely to be higher. Regarding active parallel mode, the opposite arguments will apply: design is more complex and there is performance degradation in the event of a failure, but the total cost of the system will likely be lower in comparison to redundant mode.

NOTE 1: The RAID (redundant array of inexpensive disks) approach, now common in data storage, offers a number of variations that allow different means to address failure of any single component.

NOTE 2: Where a set of identical components are used to provide redundancy in active parallel mode the TTF of the system is not always reduced.

4.4 Circuit diversity and separacy concepts in line transmission systems

Diversity is the concept of ensuring that specified circuits are not routed over the same transmission circuits. However there may be some common physical network sites and/or equipment within the circuit routings.

Separacy is a more reliable means of ensuring that specified circuits are not routed over the same cables, equipment or transmission systems and also that there are no common physical sites within the circuit routings. Normally, separated routes will even enter a building through separated ports using different service facilities (power, etc). They will only physically combine at the circuit terminal equipment.

It should be noted that separacy guarantees diversity, but diversity does not guarantee separacy.

In theory a single incident affecting one particular circuit should not affect transmission capacity in circuits that are diverse or separate. However, the avoidance of a single point of failure can only be guaranteed in fully separated circuits.

4.5 Diverse routing concepts

Diverse routing concepts relate to the ability to use, select or switch between different circuits to avoid congestion or network failure (this may also be referred to under the generic term of load balancing techniques).

Diverse routing capability is built upon the provision of transmission diversity and separacy. Routing and transmission devices are capable of detecting a reduction in performance on a particular circuit and rerouting traffic based on specific rules.

4.6 Fault-tolerant concepts

Fault tolerant systems are devices that are designed and built to correctly operate even in the presence of a software error or failed components. The term is most commonly used to describe computer systems designed to lose little or no time due to issues, either in the hardware or the software running on it.

4.7 Disaster recovery (DR) concepts

Disaster recovery (DR) is a coordinated activity to enable the recovery of telecom/IT/business systems due to a disruption. DR can be achieved by restoring telecom/IT/business operations at an alternate location, recovering telecom/IT/business operations using alternate equipment, and/or performing some or all of the affected business processes using manual methods.

4.8 Service diversity

Service diversity is a concept whereby, if a particular communications service fails, information (or a subset of information) can be transferred by an alternate communications service. Examples from the emergency telecommunications scenarios described in ETSI TR 102 445 [6] include the following:

- If a public TV service fails, public radio systems could still broadcast emergency messages.
- If a commercial cellular telephone system fails, commercial paging systems could still be used for emergency communications.

In a more general telecommunications service, having the option of using both fixed and wireless access to the network may provide a similar level of service continuity.

5 Taxonomy of risks addressed and related policies

5 Taxonomy of risks addressed and related policies

NOTE: The purpose of this section is to identify a structured vocabulary of risk-to-system resilience. It doesn't make a direct reference to standardisation activities, but provides basis for understanding the issues they have to overcome.

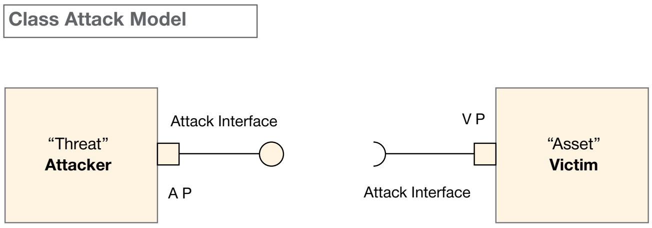
5.1 Risk and attack taxonomies

A *taxonomy* is most often defined as a classification of terms and it has a close relationship with the use of ontologies. It has been suggested that there are three characteristics that define a taxonomy:

- A taxonomy is a form of classification scheme.
  - Classification schemes are designed to group related things together and to define the relationship these things have to each other; an example is given in figure 5.2 of a classification of threats.
- Taxonomies are semantic.
  - Taxonomies provide a vocabulary to describe knowledge and information assets. The vocabulary must be controlled to ensure that each entry in the taxonomy is unambiguous and to ensure also that alternate or less precise terms are excluded (the example in figure 5.1 applies).
- A taxonomy is a kind of knowledge map.
  - A user of the taxonomy should immediately have a grasp of the overall structure of the knowledge domain covered by the taxonomy. The taxonomy should be comprehensive, predictable and easy to navigate; the example of figure 3.2 is a knowledge map of the impact of attacks on systems.

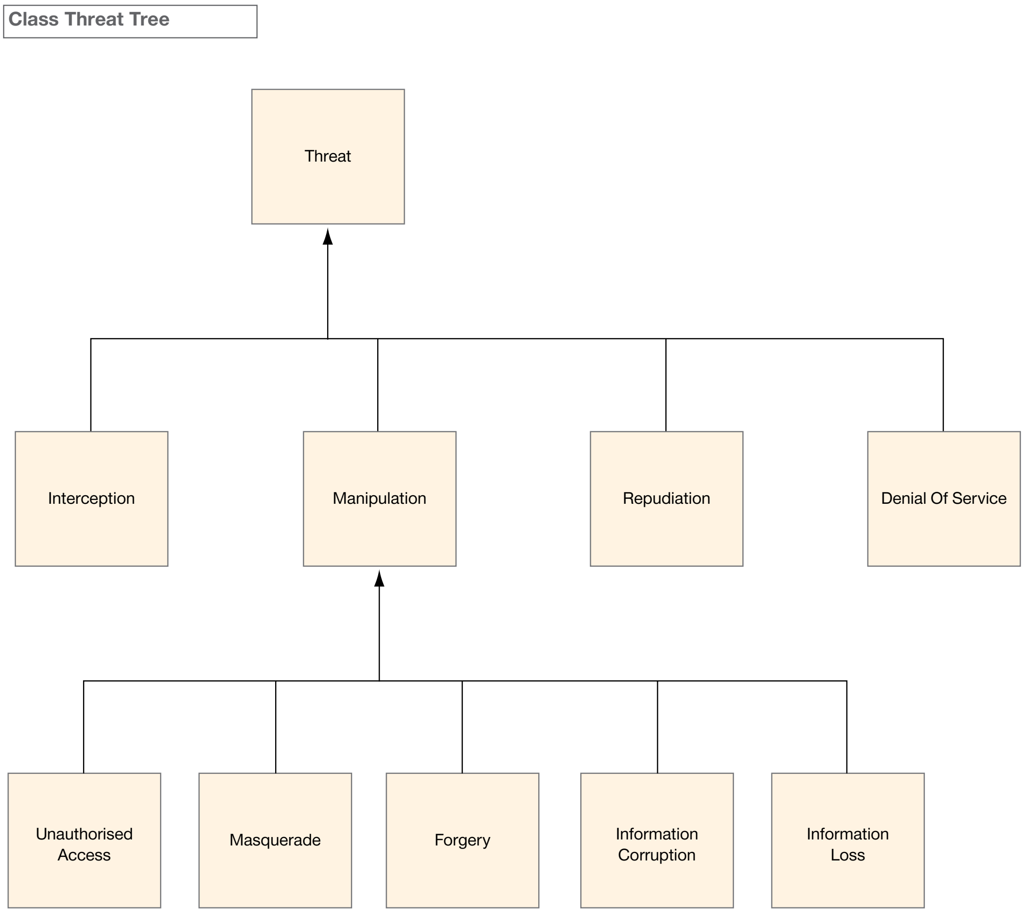
In many instances, a taxonomy is considered two-dimensional whereas ontologies are often considered as three-dimensional. A general model of attacker (as an instance of a threat stereotype) and victim (as an instance of an asset stereotype) is shown in figure 5.1, where the victim is vulnerable through an attack interface that is exploited by the attacker. A taxonomy or ontology of the role of resilience in attaining cyber security may then be developed.

Figure 5.1 – **Attacker – victim model for risk**



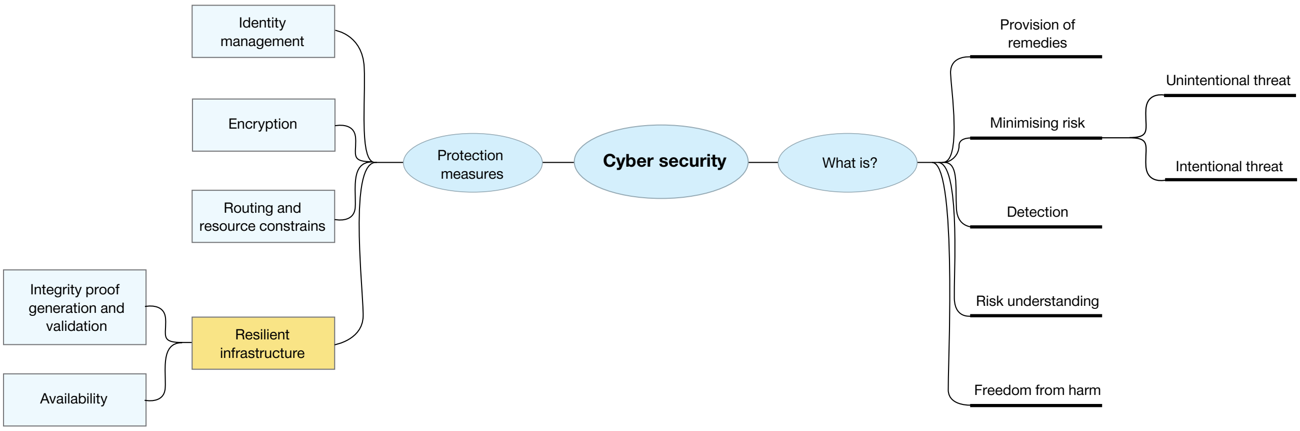
An alternative model for considering both ontologies and taxonomies is presented in figure 5.2, an illustration of a threat hierarchy. In each case, the hierarchy expresses the relation 'is a form of' (eg, forgery is a form of manipulation threat).

Figure 5.2 – **Hierarchy of threat types in generic systems**



The ITU-T and ETSI in TR 187 010 [5] have identified an ontology of cyber-security, which is illustrated in Figure 3.2 and simplified in Figure 5.3, where it has been revised slightly to show that 'resilient infrastructure' is one of the capabilities that enables protection. In this view, resilience is shown to include measures to assure both availability and network integrity.

Figure 5.3 – **Simplification of ITU-T ontological model of cyber security stressing resilience**

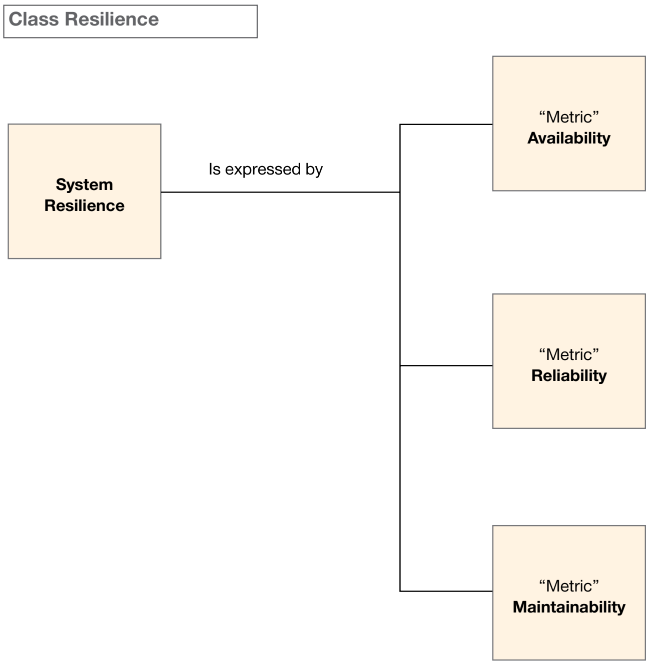


5.2 Metrics

5.2.1 Resilience metrics

In addition to taxonomies and ontologies for the assessment of cyber security, there is a need to develop metrics that allow an instantiation of a system to express its resilience. In this case, system resilience may be measured or expressed in terms of its metrics. This is illustrated in figure 5.4.

Figure 5.4 – **Metrics used to express system resilience**



Availability

In general, the *availability of a system as a function of time* [A(t)] can be defined as the probability that the system is operational at a particular instant of time [t]. If the limit of this function exists as t goes to infinity, it expresses the expected fraction of time that the system is available to perform useful computations.

ITU-T defines the IP service availability metric in chapter 7 of Recommendation Y.1540 [56]. It is based on the notion of IP packet loss ratio (IPLR), measured as a percentage of lost packets across an interval of time. If, during this time interval, the percentage loss is below a certain selected level then the service is described as 'available in this time slot', otherwise as 'unavailable'. Based on the availability results (yes/no) for consecutive time intervals, the document defines the percentage of (un)availability:

- Percent IP service unavailability (PIU) is:
  - the percentage of total scheduled IP service time (the percentage of Tav intervals) that is (are) categorized as unavailable using the IP service availability function.
- Percent IP service availability (PIA) is:
  - The percentage of total scheduled IP service time (the percentage of Tav intervals) that is (are) categorized as available using the IP service availability function: PIA = 100 – PIU.

IETF defines the *concept of connectivity* as a measure of the expected probability that one host can reach another and then as an attribute affecting the service availability. RFC 2678 [26] defines the metrics that allow the level of connectivity between two hosts A1 and A2 to be defined. It starts with the definition of an analytic metric, called Type-P-Instantaneous-Unidirectional-Connectivity, to define one-way connectivity at one single moment in time. This metric is extended to the notion of bi-directional connectivity (for one single moment in time), and later to connectivity within a certain period of time. Each metric delivers, as a result, a Boolean value which states whether the desired level of connectivity has been reached or not. A methodology for estimating the last defined metric, called Type-P1-P2-Interval-Temporal-Connectivity, is sketched in the document. This methodology expects randomly distributed start times for sending the probe packets within a selected interval of time. The document also shows how to apply this testing methodology for checking TCP-based connectivity.

Reliability

The *reliability of a system as a function of time* [R(t)] is the conditional probability that the system has survived the interval [0, t], given that the system was operational at time t = 0.

NOTE: Reliability in this context is used to describe systems in which repair cannot take place, eg, systems in which the computer is serving a critical function and cannot be lost even for the duration of a repair, or systems where the repair is prohibitively expensive.

The reliability function R(t) holds the following properties:

- It is a monotonically decreasing function.
- R(t=0)=1 (the component is assumed to work correctly in the beginning).
- R(t=TTF)=0 (the component will eventually fail).

Unreliability, probability of failure

Unreliability (also referred to as the probability of failure) [F(t)] is a property related to reliability by this law:

$R(t)+F(t)=1$

F(t) is the cumulative distribution function (CDF) of the time to fail (TTF) random variable and represents the probability that the system fails in the time interval (0,t). The parameter to be managed is the mean or expected value, the mean time between failures (MTBF).

Time to repair

Time to repair (TTR) is the amount of time needed to restore a system's correct service delivery after a failure has occurred. The parameter to be managed is the mean or expected value, the mean time to repair (MTTR).

Maintainability and maintenance

The *maintainability CDF* [M(t)] is defined as the probability of performing a successful repair action within a given time. In other words, maintainability measures the ease and speed with which a system can be restored after a failure has occurred, or whether a maintenance plan may extend the lifetime of a system by interceding at a point before the TFF to replace components and thus reset the TFF. For a maintenance plan to be effective the time to maintain should be less than TTR (including any time to analyse the cause of a fault and to identify the required repair).

NOTE: If a system fails, a time variable may be introduced to analyse the failure. It is sufficient to identify the required time for repair.

Coverage

The *coverage* [c] is the parameter that measures the fault tolerance effectiveness of a system. It is defined as the conditional probability that, given the existence of a failure in the operational system, the system is able to recover and continue information processing with no permanent loss of essential information, that is:

- c = Pr(system recovers | system fails).

5.2.2 Metrics in support of resilience

Delay

Delay is used to measure the expected time for an IP packet to traverse the network from one host to another. IETF RFC 2679 defines *delay* as follows: 'For a real number dT, the *Type-P-One-way-Delay* from Src to Dst at T is dT' means that Src sent the first bit of a Type-P packet to Dst at wire-time* T and that Dst received the last bit of that packet at wire-time T+dT.' The notion of wire time is used (compare RFC 2330 [23]) to take into consideration the additional delay introduced by the use of Internet hosts to make the measurements. Wire time is defined with reference to an Internet host H observing an Internet link L at a particular location. For a given packet P, the 'wire arrival time' of P at H on L is the time T at which the first bit of P has appeared at H's observation point on L. On the other hand, for a given packet P, the 'wire exit time' of P at H on L is the time T at which all the bits of P have appeared at H's observation point on L.

The ITU-T document Y.1540 [56] defines the *IP packet transfer delay* (IPTD) metric as 'the one-way IP packet transfer delay for all successful and erroneous packet transmissions across a basic section or a network section ensemble (NSE). IPTD is the time $(t_2 – t_1)$ between the occurrence of two corresponding IP packet reference events, ingress event $IPRE_1$ at time t_1 and egress event $IPRE_2$ at time t_2, where $(t_2 > t_1)$ and $(t_2 – t_1) \leq T_{max}$.'

The document defines an IP packet reference event as follows. An IP packet transfer event occurs when:

- an IP packet crosses a measurement point (MP);
- standard IP procedures applied to the packet verify that the header checksum is valid; and,
- the source and destination address fields within the IP packet header represent the IP addresses of the expected source host and destination host.

Delay variation

Delay variation is used to measure the variation in a sequence of delay values over time. In RFC3393 [28], the IP packet delay variation (IPDV) is presented as the difference between the one-way-delay of two consecutive packets from a stream of selected packets across Internet paths. The definition relies on the introduction of a selection function ***F*** defining unambiguously the two packets from the stream selected for the metric.

More precisely, RFC3393 defines the IP Packet Delay Variation from a source host to a destination host, for two packets selected by the selection function ***F*,** as the difference between the value of the one-way-delay from the source host to the destination host at time T2 and the value of the one-way-delay from the source host to the destination host at time T1. T1 is the wire arrival time at which the source host sent the first bit of the first packet, and T2 is the wire exit time at which the source host sent the first bit of the second packet.

ITU-T Recommendation Y.1540 defines an *end-to-end 2-point IP packet delay variation* as follows: 'The end-to-end 2-point packet delay variation (v_k) for an IP packet k between a source host and a destination host is the difference between the absolute IP packet transfer delay (x_k) of the packet and a defined reference IP packet transfer delay, $d_{1,2}$, between the same measurement points: $v_k = x_k – d_{1,2}$.'

The reference IP packet transfer delay, $d_{1,2}$, between the source host and the destination host can be the absolute IP packet transfer delay experienced by the first IP packet between the two measurement points or any other fixed packet delay.

Packet loss

Packet loss indicates the expected probability that a transmitted packet will get to its destination, and is usually expressed as a percentage.

IETF RFC2680 [27] provides the following definition for the *one-way-packet-loss metric*:

> The one-way-packet-loss of a type-P packet from a source host to a destination host is 0 if the source host sent the first bit of the type-P packet to the destination host at wire-time T and the destination host received that packet. The one-way-packet-loss of a type-P packet from a source host to a destination host is equal to 1 if the source host sent the first bit of the type-P packet to the destination host at wire-time T and the destination host did not receive that packet.

Recommendation Y.1540 defines the *IP packet loss ratio* (IPLR) as 'the ratio of total lost IP packet outcomes to total transmitted IP packets in a population of interest'.

5.3 Conclusion (taxonomy and metrics)

There is no consistent taxonomy for cyber security that identifies the role of resilience.

Existing standards in the field, as identified above, only address resilience indirectly and without a detailed definition of the role of resilience to the taxonomy and thus to the semantics of security. As metrics play a significant role in giving meaning to any comparison of system resilience, it is essential that metrics are normalised and promoted. This refers to the need to support the specification of metrics and the supporting test or validation criteria to be used in the assessment of resilience and, wherever possible, to do so from existing metrics used in assessing reliability and failure analysis.

NOTE: The values applied to the metrics may need to differentiate between acceptable values for operation in:

- emergency situations;
- non-emergency situations; and
- communication infrastructure supporting other critical infrastructure (eg, electrical supply, banking sector, etc).

6 Forms of attacks on network resilience

6 Forms of attacks on network resilience

NOTE: this section refers to the theory of network resilience and identifies basically the areas of interest for the SDOs.

6.1 Cyber attacks

A cyber attack is viewed as a malicious attack on a network using the computers, network elements and applications that are used to build up the network to attack the network. Whilst analyses of many forms of cyber attack are well documented, and whilst methods of analysis are well documented in standards, there is no direct link between standardised countermeasures and the reduction in network resilience caused by a combined cyber attack. However the metrics from ISO/IEC 15408 [44] and ETSI TS 102 165-1 [11] do describe attack intensity and its application in risk assessment but do relatively little in assessing the complex composite attacks often found in managed cyber attacks. This is an area where standards bodies should work to strengthen the metrics and calculations of system assurance of resilience.

The attack vectors used in launching a cyber attack that directly attempt to impact network resilience include the following:

- Internet social engineering attacks
- packet spoofing
- hijacking sessions
- automated probes and scans
- widespread denial-of-service attacks
- widespread attacks on DNS infrastructure
- wide-scale Trojan distribution.

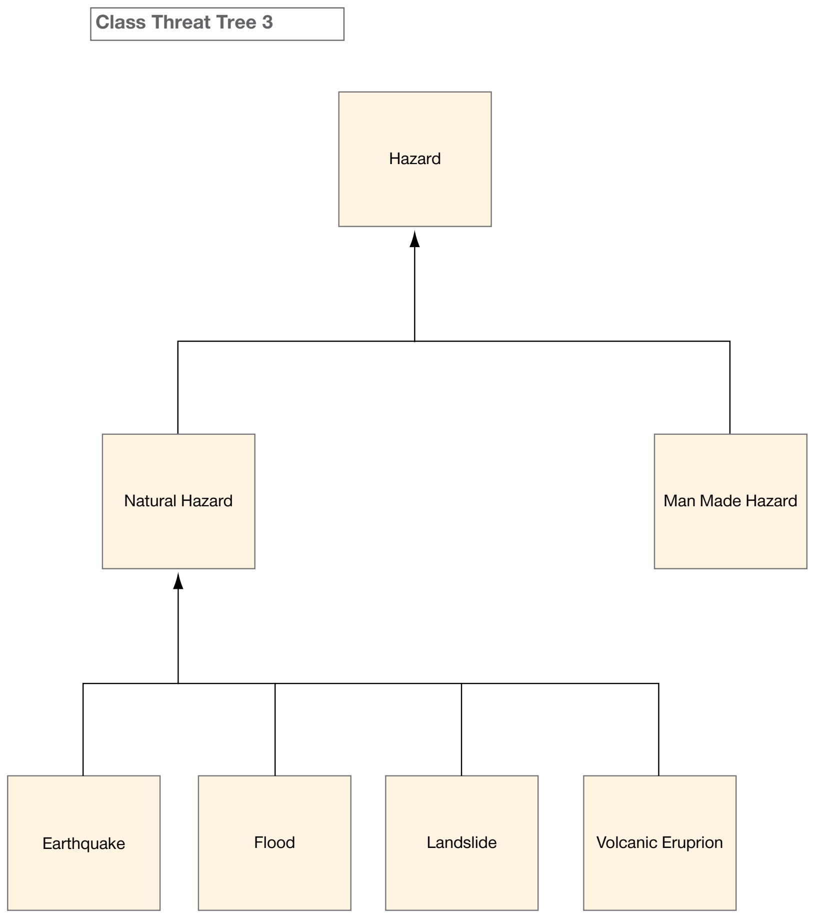
In any network where sensed data is analysed and propagated in order to make decisions, an attacker may introduce false but plausible data to force the system to make invalid decisions. Where the data is distributed without oversight by an independent analyst, eg, in an automated traffic management system, the impact may be sufficient to severely affect the function of day-to-day life. This may lead to such events as gridlock or loss of access to key resources.

In order to minimise attacks on resilience from cyber attack, data should be prevented from automatic propagation and from being the sole source of decision-making.

6.2 Natural disasters

A *natural disaster* is the effect of a natural hazard (eg, flood, volcanic eruption, earthquake, or landslide) that affects the environment and leads to financial, environmental and/or human losses. A number of international conventions and agreements have been endorsed (the Tampere Declaration of 1991; Resolution 7 of the 1994 World Telecommunication Development Conference; Resolution 36 of the 1994 ITU Plenipotentiary Conference). The main impact on network resilience is to ensure that the obligations on SDOs arising from these agreements have been met. The current status of work in the SDOs is that there is no traceability from the SDOs to these agreements.

Figure 6.4 — **Hierarchical taxonomy of Hazards**



6.3 Flash crowd events

A *flash mob* or *flash crowd event* is a large group of people who assemble suddenly in a public place, perform an unusual action for a brief time, and then quickly disperse. The term *flash mob* is generally applied only to gatherings organized via telecommunications, social media, or viral emails. The term is generally not applied to events organized by public relations firms or as publicity stunts. One consequence not foreseen by the builders of the Internet was that, with the almost instantaneous reporting of newsworthy events, tens of thousands of people worldwide — along with criminals — would flock to the scene of anything interesting, hoping to experience or exploit the instant disorder and confusion so created.

In a number of fields where telecommunication technology is being introduced, eg, in intelligent transport systems (ITS), a flash event may lead to cyber attack. This is possible as the localised concentration of active devices gives rise to a high likelihood of a localised denial of service attack. The role of standards in recognising flash events is important and the likelihood and impact of such attacks should be considered in calculations for the analysis of system risk. Means to mitigate such attacks need to be explored, and standards-based solutions to protect system integrity (one factor of system resilience) and system availability (one factor of system resilience) should be defined.

NOTE: Flash crowd events are distinguished from those regular crowd events where planning can be used to prevent an attack on system resilience; examples include large sporting events where tens of thousands of spectators congregate in a single location for a period of a few hours and for which the network should be designed.

6.4 Logical failures

Electronic equipment can logically fail at some point in its life because of programming mistakes, misconfiguration or the use of inappropriate software. Whilst this may be difficult to distinguish from an attack, the use of metrics as outlined in section 5 will allow the designer to address failure in the design of a resilient network.

6.5 Outages to other equipment affecting the network

Resilience of telecommunication networks depends also on equipment that is not specifically designed to transmit data, such as power supplies, cooling systems, etc. Similarly to logical failures, outages to this equipment, although not directly related to networks, affect the communication services.

6.6 Conclusions drawn from review of forms of attack on network resilience

The following conclusions and recommendations are outlined:

- Standards bodies should work to strengthen the metrics used in determining system assurance of resilience and to popularise their application.
- A link from provisions to assist in the mitigation of natural disaster in the output of SDOs should be documented.
- Means to mitigate flash mob attacks need to be explored, and standards-based solutions to protect system integrity (one factor of system resilience) and system availability (one factor of system resilience) should be defined.
- In order to minimise attacks on resilience from cyber attack, data should be prevented from automatic propagation and from being the sole source of decision-making.

7 Standards supporting the resilience model derived from regulation (ECN&S model)

7 Standards supporting the resilience model derived from regulation (ECN&S model)

NOTE: This extends the model introduced in section 2 and identifies some approaches to providing resilience. The examples are not exhaustive but are intended to give a review of those mechanisms considered in existing standards work that may be of use.

7.1 Transport mechanisms

There are a large number of approaches to provide resilience in the transport network (mapped to the ECN entity of the ECN&S paradigm). The requirements for network resilience aim to give assurance of the following attributes:

- network availability
- network integrity
- redundancy.

7.1.1 Means to mediate quality of service or grade of service in a network

NOTE: QoS and GoS are considered here as means to determine the degree of resilience provided to the user as a measure of the network's ability to deliver a service with a predictable level of performance (ie, time taken to establish a connection, time taken to transfer a data item, level of loss of data across a set of data items). QoS and GoS together assist in addressing availability and integrity of the core network and may indicate methods for providing redundancy to improve resilience.

Integrated services (IntServ)

IntServ is a QoS control framework that provides network applications with means to support QoS built on the assumption that network resources (eg, bandwidth) must be explicitly managed in order to meet application requirements.

Two different IntServ service classes have been defined: guaranteed quality of service and controlled load quality of service. The first one comes as close as possible to emulating a dedicated virtual circuit. It provides firm (mathematically provable) bounds on end-to-end queuing delays by combining the parameters from the various network elements in a path, in addition to ensuring bandwidth availability according to the traffic specification made by the sender. Controlled load quality of service is equivalent to 'best effort service under unloaded conditions'. Hence, it is 'better than best-effort', but cannot provide the strictly bounded service that guaranteed service promises.

RSVP (Resource ReserVation Protocol)

A reservation setup protocol, called RSVP (Resource ReserVation Protocol) [34], is used to create and manage state information along the whole path that a specific flow crosses between two network end-points. One of the features required of such a protocol is that of carrying the so-called flowspec object, ie, a list of parameters specifying the desired QoS needed by an application. At each intermediate network element along a specified path, this object is passed to admission control to test for acceptability and, in the case that the request is satisfied, used to appropriately parameterize the packet scheduler.

Differentiated services (Diffserv)

Diffserv is based upon a much simpler model than IntServ, where traffic entering the network is subjected to a conditioning process at the network edges and then assigned to one of several different behaviour aggregates, identified by means of a single DS codepoint. Furthermore, each DS codepoint is assigned a different per-hop behaviour, which determines the way packets are treated in the core of the network. Thus, differentiated services are achieved through the appropriate combination of traffic conditioning and per-hop behaviour forwarding.

DiffServ assumes the existence of a service level agreement (SLA) between networks that share a border. The SLA establishes the policy criteria and defines the traffic profile. It is expected that traffic will be policed and smoothed at egress points according to the SLA, and that any traffic 'out of profile' at an ingress point shall be treated according to the default condition of the network.

Multi Protocol Label Switching (MPLS) mechanisms

This was addressed in the ENISA study *Resilience Features of IPv6, DNSSEC and MPLS and Deployment Scenarios* [2] and is not discussed further in this report.

7.1.2 Core network protocol

IPv6

This was addressed in the ENISA study *Resilience Features of IPv6, DNSSEC and MPLS and Deployment Scenarios* [2] and is not discussed further in this report.

7.1.3 Means to mediate routing and discovery in a network

Domain Name System (DNS)

The Domain Name System (DNS) is one of the cornerstones in the architecture of the Internet. It is a distributed database based upon a hierarchical naming system for machines, services or any other kind of resources. Its main purpose is the resolution of (human-readable and -memorable) domain names into IP addresses. In addition, it provides the resolution of domain names into other kinds of resources, eg, into other domain names or uniform resource identifiers (URIs). The structure and architecture of the DNS is based upon the following main four components: the domain name space which follows a tree-based structure in order to build up domain names; the name servers that publish information about specific domains or sub-domains; the resolvers that are the software modules at the client side; and the DNS protocol.

E.164 NUmber Mapping (ENUM)

ENUM, the E.164 (ITU-T recommendation on the telecommunication numbering plan) NUmber Mapping, is an application of the domain name system (DNS) to map telephone numbers to uniform resource identifiers (URIs). Its target is that a subscriber can be available under the same phone number over the conventional telephone network as well as over the Internet. The mechanism of translation is that a phone number is transformed into a corresponding *fully qualified domain name (*FQDN) under the ENUM specific zone (with the suffix 'e164.arpa'). A DNS resource record for such a derived DNS-name contains one or more pointers to one or more URIs for contacting the subscriber, eg, the URIs can be a SIP- and a mailto-URI. ENUM is specified in RFC 3761[30].

DNS security (DNSSEC)

This was addressed in the ENISA study *Resilience Features of IPv6, DNSSEC and MPLS and Deployment Scenarios* [2] and is not discussed further in this report.

Secure Border Gateway Protocol (S-BGP)

Attacks at the border of a network impact the reachability of entities inside the network. The Secure Border Gateway Protocol (S-BGP) is a class of routing security approaches that provide countermeasures to the vulnerabilities affecting the BGP and thus may improve the resilience of networks by minimising risk to a network.

7.2 Architecture specific mechanisms

NOTE: the subsections below are mostly based on ETSI-TR-102445.

7.2.1 Radio access networks

Redundancy in the radio access network (RAN)

The radio access network itself can offer redundancy in a number of ways:

- overlapping coverage from multiple cell sites in the same area;

NOTE: This is more likely to be found in 2G systems but is also a requirement of CDMA 3G systems (also known as a hierarchical cell structure).

- redundancy of components on cell sites (eg, transceivers, site controllers, antennas, etc);
- redundancy of power supply capability, including battery and generator powered supplies;
- fallback strategies to allow stand-alone operation of sites disconnected from switching sites; in this case trunked communications are possible between terminals connected to the same site.

NOTE: The notion of 'hierarchical cell structure' is part of the 3G specifications (IMT-2000) and allows a geographical cell coverage area to be managed by a network of overlapping cells (ranging from pico- to macro-cells).

Radio access network availability is highly dependent on the topology of the transmission network supporting the cell sites and by the availability of the core network switching components. The availability of the radio access network can be enhanced by:

- use of multiple transmission links to sites using various topologies including redundant stars and rings;
- configuration of the network such that adjacent sites are connected to different switches: loss of a switch will still allow remaining sites to provide a reduced coverage across the served area if enough overlap in coverage is provided between the cell sites.

In areas where there is insufficient coverage overlap between sites, cell sites typically employ a means of providing communications in the event of network faults that isolate the sites from their switching centres. Where older analogue systems are in place, this communication is achieved, typically, by forcing the site to perform a stand-alone repeater system, whereby the base station transmitter relays all received transmissions and different users will typically share the same channels.

Resilience in the radio access network (RAN)

In addition to the mechanisms employed to provide protection against failures in the radio access network, mechanisms are also employed to provide resilience against interference, both deliberate and accidental.

The strongest protection against deliberate eavesdropping is the use of air interface encryption, often together with an authentication process, which protects signalling and traffic from eavesdropping and also makes it difficult for an attacker to manipulate the air interface by replaying valid traffic or introducing interfering traffic. The encryption process can also be maintained during stand-alone operation of a cell site.

Networks can also provide protection against accidental interference by monitoring the quality of the signal link between cell site and mobile device, and assigning different frequencies where interference occurs on a frequency in use. A number of techniques in data encoding and in receivers may also improve the resilience or reliability of the radio link and thus contribute to overall system resilience.

7.2.2 Core transmission networks

Resilience in the transmission network

The transmission network (also termed ground based network in PSRNs) is usually composed of a number of technologies including:

- copper based landlines
- optical fibre networks
- microwave links.

Redundancy can be applied at a link level duplication of equipment supporting a single link, eg, duplicate microwave transceivers, and duplications of the links themselves. Where links are duplicated, the physical separation of routes (separacy) is generally employed to protect against a single physical event interrupting main and backup paths (eg, severing of cables by digging machinery).

Redundancy can be applied at the network level, whereby the network is designed with multiple node-to-node links in a mesh configuration, and paths between pairs of nodes can carry traffic between other more distant nodes. Loss of a link or node causes the network to automatically reroute traffic through different nodes and links (diverse routing). This approach is more common with systems employing packet switching techniques, such as IP.

Resilience in the switching network

Switching sites are typically constructed using redundant or highly resilient components. The following techniques can be used within a switching site:

- duplication of system databases, both within a site and between sites, to ensure resilience of user and system configuration;
- duplication of switching intelligence to ensure mobility and call control functions are maintained in the event of failures;
- duplication of switching components or, more recently adoption of more resilient distributed approaches, typically based on an IP, with redundant routing components;
- redundant local area networks connecting switching components;
- redundancy in network interfaces connecting each switching site with other switching sites and with cell sites
- duplication of power supplies with the use of uninterruptible power supplies and back-up options using batteries and generators.

In addition, duplicate switching sites can be used, such that a single switching site may be configured and switched into the place of any failed switching site, or multiple switching sites may be employed up to the point where in which each primary switching site is duplicated. Duplication of switching sites takes place across multiple geographic locations to increase resilience in the event of loss through disaster.

Representational state transfer (REST)

Representational state transfer (REST) refers to a variant of client-server architecture for distributed hypermedia systems. The concept of REST is of a request-response dialogue between the client and server, where the state of the interaction is not held on the server but forms a client side only state machine whose current state is communicated to the server with each request. Adoption of REST models may impact the required resilience of the core network as the network is no longer required to maintain state for each connection but the same state is instead maintained in the end point. Detail analysis of such modes for highly interactive services or for unattended services (eg, service forwarding), is required.

NOTE: The design of the Hypertext Transfer Protocol (HTTP) was based on REST principles.

7.3 Content layer

7.3.1 Requirements

Resilience on the content layer is required to guarantee the following targets:

- production and provision of content without interruption, serious delay and compromise of integrity at the side or servers of the content provider(s);
- consummation and display or representation without interruption, serious delay and compromise of integrity at the site of the content provider(s).

The requirements concerning resilience on the content layer can be derived mainly from the specifications and/or explanations established in chapter 4.

The requirements are the following:

- business continuity management
- fault-tolerance concepts
- disaster recovery (DR) concepts
- availability of content
- integrity
- authenticity
- authorization information: 'resilient' authorization mechanisms should guarantee uninterrupted access to resources for qualified users.

7.3.2 Content provision and related resilience standards

Service oriented architecture

CEN CWA 15537 *Network Enabled Abilities - Service-Oriented Architecture for civilian and military crisis management* [1] identifies mechanisms to make more efficient use of multi-national resources in the command and control of future European network centric operations in times of crisis. The CWA specifies services and other items, mandatory or optional, for a 'network enabled abilities' environment. It also includes an inventory of standards and standard-like specifications applicable to each such item. These items include recommended general principles and a framework for system design, overall architectures, generic functionality to be considered, concepts, conventions and terminology in order to ensure an optimum multi-purpose interoperability.

NOTE: The term 'network enabled abilities' is considered a synonym for 'network centric operations' or 'network enabled capabilities'.

Application space

Malware-free content

The malware-freeness of content is a key necessity in order to provide a correct processing or display of content on the user's device. The following standardization activities have been identified concerning this issue:

metadata for the exchange of information about malware: work is being done by the Malware Working Group of Industry Connections Security Group (ICSG) which is itself a subgroup of the Institute of Electrical and Electronics Engineers (IEEE) Standards Association;

testing standards for testing security products in order to provide a malware-free content on the user's device.

Business continuity management

In order to assure a steady, continuous and therefore resilient provision of content to the users, the security risks at the site(s) of the content provider have to be assessed and the necessary measures taken accordingly.

File formats

There exist a wide variety of media-formats for delivering content as audio, still images, animation, video and as combinations of these kinds of content. In many instances, file coding schemes are designed to be robust in the presence of bit or message error (where message refers to a discrete packet of data from the overall file). An appropriate choice of coding scheme may provide greater resilience in the presence of errors in the transmission path or may allow transmission of a reasonable facsimile of content where bandwidth is constrained.

NOTE: Encoding schemes (either loss-likely or lossless) provide an approximation of the content to be transmitted by compression but may remain intolerant of transmission loss. For highly resilient transmission the encoding scheme may have to be tolerant (including recoverable) of transmission loss and not just maximise the efficiency of transmission (by compression).

7.4 Conclusion

The following conclusion can be drawn from the discussion in this chapter:

- Although considerable standardization work has been performed concerning some specific aspects of resilience on the content level, eg, concerning business continuity management, resilience is not addressed specifically by SDOs and the topic is not treated with an approach that provides full coverage. As examples:
  - Resilience as a goal of standards has not been declared as being within the scope of SDOs.
  - The specific standards that may give support to resilience do not acknowledge this role.
  - SDOs have not prepared specific guidelines for using standards to provide system resilience (eg, there is no guide to providing resilience in 3G-UMTS networks).

8 Standards supporting resilience model derived from security analysis

8 Standards supporting resilience model derived from security analysis

8.1 Overview

Resilience is not directly addressed in existing security standardisation but may be seen as a requirement derived from provisions of the CIA (confidentiality, integrity, availability) paradigm.

NOTE: The CIA paradigm has been variously extended to cover accountability, authenticity, and authority but these extensions are covered by the more general use of the term availability.

8.2 Recommendations

The first and most straightforward recommendation is to promote the concept of resilience as a goal of security standardisation and thus make resilience explicit rather than implicit. This may be achieved, in the first instance, by introducing resilience as a keyword in the classification of standards (eg, the keyword list used by ETSI for classifying work items at http://webapp.etsi.org/ContextHelp/WorkProgram_help.asp?type=CODES_KEYWORDS).

A second recommendation is to add resilience as a matter to be considered by SDOs when approving work items. This should put considerations of resilience on a peer with the testing and verification requirements used in ETSI standardisation, for example.

9 Economics

9 Economics

9.1 Overview

Any countermeasure added to a system will add to the cost of the system and there has to be a reasonable balance between the cost of a countermeasure and the cost and likelihood of the occurrence of an incident. The threat analysis methods used in standards from ETSI (in TS 102 165-1[11]), in Common Criteria (ISO/IEC 15408 [44]), and in other sources (eg, AS/NZS 4360 [52]) almost universally address risk and risk reduction by identifying the impact on a system. The metric for impact (taken from ETSI TS 102 165-1 and thus stated in terms applicable to communications technology) is given in table 9.1 and applies to an asset of the system or to the system as a whole:

Figure 9.1 – **Impact**

Value	Impact	Explanation
1	Low	The concerned party is not harmed very badly; the possible damage is low.
2	Medium	The threat addresses the interests of providers or subscribers and cannot be neglected.
3	High	A basis of business is threatened and severe damage might occur in this context.

Whilst it may seem intuitive, in most methods of analysis it is considered that the provision of resilience and reliability against any attack with medium or high impact must be balanced by the likelihood of the attack.

The economics of providing countermeasures to reduce risk are not straightforward and whilst they depend on a risk model to identify how susceptible the system and its assets are to attack, one also has to consider the resultant cost to the market. In some cases money has to be spent, even if the technical risk is negligible, as other factors come into play; these include market perception, competitor behaviour and insurance against market evolution.

9.2 Financial evaluation of threats

NOTE: The evaluation metrics in this section are not covered in the metrics section as they do not directly impact resilience.

As identified in TS 102 165-1 [11] and in Common Criteria [44], there are metrics for the evaluation of the likelihood of a threat. These take account of a number of factors as listed below.

Knowledge factor

- Knowledge of the asset refers to specific expertise in relation to the asset. This is distinct from generic expertise, but not unrelated to it. Identified levels are as follows:
  - **public** information concerning the asset (eg, as gained from the Internet);
  - **restricted** information concerning the asset (eg, knowledge that is controlled within the developer organization and shared with other organizations under a non-disclosure agreement);
  - **sensitive** information about the asset (eg, knowledge that is shared between discrete teams within the developer organization, access to which is constrained only to members of the specified teams);

  - **critical** information about the asset (eg, knowledge that is known by only a few individuals, access to which is very tightly controlled on a strict need-to-know basis and individual undertakings).

Time factor

- The role of time in evaluating the likelihood of an attack requires evaluation of the total amount of time taken by an attacker to identify that a particular, potential weakness may exist, then to develop an attack method (threat agent) and to sustain the effort required to mount the attack. When considering this factor, the worst case scenario should be used to estimate the amount of time required.
  - Within **minutes** means an attack can be identified or exploited in less than an hour.
  - Within **hours** means an attack can succeed in less than a day.
  - Within **days** means an attack can succeed in less than a week.
  - Within **weeks** means an attack can succeed in less than a month.
  - In **months** means a successful attack requires in excess of a month.

Expertise factor

- Specialist expertise refers to the level of generic knowledge of the underlying principles, product type or attack methods (eg, Internet protocols, UNIX operating systems, and buffer overflows). The levels of expertise to be applied within this factor are defined as below:
  - **Laymen** are not knowledgeable compared to experts or proficient persons, with no particular expertise.
  - **Proficient** persons are knowledgeable in that they are familiar with the security behaviour of the product or system type.
  - **Experts** are familiar with the underlying algorithms, protocols, hardware, structures, security behaviour, principles and concepts of security employed, techniques and tools for the definition of new attacks, cryptography, classical attacks for the product type, attack methods, etc, implemented in the product or system type.

Opportunity factor

- Opportunity is also an important consideration, and it has a relationship to the elapsed time factor. Identification or exploitation of a vulnerability may require considerable amounts of access to an asset, which may increase the likelihood of detection. Some attack methods may require considerable effort off-line and only brief access to the asset to exploit. Access may also need to be continuous or spread over a number of sessions.
  - **Unnecessary or unlimited** access means that the attack does not need any kind of opportunity to be realized.
  - **Easy** means that access is required for less than a day or that the number of asset samples required to perform the attack is less than ten.
  - **Moderate** means that access is required for less than a month or that the number of asset samples required to perform the attack is less than fifty.
  - **Difficult** means that access is required for at least a month or that the number of asset samples required to perform the attack is less than one hundred.
  - **None** means that the opportunity window is not sufficient to perform the attack (the length of time for which the asset to be exploited is available or is sensitive is less than the opportunity time needed to perform the attack, eg, if the asset key is changed each week and the attack requires two weeks).

Equipment factor

- IT hardware, software or other equipment refers to the equipment required to identify or exploit a vulnerability.
  - **Standard** equipment is readily available to the attacker, either for the identification of a vulnerability or for an attack. This equipment may be a part of the asset itself (eg, a debugger in an operating system) or can be readily obtained (eg, Internet downloads, protocol analyser or simple attack scripts).
  - **Specialized** equipment is not readily available to the attacker but could be acquired without undue effort. This could include the purchase of moderate amounts of equipment (eg, power analysis tools; use of hundreds of PCs linked across the Internet would fall into this category) or the development of more extensive attack scripts or programs.
  - **Bespoke** equipment is not readily available to the public as it may need to be specially produced (eg, very sophisticated software) or because the equipment is so specialized that its distribution is controlled, possibly even restricted. Alternatively, the equipment may be very expensive.

Intensity factor

- The intensity of an attack may be modified by use of:
  - distributed threat agents (many sources of attack);
  - reduced the time interval between attacks; or,
  - a combination these two.

9.3 Recommendations

The tools for risk analysis should be extended to cover cost: benefit analysis.

NOTE: It is understood this is an active area of work in ETSI TISPAN as they seek to update TS 102 165-1.

10 Overall conclusions

10 Overall conclusions

The analysis at the core of this document identifies the fact that resilience is not currently being addressed by the key standards developing organizations (SDOs) other than as guidance for management processes.

#1 Work items should be actively promoted in the SDOs to support the specification of metrics and supporting test and validation criteria to be used in the assessment of resilience (derived, where possible, from existing metrics used in the assessment of reliability and failure analysis).

#2 Work items should be actively promoted in the SDOs to support development of a taxonomy for resilience.

#3 As a very large part of system resilience is enabled by features and capabilities not covered by the conventional telecommunications SDOs, those SDOs should be encouraged to build links from their work to the output of bodies dealing with those ancillary features (eg. power, heat, light, flood control, environmental control, and access, ie, transport links to get maintenance staff to site for repairs).

#4 Add 'resilience' as a 'keyword' in classifying standards in the SDOs.

#5 Update the procedures of SDOs in approving work items to address how resilience will be achieved, eg, if the system implemented using the present document fails, how will the system be maintained (ie, what measures are offered in support of resilience by this standardisation effort).

Although considerable standardization work has been performed concerning some specific aspects of resilience, eg, concerning business continuity management, resilience is not addressed specifically by SDOs and the topic is not treated by an approach that provides full coverage. For example:

- Resilience as a goal of standards is not declared in the scope of SDOs.
- The specific standards that may give support to resilience do not acknowledge this role.
- SDOs have not prepared specific guidelines for using standards to provide system resilience (eg, there is no guide to providing resilience in 3G-UMTS networks).

Annex A: Standardisation activities considered in this study

Annex A: Standardisation activities considered in this study

A.1 Review of contributing standards bodies

The key standards bodies examined for the purpose of this report are as follows:

ETSI (European Telecommunications Standards Institute)

ETSI is the recognized regional standards body dealing with telecommunications, broadcasting and other electronic communications networks and services. ETSI produces standards and specifications supporting EU and EFTA policy issues such as the New Approach, other EU legislation (eg, Electronic Fee Collection, the interoperability regulation under the Single European Sky (SES) initiative, the Electronic Communication Network and Services Framework Directives), mandated activity and other EU initiatives (eg, eEurope and i2010).

In the area of security ETSI is active in cryptographic algorithm development, protocol development and testing, as well as in the development of methods for developing security standards and metrics.

CEN (European Committee for Standardization)

CEN is the European Committee for Standardization; its main fields of activity cover various sectors such as air and space, chemistry, construction, consumer products, energy and utilities, food, health and safety, healthcare, heating, cooling, ventilation, ICT, materials, measurement, mechanical engineering, nanotechnology, security and defence, services, transport and packaging, among others.

CENELEC (European Committee for Electro-technical Standardization)

Its main field of activity covers the electro-technical domain.

ISO (International Organisation for Standardisation)

ISO is a network of the national standards institutes of 162 countries, one member per country, with a central secretariat in Geneva, Switzerland, that coordinates the system. ISO is a non-governmental organization that forms a bridge between the public and private sectors. On the one hand, many of its member institutes are part of the governmental structure of their countries or are mandated by their government. On the other hand, other members have their roots uniquely in the private sector, having been set up by national partnerships of industry associations.

ITU-T (International Telecommunication Union - Telecommunication Standardization Sector)

ITU is the leading United Nations agency for information and communication technology issues, and the global focal point for governments and the private sector in developing networks and services.

IETF *(Internet Engineering Task Force)*

The IETF is the protocol engineering and development arm of the Internet which is governed as one of five bodies in the development of the Internet (the other four bodies are listed below):

- The Internet Architecture Board (IAB) is responsible for defining the overall architecture of the Internet, providing guidance and broad direction to the IETF. The IAB also serves as the technology advisory group to the Internet Society, and oversees a number of critical activities in support of the Internet.
- The Internet Assigned Numbers Authority (IANA), based at ICANN, is in charge of all 'unique parameters' on the Internet, including IP (Internet Protocol) addresses. Each Internet host is associated with a unique IP address, a numerical name consisting of four blocks of up to three digits each, eg, 204.146.46.8, which systems use to direct information through the network.

- The Internet Engineering Steering Group (IESG) is responsible for the technical management of IETF activities and the Internet standards process. As part of the ISOC, it administers the process according to the rules and procedures which have been ratified by the ISOC Trustees. The IESG is directly responsible for the actions associated with entry into and movement along the Internet 'standards track', including final approval of specifications as Internet Standards.
- The Internet Society (ISOC) is a professional membership organization of Internet experts that comments on policies and practices and oversees a number of other boards and task forces dealing with network policy issues.

A.2 CEN

[1] CEN CWA 15537: *Network Enabled Abilities - Service-Oriented Architecture for civilian and military crisis management*, 2006.
ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/NEA/cwa15537-00-2006-Apr.pdf

A.3 ENISA

[2] ENISA: Stock Taking Report on the Technologies Enhancing Resilience of Public Communication Networks in the EU Member States, 2009. http://www.enisa.europa.eu/act/it/library/deliverables/stock-tech-res/

[3] ENISA study: Resilience Features of IPv6, DNSSEC and MPLS and Deployment Scenarios, 2008. http://www.enisa.europa.eu/act/it/library/deliverables/res-feat

A.4 ETSI

NOTE: All ETSI documents are available for download at http://pda.etsi.org/pda/ for registered users.

[4] ETSI EG 202 387: *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN): Security Design Guide: Method for application of Common Criteria to ETSI deliverables*.

[5] ETSI TR 187 010: *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN): NGN Security: Report on issues related to security in identity management and their resolution in the NGN*

[6] ETSI TR 102 445: *Emergency Communications (EMTEL): Overview of Emergency Communications Network Resilience and Preparedness*

[7] ETSI ES 202 383: *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN): Security Design Guide: Method and pro-forma for defining Security Targets*

[8] ETSI ES 202 382: *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN): Security Design Guide: Method and pro-forma for defining Protection Profiles*

[9] ETSI ES 282 004: *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN): NGN Functional Architecture: Network Attachment Subsystem*

[10] ETSI ETR 332 (1996): *Security Techniques Advisory Group (STAG): Security requirements capture*

[11] ETSI TS 102 165-1 (2006) *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN): Methods and protocols: Part 1: Method and pro-forma for Threat, Risk, Vulnerability Analysis*

[12] ETSI TS 102 165-2 (2006) *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN): Methods and protocols: Part 2: Protocol Framework Definition: Security Counter Measures*

[13] ETSI TR 102 055: *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN): ENUM scenarios for user and infrastructure ENUM*

[14] ETSI TR 102 420: *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN): Review of activity on security*

[15] ETSI TS 187 001: *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN): NGN SECurity (SEC): Requirements*

[16] ETSI TS 101 903: *XML Advanced Electronic Signatures (XAdES)*

A.5 EU

[17] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002: A common regulatory framework for electronic communications networks and services (Framework Directive)
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:108:0033:0050:EN:PDF

[18] Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002: Access to, and interconnection of, electronic communications networks and associated facilities (Access Directive).
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:108:0007:0020:EN:PDF

[19] Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002: The authorization of electronic communications networks and services (Authorization Directive).
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:108:0021:0032:EN:PDF

[20] Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002: Universal service and users' rights relating to electronic communications networks and services (Universal Service Directive).
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:108:0051:0077:EN:PDF

[21] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002: The processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:EN:PDF

A.6 IETF

NOTE: All IETF RFCs are available at http://tools.ietf.org/html/

[22] IETF RFC 1157: *A Simple Network Management Protocol (SNMP)*

[23] IETF RFC 2330: *Framework for IP Performance Met*

[24] IETF RFC 2535: *Domain Name System Security Extensions*

[25] IETF RFC 2616: *Hypertext Transfer Protocol -- HTTP/1.1*

[26] IETF RFC 2678: *IPPM Metrics for Measuring Connectivity*

[27] IETF RFC 2680: *A One-way Packet Loss Metric for IPPM*

[28] IETF RFC 3393: *IP Packet Delay Variation Metric for IP Performance Metrics (IPPM)*

[29] IETF RFC 3414: *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*

[30] IETF RFC 3761: *The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)*

[31] IETF RFC 3403: *Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database*

[32] IETF RFC 2915: *The Naming Authority Pointer (NAPTR) DNS Resource Record*

[33] IETF RFC 1633: *Integrated Services in the Internet Architecture: an Overview'*

[34] IETF RFC 2205: *Resource ReSerVation Protocol (RSVP) - Version 1 Functional Specification*

[35] IETF RFC 2475: *An Architecture for Differentiated Services*

[36] IETF RFC 2598: *An Expedited Forwarding PHB*

[37] IETF RFC 2597: *Assured Forwarding PHB Group*

[38] Draft-ietf-dnsext-dnssec-protocol-06 (2004): *Protocol Modifications for the DNS Security Extensions*

[39] Draft-ietf-dnsext-dnssec-records-08 (2004): *Resource Records for DNS Security Extensions*

[40] Draft-ietf-dnsext-dnssec-intro-11 (2004): *DNS Security Introduction and Requirements*

A.7 ISO/IEC

[41] ISO/IEC 15408-1: *Information technology - Security techniques: Evaluation criteria for IT security - Part 1: Introduction and general model*

[42] ISO/IEC 15408-2: *Information technology - Security techniques: Evaluation criteria for IT security - Part 2: Security functional requirements*

[43] ISO/IEC 15408-3: *Information technology - Security techniques: Evaluation criteria for IT security - Part 3: Security assurance requirements*

[44] ISO/IEC 15408: *Information technology - Security techniques: Evaluation criteria for IT security*

NOTE: When referring to all parts of ISO/IEC 15408 the reference above is used.

[45] ISO/IEC 13335: *Information technology - Security techniques: Guidelines for the management of IT security*

NOTE: ISO/IEC 13335 is a multipart publication and the reference above is used to refer to the series.

[46] ISO/IEC 27001 2005: *Information Technology - Security Techniques: Information Security Management Systems - Requirements*

[47] ISO/IEC 27002 2005: *Information technology - Security techniques: Code of practice for information security management*

[48] ISO/IEC 17799 2005: *Information technology - Security techniques: Code of practice for information security management*

A.8 Others

[49] UK Home Office; R V Clark: *Hot Products: understanding, anticipating and reducing demand for stolen goods*; ISBN 1-84082-278-3

[50] *Common Methodology for Information Technology Security Evaluation: Evaluation methodology,* July 2005, Version 3.0 Revision 2 (CCMB-2005-07-004)

[51] *Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model*, June 2005, Version 3.0 Revision 2 (CCMB-2005-07-001)

[52] AS/NZS 4360: *Standards Australian, Risk Management*

[53] ASIS SPC.1-2009: *Organizational Resilience: Security, Preparedness and Continuity Management Systems— Requirements with Guidance for Use*

[54] Object Management Group: *UML 2.0 Superstructure Specification*, document: ptc/ 04-10-02 edition, 2004

[55] BS 25999: *The British Standard for Business Continuity Management*

[56] ITU-T Recommendation Y.1540: Internet protocol aspects – Quality of service and network performance, 2007. http://www.itu.int/rec/T-REC-Y.1540-200711-I

Annex B: Definitions

Annex B: Definitions

asset: anything that has value to the organization, its business operations and its continuity

authentication: ensuring that the identity of a subject or resource is the one claimed

availability: property of being accessible and usable on demand by an authorized entity ISO/IEC 13335-1 [45]; for a broader description see section 5.2.1

confidentiality: ensuring that information is accessible only to those authorized to have access

CRAVED (concealable, removable, available, valuable, enjoyable, and disposable): acronym for a classification scheme to determine the likelihood that a particular type of item will be the subject of theft [49]

identifier: series of digits, characters and symbols used to uniquely identify subscriber, user, network element, function or network entity providing services or applications

impact: result of an information security incident, caused by a threat, which affects assets

integrity: safeguarding the accuracy and completeness of information and processing methods

mitigation: limitation of the negative consequences of a particular event

preparedness: activities, contingencies and measures taken in advance to ensure an effective response to the impact of hazards

NOTE: Source: United Nations International Strategy for Disaster Reduction; available at: http://www.unisdr.org/

residual risk: risk remaining after risk treatment

resilience: concept associated with resisting the loss of capacity of a failure or foreseen overload, by optimizing the availability and quality of service of telecommunications systems and support resources, thus enabling a system to return to a previous normal condition

risk: potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization

threat: potential cause of an incident that may result in harm to a system or organization

NOTE 1: A threat consists of an asset, a threat agent and an adverse action of that threat agent on that asset [41].

NOTE 2: A **threat** is enacted by a **threat agent**, and it may lead to an **unwanted incident** that breaks certain pre-defined security objectives.

threat agent: an entity that can adversely act on an asset

unwanted incident: incident such as loss of confidentiality, integrity and/or availability [52]

user: person or process using the system in order to gain access to some system resident or system accessible service

vulnerability: weakness of an asset or group of assets that can be exploited by one or more threats

NOTE: A **vulnerability**, consistent with the definition given in ISO/IEC 13335 [45], is modelled as the combination of a **weakness** that can be exploited by one or more **threats**.

Annex C: Abbreviations

Annex C: Abbreviations

ACARS	aircraft communications addressing and reporting system
ADS	automatic dependent surveillance
AEEC	Airlines Electronic Engineering Committee
AF	assured forwarding
AIS	aeronautical information services
ANSP	air navigation service provider
ARTES	advanced research in telecommunications systems
AS	autonomous system
ASN.1	Abstract Syntax Notation One
ATC	air traffic control
ATM (1)	asynchronous transfer mode
ATM (2)	air traffic management
ATN	aeronautical telecommunication network
BCM	business continuity management
BCMS	business continuity management system
BGP	Border Gateway Protocol
Calit2	California Institute for Telecommunications and Information Technology
CDF	cumulative distribution function
CDMA	Code Division Multiple Access
CEN	Comité Européen de Normalisation / European Committee for Standardization
CENELEC	Comité Européen de Normalisation Électrotechnique / European Committee for Electrotechnical Standardization
CNS	communications, navigation and surveillance
CPDLC	controller-pilot data-link communication
CPE	customer premises equipment
CpoA	content point of attachment
CRAVED	concealable, removable, available, valuable, enjoyable, and disposable
CSMA/CD	carrier sense multiple access with collision detection
CWA	CEN Workshop Agreement
Diffserv	differentiated service
DL-GTW	data link gateway
DL-IR	data-link services implementing rule
DNS	Domain Name System

DNSSEC	Domain Name System Security Extensions
DR	disaster recovery
DS	differentiated service
Dst	destination
EC	European Commission
ECMP	equal cost multipath
ECN	electronic communications network
ECN&S	electronic communications networks and services
ECS	electronic communications services
EF	expedited forwarding
EMTEL	emergency telecommunications
ENISA	European Network and Information Security Agency
ESA	European Space Agency
ESP	encapsulating security payload
ETSI	European Telecommunications Standards Institute
ETSO	European Technical Standard Order
EUROCAE	European Organization for Civil Aviation Equipment
FAA	Federal Aviation Administration
FANS	Future Air Navigation System
FDMA	frequency division media access
FEC	forwarding equivalence class
FG	focus group
FIFO	first in, first out
FRAM	Functional Resonance Assessment Method
GJU	Galileo Joint Undertaking
GMPCS	global mobile personal communications via satellite
GNSS	global navigation satellite system
GoS	grade of service
GPS	global positioning system
HTTP	Hypertext Transfer Protocol
IAB	Internet Architecture Board
IANA	Internet Assigned Numbers Authority
IATA	International Air Transport Association
ICANN	Internet Corporation for Assigned Names and Numbers
ICAO	International Civil Aviation Organization

ICET-98	Intergovernmental Conference on Emergency Telecommunications of 1998
ICSG	Industry Connections Security Group
ICT	information and communications technologies
IEC	International Electro-technical Commission
IEEE	Institute of Electrical & Electronics Engineers
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IKE	key exchange
ILM	incoming label map
IntServ	integrated services
IP	Internet Protocol
IPDV	IP packet delay variation
IPLR	IP packet loss ratio
IPRE	IP packet-transfer reference event
IPsec	Internet Protocol Security
IPTD	IP packet transfer delay
IPTV	Internet Protocol Television
ISMS	information security management system
ISO	Organisation Internationale de Normalisation / International Organization for Standardization
ISOC	Internet Society
ITS	intelligent transport systems
ITU	International Telecommunication Union
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
LER	label edge router
LSP	label switched path
M2M	machine-to-machine
MIME	multipurpose internet mail extensions
MP	measurement point
MPLS	Multi Protocol Label Switching
MSAW	minimum altitude safety warning
MTBF	mean time between failures
MTTR	mean time to repair
NAP	network access point
NGN	next generation networks
NHLFE	next hop label forwarding entry

NIPC	American National Infrastructure Protection Center
NSE	network section ensemble
NTP	network time protocol
OCC	Open Cloud Consortium
OCHA	United Nations Office for the Coordination of Humanitarian Affairs
OMP	optimal multipath
OSI	open systems interconnection
PANS	Procedures for Air Navigation Services
PIA	percent IP service availability
PIU	percent IP service unavailability
PKI	public key infrastructure
PPP	Point-to-Point Protocol
PSRN	packet-switched and routed network
QoS	quality of service
RAID	redundant array of inexpensive disks
RAN	radio access network
RCP	required communication performance
REST	representational state transfer
RFC	request for comment
RNP	required navigation performance
RPR	resilient packet ring
RPSEC	Routing Protocol Security
RSP	required surveillance performance
RSVP	Resource ReserVation Protocol
RTCA	Radio Technical Commission for Aeronautics
RTSP	required total system performance
SARP	standards and recommended practice
S-BGP	Secure Border Gateway Protocol
SDO	Standards Developing Organization
SES	Single European Sky
SESAR	Single European Sky ATM Research
SIDR	secure inter-domain routing
SIP	Session Initiation Protocol
SIS	signal-in-space
SLA	service level agreement

SMS	safety management systems
SNC	sub-network connection
SNMP	Simple Network Management Protocol
SpoA	service point of attachment
SPR	safety and performance requirements
Src	source
TCP	Transmission Control Protocol
TDMA	time division media access
TFF	time to fail
TISPAN	Telecommunications and Internet converged Services and Protocols for Advanced Networking
TpoA	transport point of attachment
TTF	time to fail
TTR	time to repair
UAC	user authentication code
UDP	User Datagram Protocol
URI	uniform resource identifier
URL	uniform resource locator
W3C	World Wide Web Consortium
WGET	Working Group on Emergency Telecommunications
XAdES	XML Advanced Electronic Signatures
XML	eXtensible Markup Language
XML-DSig	XML Signature Syntax and Processing
XSD	XML Schema Definition Language

enisa
European Network
and Information
Security Agency

P.O. Box 1309 71001 Heraklion - Crete - Greece
Tel: +30 28 10 39 1280, Fax: +30 28 10 39 1410
Email: resilience@enisa.europa.eu