enisa
European Network and Information Security Agency

Ontology and taxonomies of resilience

Version 1.0 – December 2011

Contributors to this report

Authors of the report:

- Panagiotis T. Vlacheas – University of Piraeus Research Centre
- Vera Stavroulaki – University of Piraeus Research Centre
- Panagiotis Demestichas – University of Piraeus Research Centre
- Scott Cadzow – Cadzow Communications Consulting Ltd

- Slawomir Gorniak – ENISA
- Demosthenes Ikonomou – ENISA

Acknowledgements

ENISA would like to thank the contributors and reviewers of this study.

About ENISA

The European Network and Information Security Agency (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact details

For contacting ENISA or for general enquiries on resilience, please use the following details:

- E-mail: resilience@enisa.europa.eu
- Internet: http://www.enisa.europa.eu

For questions related to this paper, please use the following details:

- E-mail: sta@enisa.europa.eu

Contents

1 Executive Summary

The present report provides an ontology of resilience alongside and embedding a taxonomy of resilience. Telecommunications networks have been extended from the original circuit switched model where reliability and availability were often simply stated as five nines, i.e. uptime should be 99.999% over a year and availability was to give service at five-nines to all subscribed users. How big the system had to be was most often simply determined using Erlang's traffic modelling taking account of call attempts per hour and call hold time. As networks have become increasingly more complex and more critical to business their reliability and resilience have themselves become more critical to understand and engineer into the network design.

The present report introduces two tools for understanding resilience as a network design target and the output of those tools when applied to resilience. The tools introduced are classification using taxonomy, and relationship modelling using ontology with taxonomy at its core.

The following key elements that are addressed by the ontology design presented the document:

- Application at multiple implementation levels (hardware, middleware, software), network layers (network, application layers) on both the network and the user side.
- Application to the aggregation of cloud computing, real time detection and diagnosis systems, sensor networks, future wireless networks and supply chain integrity.
- Extension of means to derive definitions in standardization.
- Identification of the use of metrics for resilience measurement and compliance.

The ontology presented in this document offers an open, interoperable and scalable framework, which is intended to lead to further development in standardization. The document addresses ontology and taxonomy as methods that extend the role of standards in complex areas by allowing more complex scenarios to be addressed than are normally considered by standardisation. Resilience falls into this class of complex scenarios as the solution set covers many different technologies and strategies than many simpler though complex protocols.

The target audience consists of specialised audience of stakeholders involved in resilience and the standardisation bodies that may contribute to resilience solutions.

This report was prepared for ENISA by a consortium formed by Cadzow Communications Consulting Ltd. (UK) and the University of Piraeus Research Center (Greece) under the leadership and guidance of the "*Resilience of public Communication Networks and Services*" group at ENISA.

2 Introduction

The ENISA report on gaps in standardisation related to resilience of communication networks [3] stated that there is no consistent taxonomy for cyber security that identifies the role of resilience. The purpose of the present document is to address this gap for resilience. The document defines an ontology of resilience in order to address a behavioural dimension of the topic with a taxonomy of resilience, network and security terms at its core.

In was shown in [3] that existing standards in the field of networks and network security have so far only addressed resilience indirectly if at all and thus without detail definition of the role of resilience as an objective in making networks secure (in the meaning of availability from the conventional Confidentiality Integrity Availability (CIA) paradigm). However whilst in the CIA paradigm the success of a measure is often directly measurable and thus a set of metrics exist for comparison of 2 or more approaches, for say integrity verification, the existence of such metrics in resilience is mostly lacking. As such metrics play a significant role in giving meaning to any comparison of system resilience the identification of them is addressed within the ontology developed and proposed in the present document.

The primary purpose of the ontology and its contained taxonomy defined in this document is to use the results as the basis of definitions and processes in future work. The current approach to definition in most Standards Development Organisations (SDOs) is to separate definition from use and assume terms are always understood. For example the term **threat** is defined as "potential cause of an incident that may result in harm to a system or organization" but this approach doesn't put threat into context whereas using the approach of taxonomy and ontology introduces the additional contextual dimensions, in other words the additional concepts that a threat is enacted by a threat agent and leads to attack on the system objectives. Ultimately the intent is to use the ontology within standards that have to be followed for all network based resilience measures. This is not to state that ontologies are not used in development of standards or of networks although it is hard to find explicit use of the terms in existing standards. In practice it can be shown that many existing standards, particularly in the security domain, tend towards ontologies in their structure (but not in their terminology).

Before defining an ontology or a taxonomy it is essential to define what they are and why they are of benefit. Supporting the definitions and rationale given in this document a complete analysis can be found in [14] that also presents a methodology for developing and evaluating ontologies (a summary of research in the field is given in Annex D).

Where stakeholders, i.e. the people, organisations, and software systems, are required to communicate among themselves to achieve some specific objective they often misinterpret the same subject matter due to a desire or imperative to translate to their personal context. The misinterpretation leads to lack of a *shared understanding* that then leads to a number of unwanted consequences that include:

- *poor communication* between these people and within their organisations,

- difficulties when identifying requirements and defining a *specification* of an IT system,
- lack of *interoperability*, *reliability*, *re-use and sharing* capabilities, which lead to much *wasted effort* (in common terminology leading to endless cycles of *re-inventing the wheel*) because of different methods, sector specific terminology (jargon) and tools.

Without *shared understanding* acting as a *unifying framework* for the different viewpoints the problems that arise from misunderstanding will continue, and exaggerate conceptual and terminological confusion. Ontology is the term used to refer to the science and methods of developing a shared understanding of some domain of interest which may be used as a unifying framework to solve the above problems. An ontology entails or embodies a set of concepts (e.g. entities, attributes, and processes), their definitions and their inter-relationships with respect to a given domain. This is referred to as a conceptualisation and may be *implicit* or *explicit,* depending on whether a subjective or objective analysis is undertaken. Note however that the aims of standardisation and of both, ontologies and taxonomies, is the same even if the practice is different. To this end a standard defines only the minimum requirements for a product or service that implements it to work safely and dependably with other products implementing the same (or associated) standards, i.e. if 2 mobile phones each implement the GSM standards they will be able to communicate with a standards compliant GSM base station and make calls to each other. The key matter than distinguishes those areas where taxonomy and ontology will give gain over conventional approaches to standardisation is where complex multi-factor environments are brought together to achieve new objectives. This is the case for resilience where conventional requirements for availability do not address resilience directly but address the more readily understood areas of reliability, maintainability and availability discretely rather than as they would by consideration using ontology: In combination.

The following quote taken from the Shared Re-usable Knowledge Bases (SRKB)[1] electronic mailing list summarises what an ontology is and the various forms and contexts it arises in.

QUOTE: "Ontologies are agreements about shared conceptualizations. Shared conceptualizations include conceptual frameworks for modelling domain knowledge; content-specific protocols for communication among interoperating agents; and agreements about the representation of particular domain theories. In the knowledge sharing context, ontologies are specified in the form of definitions of representational vocabulary. A very simple case would be a type hierarchy, specifying classes and their subsumption relationships. Relational database schemata also serve as ontologies by specifying the relations that can exist in some shared database and the integrity constraints that must hold for them."

[1] *http://www-ksl.stanford.edu/email-archives/srkb.index.html*

In [14], the domains or subject areas for use of ontologies is subdivided into the following categories:

- Communication:
  - Ontologies enable shared understanding and communication "between people with different needs and viewpoints arising from their particular contexts" [14].
- Interoperability:
  - Many applications of ontologies address interoperability in which different users need to exchange data either in a practical deployment environment or in development between different software tools. A major theme for the use of ontologies in domains such as enterprise modelling and multiagent architectures is the creation of an integrating environment for different software tools.
- Systems engineering:
  - Specification:
    - In the specification of software systems, ontologies facilitate the process of identifying the requirements of the system and understanding the relationships among the components of the system among distributed teams of designers working in different domains and provide a declarative specification of a software system, which allows to reason about what the system is designed for, rather than how the system supports this functionality.
  - Reliability:
    - Ontologies enable the use of (semi-)automated consistency checking of the software system with respect to the declarative specification and can be used to make explicit the various assumptions made by different components of a software system, facilitating their integration.
  - Reusability:
    - Ontologies in order to be effective must also support reusability, so that the modules can be imported and exported among different software systems and are used to provide a framework for determining which aspects of an ontology are reusable between different domains and tasks. To be useful, these ontologies must be customisable through extension, both to the class of problems and the class of users, allowing the incorporation of new classes of constraints and the specialisation of concepts and constraints for a particular problem.

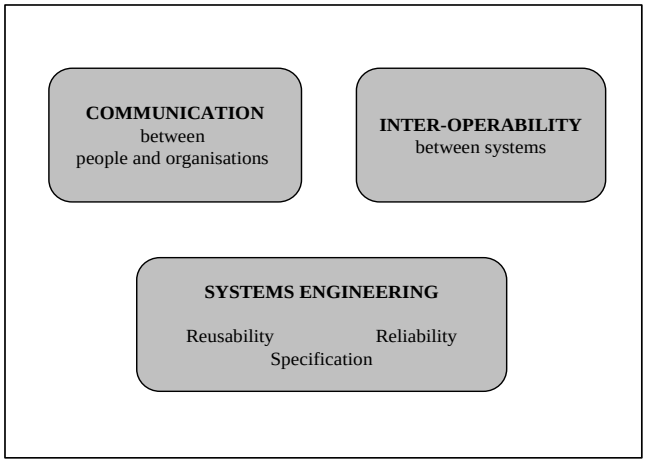


Figure 1: Uses for ontologies

Taxonomies have a close relationship to ontologies. Taxonomy is derived from 2 Greek words: taxis, meaning the arrangement or ordering of things; and, nomos meaning anything assigned a name, and the usage addressed by the thing. Taking an almost literal interpretation of this suggests that taxonomies give structure to the naming of things and this is clearly the approach used in biology and similar sciences. 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.
- 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 also ensure that alternate or less precise terms are excluded.
- 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.

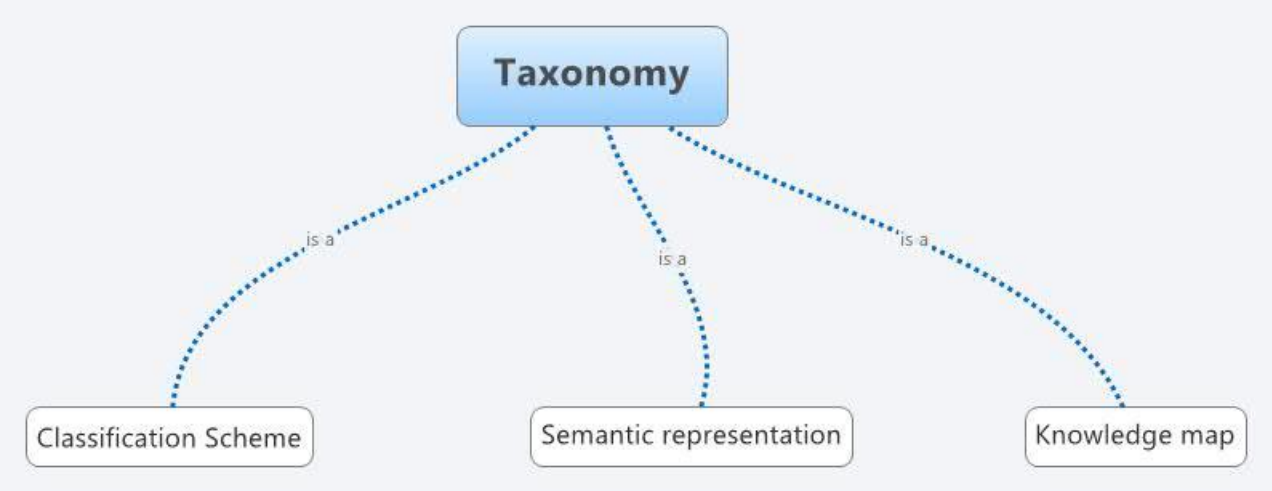


Figure 2: Visualisation of the definition of a taxonomy

In many instances a taxonomy is considered 2-dimensional (which could be presented as a simple table) whereas ontologies are often considered as 3-dimensional although by using a taxonomy in an ontology as it proposed in this document the boundary between taxonomy and ontology is blurred.

3 An ontology for defining resilience requirements in network design

The design of a network has to balance a number of competing requirements. There are a number of models that can be presented to express requirements but the one that is prevalent in the security standards work presented at ETSI is that found in TR 187 011[2] and in TS 102 165-1[3] in which requirements are derived from objectives as shown in figure 1 (taken from TR 187 011).

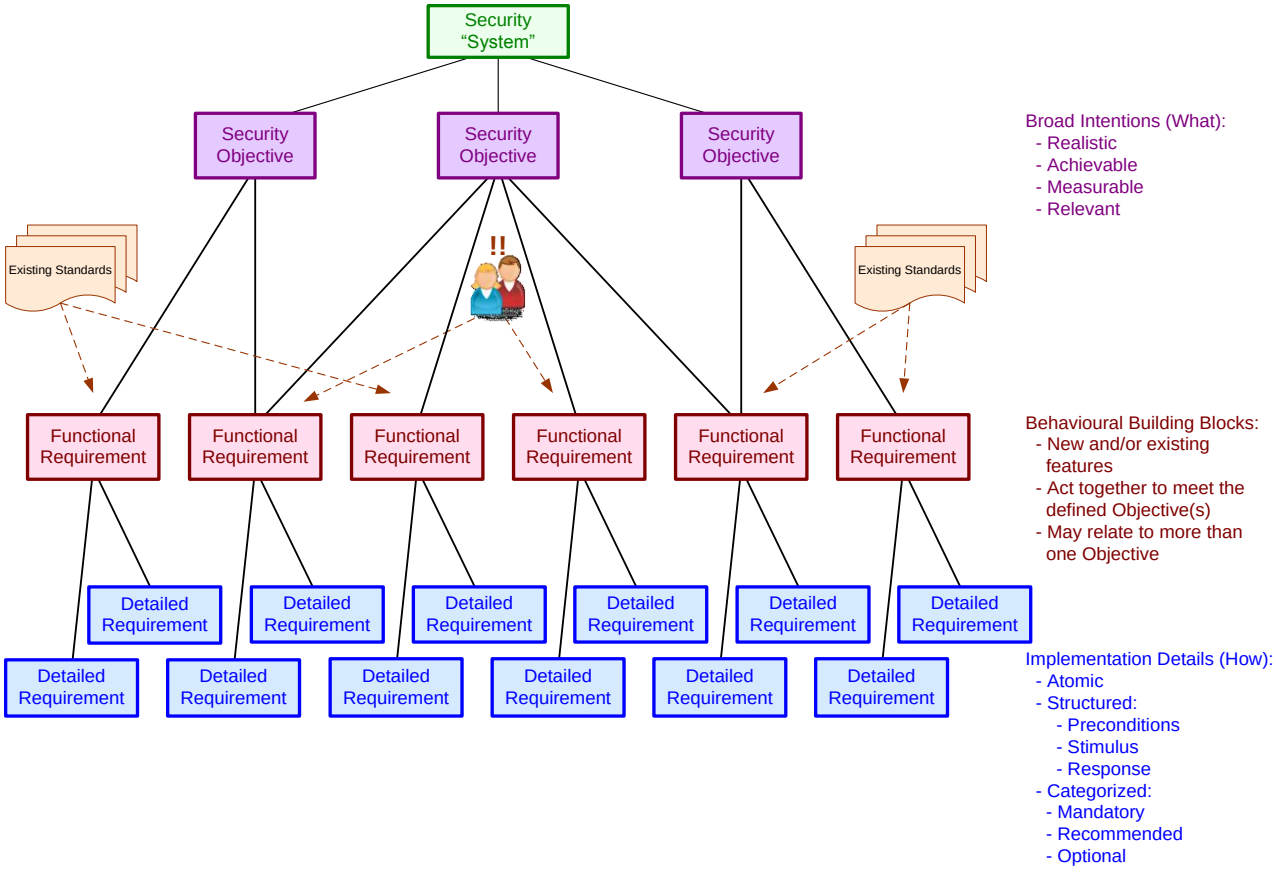


Figure 3: Security objectives and requirements

This hierarchy of objectives and requirements is related to the Threat Vulnerability Risk Analysis approach to security design shown in figure 2 (taken from TR 187 011). However it should be noted that by some additional modelling it can be shown that this approach to requirements specification is ontological in structure:

- An objective is satisfied by a functional requirement(s), the corollary or ontological reverse relationship is that a functional requirement contributes to the satisfaction of one or several objectives

[2] *http://docbox.etsi.org/TISPAN/Open/NGN_LATEST_DRAFTS/RELEASE3/07053-ngn-r3v372.pdf*

[3] *http://docbox.etsi.org/EC_Files/EC_Files/ts_10216501v040101p.pdf*

- A functional requirement is satisfied through one or several detailed requirements, corollary or ontological reverse relationship is that a detailed requirement contributes to the satisfaction of one or several functional requirements

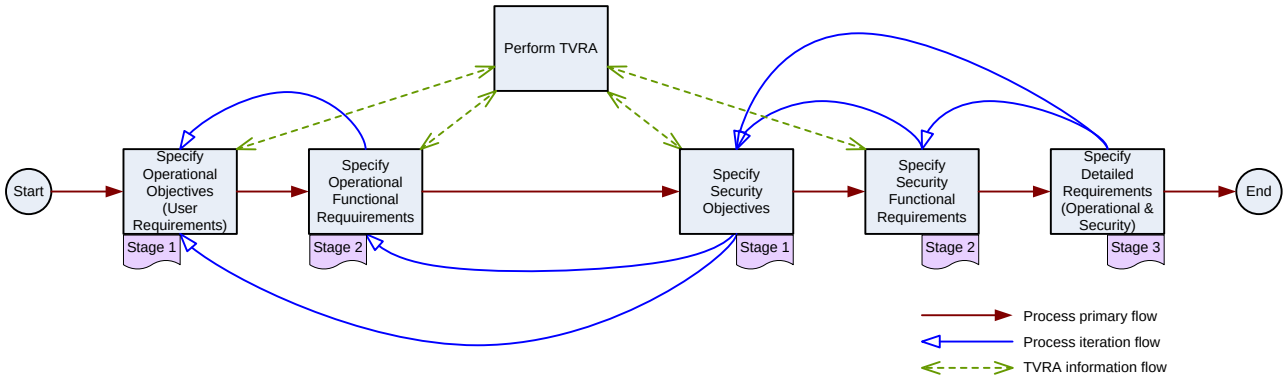


Figure 4: Standards development process including security aspects

The set of requirements that is to be considered in networks covers a broad area with many dependencies between requirements classes.

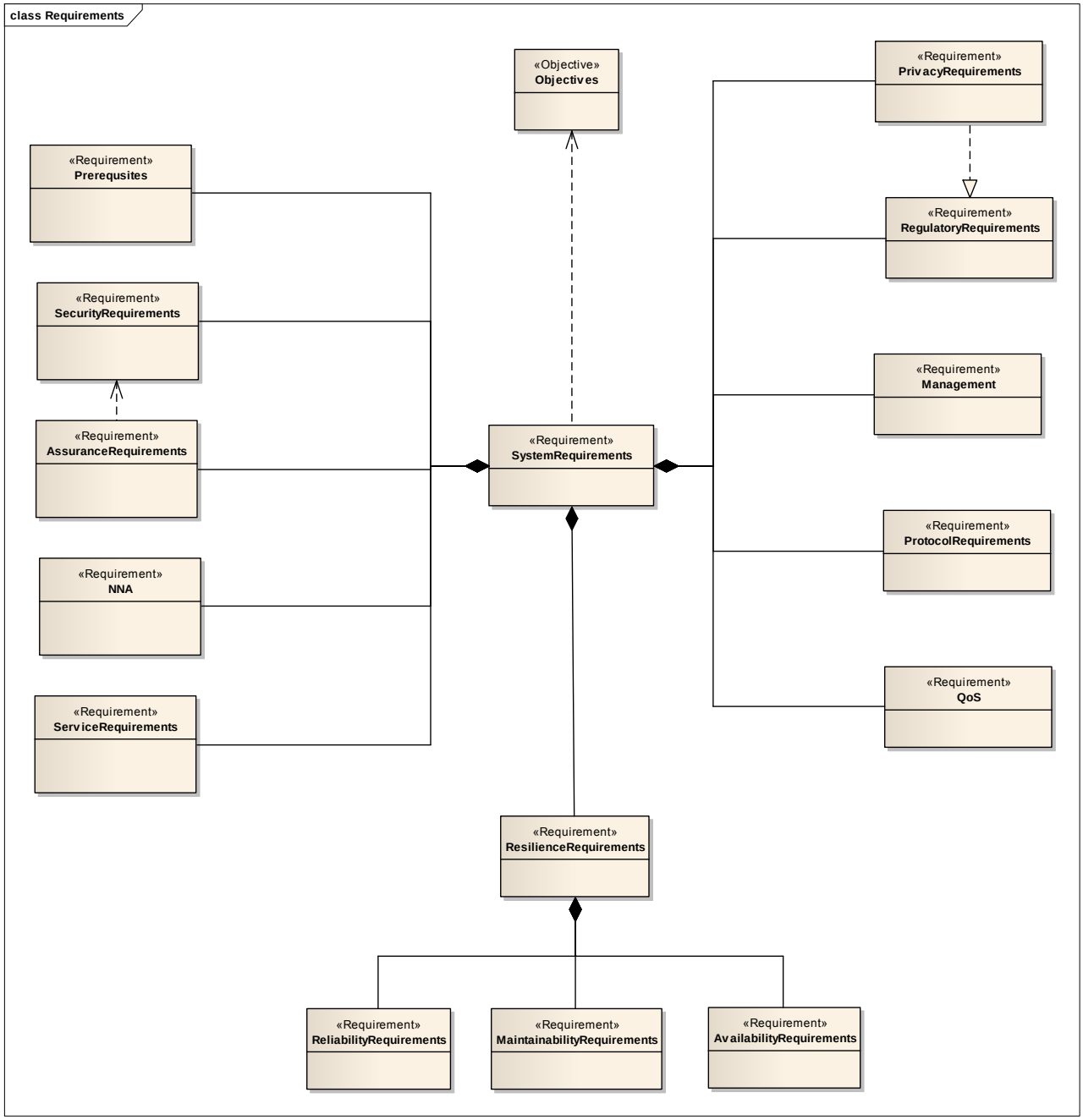


Figure 5: Structure of requirements to be considered in network design

The addition of a specific class of "Resilience Requirements" which are themselves a composition of requirements for reliability, maintainability and availability brings the concept of resilience into the network design. Related to this is a requirement to have resilience objectives for the system that are themselves realistic, achievable, measurable and relevant as defined in ETSI TR 187 011 []. Underlying the introduction of resilience is the introduction of requirements that relate directly to the 3 main metrics considered in [3] for the test and

measurement of resilience: Reliability; Maintainability; and, Availability. Availability is already explicitly described in the ontology for cyber-security described by ITU-T and by ETSI in TR 187 010 [].

The characteristics of resilience have been explored in earlier work in ENISA and there is a degree of uncertainty over the point at which a system maintains availability and reliability but fails to be resilient. Resilience can be perceived as a measure of ability to work through stress and recover to the same initial condition when the stress is removed. In telecommunications and information processing networks where the input conditions typically tend towards chaotic identifying the stable point to return to after a stress event has a degree of uncertainty. As such resilience is not a very straightforward item to define by requirements. Using the model for specifying detail requirements in TR 187 011 of preconditions, stimulus and response the precondition of resilience is the steady state, the stimulus is the load that leads to stress, and the response is (eventually) a return to the steady state. The problem from a requirements point of view is that if the initial response to stress is to stop but the eventual response is to restart in the same initial state this could be argued to be "resilient" but it is not as it is more correctly simply recoverable. A truly resilient network has to maintain operation throughout the stress event (i.e. availability should not be degraded) and also return to a state as if unaffected by the stress when the stress is removed.

EXAMPLE: A longbow has to be stressed to perform and as such the material of the bow has to be designed to be sufficiently rigid such that when the bowstring is drawn the bow itself does not fold but has to "give" at the ends of the bow to allow the bowstring to be extended. When the arrow is released the bow returns to its initial resting state. A failure of this stress-recovery cycle would break the longbow so the entire bow as a system has to be designed to be resilient.

4 Stakeholder model in network resilience

In the modelling of the ontology the key stakeholders in network resilience are identified. The stakeholder model for resilience is similar to that in development at ETSI TISPAN for TS 187 001 but extended to the business domain.

Table 1: Stakeholders (actors) in the NGN and their roles

Actor	Role in resilience	Has relationships with …
End user	Receiver of service (push) Initiator of service (pull)	Content provider Service provider Regulatory authority Manufacturer
Content owner	Provides content for distribution by the content provider	Content provider Regulatory authority
Content provider	Distributes content • On demand • Broadcast/Multicast	Content owner End user Service provider
Service provider	Provides services • On demand (Pull) • On event (Push)	Service provider End user Content provider
Regulatory authority	Provides legal framework for such items as privacy, data protection, safety	Service provider Content owner Content provider Manufacturer End user
Law enforcement authority	Recipient of data (LI/DR)	Service provider
Manufacturer	Provides the software/hardware that enables the network or service	Regulatory authority Service provider End user
System integrator	Brings content, software, hardware and service together to supply to the service provider	Content provider Manufacturer Content provider

The stakeholder model for resilience therefore covers the same actors as for conventional network design. However the role of the stakeholders in managing network resilience is somewhat different from those considered in conventional network design.

5 Taxonomy of resilience

A taxonomy that allows for classification of a network technology may for example state that TETRA is an example of a 25KHZ bandwidth, 400MHz band, TDMA cellular technology operating as a wireless access network. Unfortunately as TETRA can also operate at 900MHz it would be necessary for a taxonomy to distinguish the two modes as separate types. A taxonomy of networks where the classifications (taxoms) are based on shared characteristics is shown in part in Figure 6. The aim of the taxonomy is to ensure that there is no ambiguity in classification. In modern ICT systems however a single entity may have multiple characteristics in parallel. This is best evidenced in a smartphone that holds characteristics of a cellular phone but also contains characteristics of a personal computer. The classification schema of Figure 6 may lead to a single entity such as a smartphone having multiple entries which is potentially unsafe as it could lead to ambiguity.

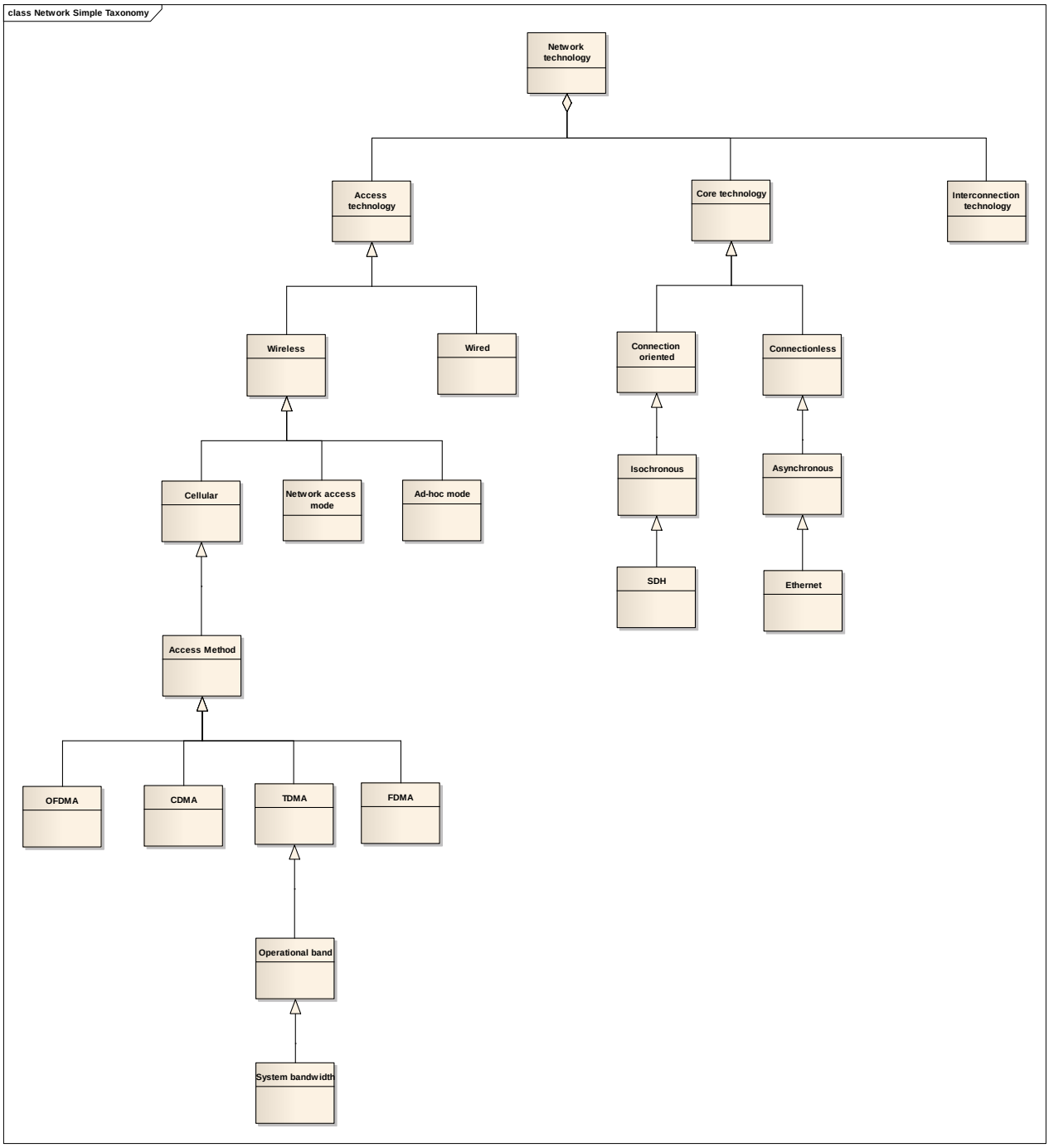


Figure 6: Taxonomy of networks based on shared characteristic classification

If we take the model presented by Lacy in [8] the relationships in this simple hierarchical taxonomy should represent "*is a*" relationships, so from the model given in Figure 6 we should be able to state that "CDMA *is an* Access Method *is a* Cellular *is a* Wireless *is an* Access Technology *is a* Network Technology" which doesn't in fact make a lot of sense when written back in this form although it could be argued that the diagram itself is meaningful. So for use

in a semantic network (such as advanced telecommunications) that uses taxonomies and ontologies illustrative approaches such as in Figure 6 may need to be re-thought to be more amenable to machine processing.

The alternative to a shared characteristic classification of an evolutionary classification scheme is similar to the one adopted in Figure 7 for the countermeasures and threat modelling in the security domain.

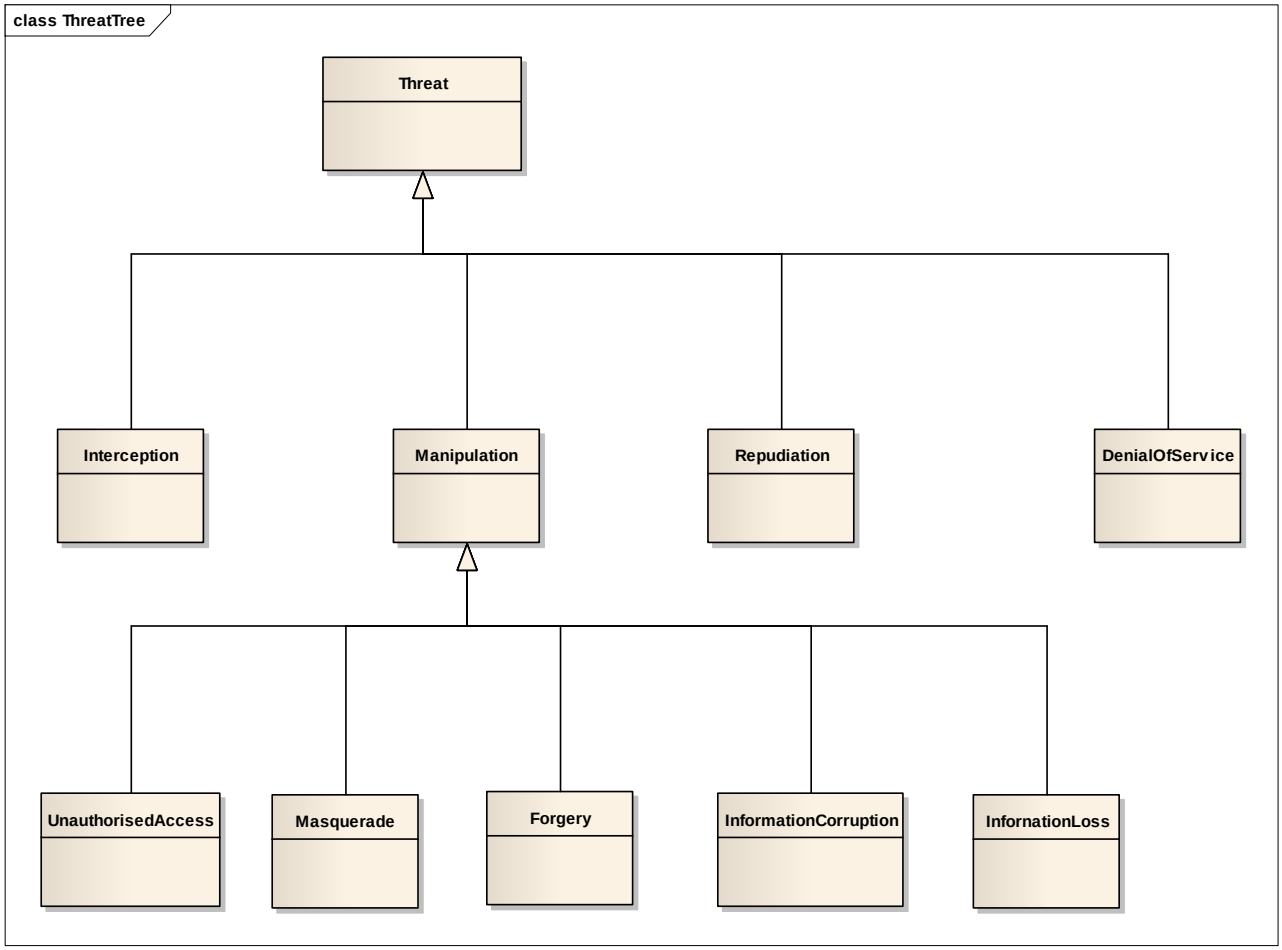


Figure 7: Taxonomy of threat

Here we can state that "Forgery *is a* Manipulation" and of course "Manipulation *is a* Threat" (more correctly the "*is a*" relationship should be seen as "*is a specialisation of*", allowing the reverse relationship to be written as "*is a generalisation of*"). Another example of describing threat agents is given in Figure 8 although in this case each leaf requires additional definition text to make it clear why for automated threat agents there is a distinction between "scripted", "controlled" and "autonomous".

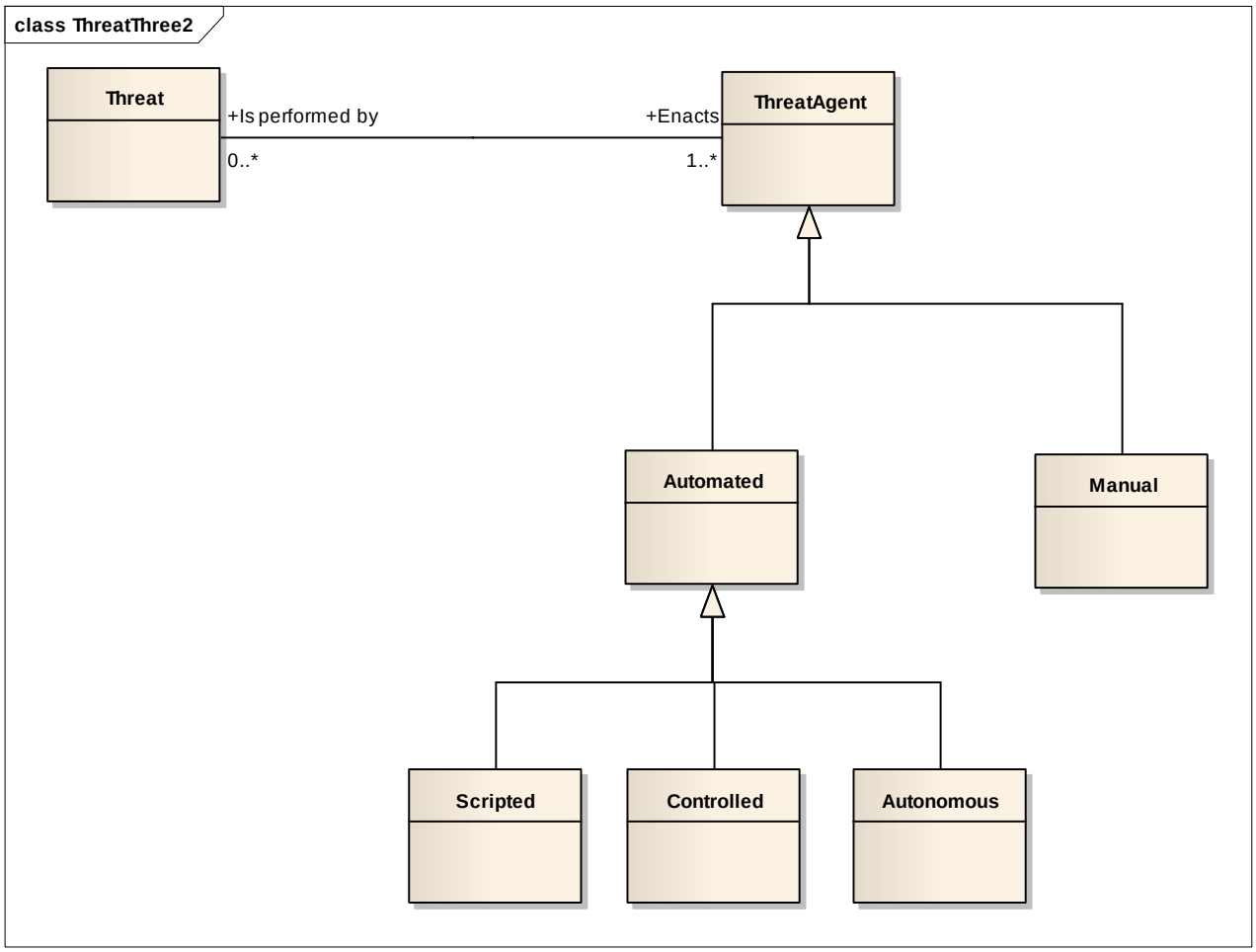


Figure 8: Taxonomy of threat agent showing link to threat taxonomy

Resilience can be expressed in the security model as shown in Figure 9. In this case 2 aspects of resilience are shown:

- Resilience degrading measure is a specialisation of a threat agent; and,
- Resilience improving measure is a specialisation of a security countermeasure.

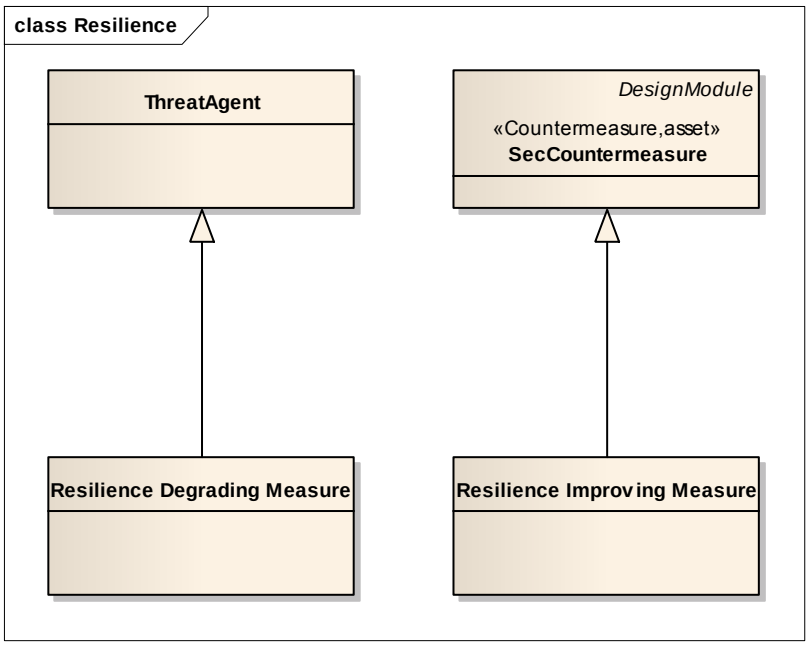


Figure 9: Resilience measures in the security domain

When expressed as a threat agent the resilience degrading measures may be considered as leading to a denial of service therefore the threat family attacked by the threat agent is denial of service. In general however resilience is not a tangible asset in that providing resilience to a system does not of itself guarantee a working model that the system will be invulnerable to denial of service. If this is considered in the manner ENISA's report [] and the more recent work on metrics there is a requirement to be able to express resilience by those system elements we can control. This is shown in Figure 10.

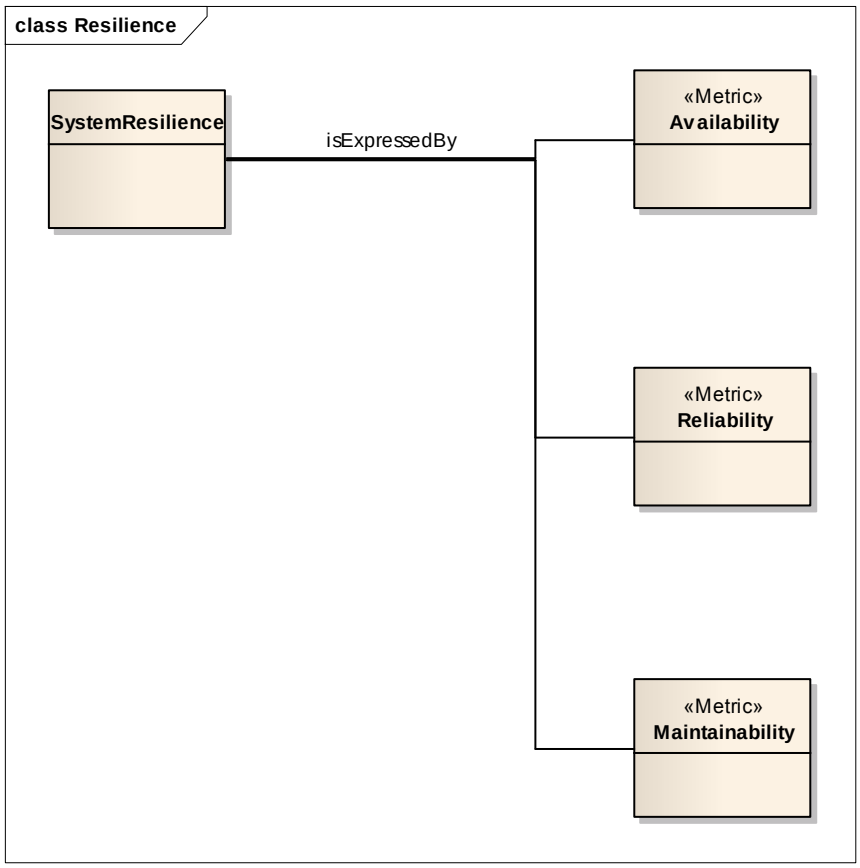


Figure 10: Resilience expression through metrics

To move this towards the grammar favoured by Lacy in [8] we may state:

- System resilience is expressed by the combination of the system's availability, reliability and maintainability.

This allows further expression of how to give assurance of availability, of reliability and of maintainability. The further development of the taxonomy is moved into the development of the ontology in the next clause where the ontology described so far is used in the root of the definitions and resulting associations.

6 Ontology of resilience

6.1 Towards an ontology for network resilience

As identified in Annex D, there is a need for an ontology which will address the end-to-end resilience, considering a heterogeneous mix of different implementation levels, network technologies, human factors, and application domains.

Figure 11 shows the model for the end-to-end resilience ontology that is further decomposed and examined in the remainder of this clause. "Resilience" is the main class located at the centre of the ontology and is considered as the root for this analysis. It has direct relationships with the classes "ThreatAgent", "Domain", "Metrics", "Threats" and "Means" where all the relationships are defined based on the root, i.e. network resilience.

"Threats" are what "Resilience" confronts, namely the potential attacks against network assets. In this concept, "confronts" is the relationship, while the inverse relationship may be defined as "are confronted by". The "Threats" class has also its subclasses. Therefore, there are "Security Threats", "Dependability Threats", "Disasters" as physical threats caused by natural events, "Interaction Conflicts" as implicit threats due to incompatibilities/conflicts among interacting network assets, "Changes" with respect to threats due to dynamic conditions and "Supply Chain Attacks" (attacks being performed throughout the supply chain, until the delivery of the equipment or service).

A "ThreatAgent" denotes the entity that threatens "Resilience", namely the agent who performs the "Threats". In this concept, "is threatened by" is the relationship, while the inverse relationship is "threatens". A "ThreatAgent" may be a "Human", a "Machine" or the "Nature" itself.

"Domain" is by which "Resilience" is required, namely the domain where resilience applies. In this concept, "is needed by" may be considered as the relationship and "needs" the inverse relationship. Four domains can be distinguished in order to have an end-2-end consideration of resilience, namely "Network", "Service", "Customer" and "Business".

"Metrics" are the attributes by which "Resilience" is expressed, since network resilience is an integrating concept that encompasses such attributes. So, "is expressed by" is the relationship and "express" the inverse relationship. There are mainly six resilience metrics [i.3], namely "Availability", "Reliability", "Safety", "Confidentiality", "Integrity" and "Maintainability". Confidentiality has a great prominence especially when addressing security, in the sense that it represents the absence of unauthorized disclosure of information. In general, security is considered as a concurrent composite of confidentiality, integrity and availability.

The "Means" class represents the means which have been developed to attain the various resilience metrics and intend to either eliminate threats or fix vulnerabilities. Therefore, "is enabled by" is the relationship and "enables" the inverse relationship. In this ontology, the resilience means are kept at a high level representing management functions, since one of the objectives, as also found out in Annex D, is to target an audience consisting of resilience

stakeholders and mainly industry stakeholders. Of course, these management functions manage some instruments/tools to which we will refer later. Resilience "Means" consist of "Fault Management", "Trust Management", "Supply Chain Integrity Management", "Cooperation" when "Interaction Conflicts" exist, "Risk Management", "Governance", "Security" in terms of security standards and tools, "Cognitive and Self-Management".

Each class is connected to its subclasses with an "is" relationship. Inverse relationship may be "is a kind of". For simplicity, these relationships are only referred to when absolutely necessary.

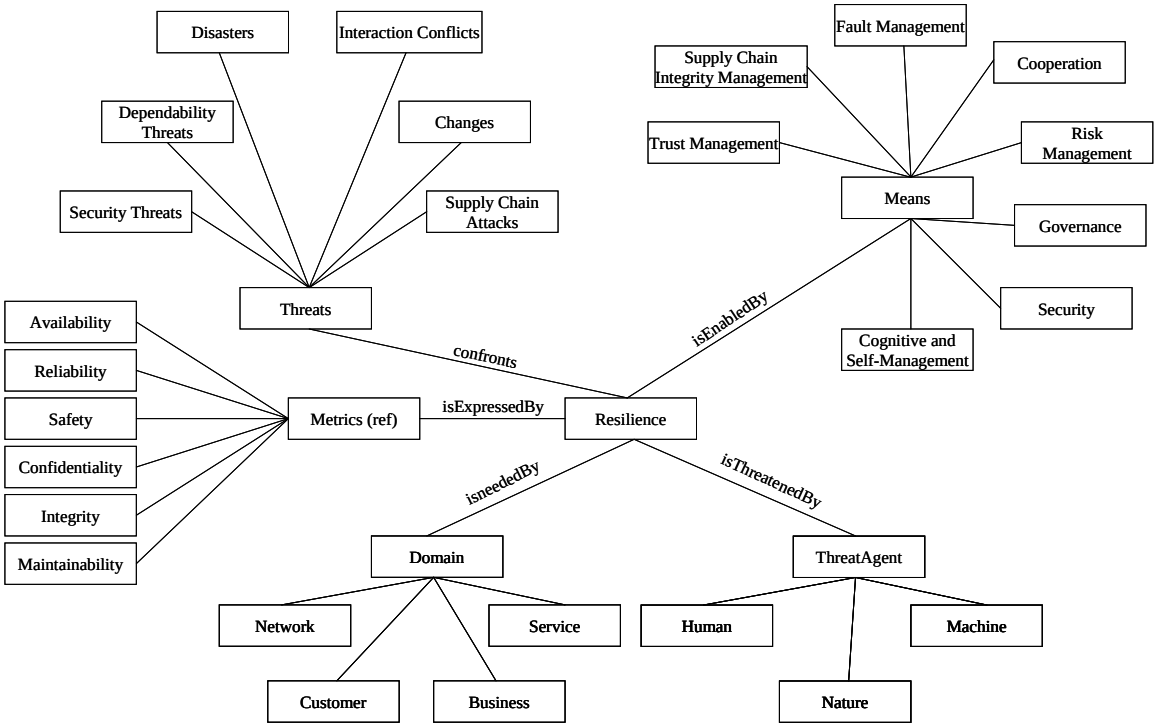


Figure 11: High level overview of resilience ontology

Some of the classes existing in Figure 11 are analysed in more detail in succeeding clauses. The relationship and inverse relationship remain "is" and "is a kind of", respectively.

"Security threats" consist of "Interception", "Manipulation", "Repudiation" and "Denial Of Service", to which we have also referred to in subsection 3.3 and which are depicted in Figure 12.

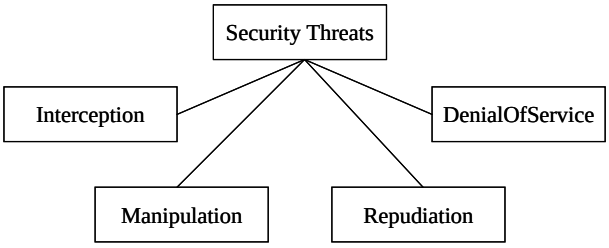


Figure 12: Security Threats

"Dependability threats" include "Failures", "Errors" and "Faults" as analysed in [i.3] and can be found in Figure 13. "Supply Chain Attacks" are presented in the ENISA study [4] and "Disasters" in the ENISA study [3].

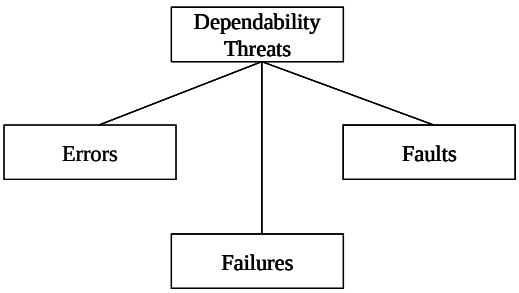


Figure 13: Dependability Threats

"Supply Chain Integrity Management" is presented in the ENISA study [4]. "Fault Management" is analysed in [i.3] and consists of "Fault Forecasting", "Fault Removal", "Fault Prevention" and "Fault Tolerance" as depicted in Figure 14.

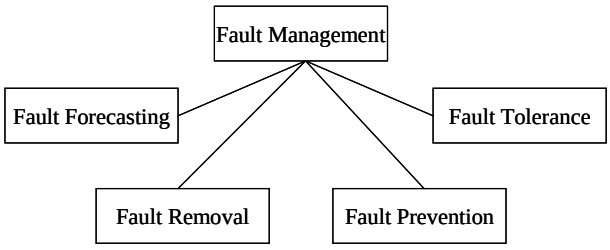


Figure 14: Fault Management

"Cognitive and Self-Management" corresponds to the well-known MAPE cycle [15]-[17], namely Monitor, Analyse, Plan, Execute enabled with Learning (Knowledge) capabilities, and is depicted in Figure 15.

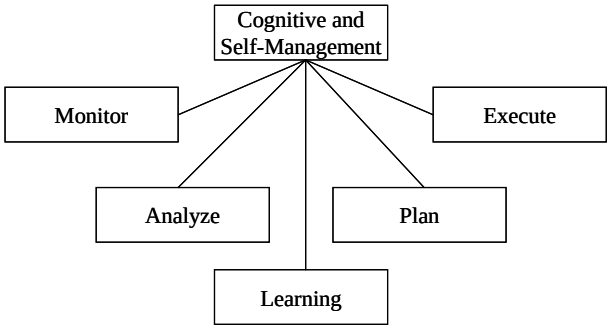


Figure 15: Cognitive and Self-Management Management

The "Means" are supported by specific instruments, which make their effectiveness possible. The relationship between "Means" and "Instruments" is "use" and the inverse relationship "are used by". Therefore, the "Trust Management" uses mainly "Certification" (Figure 16).

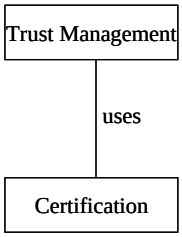


Figure 16: Trust Management instruments

"Security" requires mechanisms, services and policies according to [i.12]. Generic security services include authentication, authorization, non-repudiation, privacy, intrusion-tolerance, etc., while security mechanisms include specific techniques like encryption, digital signatures, traffic padding, routing control, access control, firewall, redundancy, etc." [i.12] Security policies define high level of assumptions and rules, such as the Bell-LaPadula confidentiality model in military systems and the Clark-Wilson integrity model in commercial systems. "Security" instruments are depicted in Figure 17.

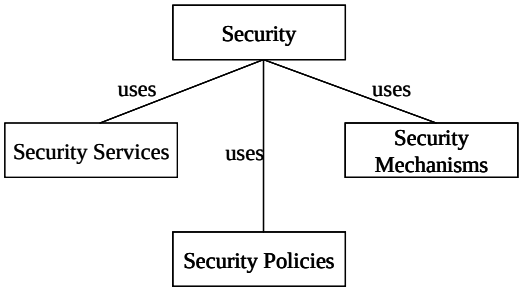


Figure 17: Security instruments

"Cognitive and Self-Management" uses "Policies", "Context", "Profiles", which are analysed later.

At this point, the definition of relationships and inverse relationships of the several classes without the intervention of the root class "Resilience" is shown (the relationships are shown in bold). Therefore:

- "Domain" **is attacked by** "Threats" (relationship) - "Threats" **attack** "Domain" (inverse relationship).
- "Means" **confront** "Threats" (relationship) - "Threats" **are confronted by** "Means" (inverse relationship)
- "Means" **are attacked by** "Threats" (relationship) - "Threats" **attack** "Means" (inverse relationship).
- "ThreatAgent" **performs** "Threats" (relationship) - "Threats" **are performed by** "ThreatAgent" (inverse relationship).
- "Domain" **is protected by** "Means" (relationship) - "Means" **protect** "Domain" (inverse relationship).

The previous classes and relationships are depicted in Figure 18.

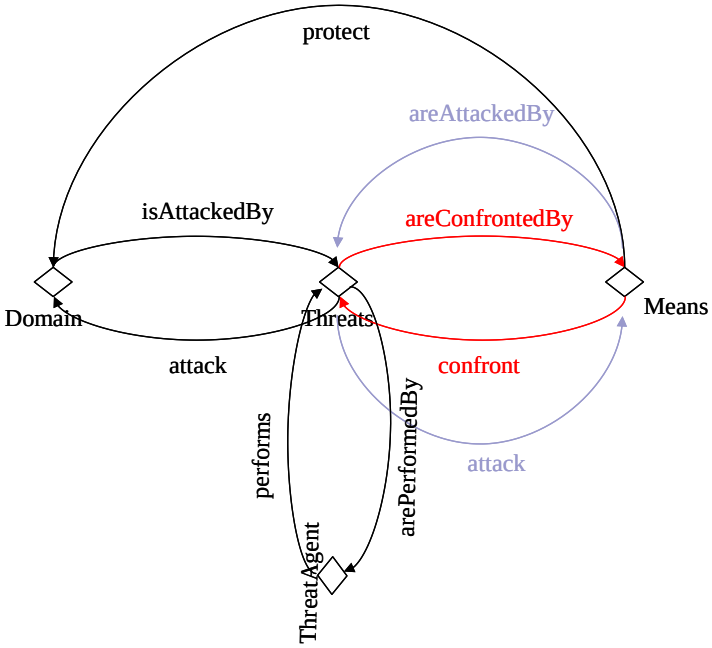


Figure 18: Resilience classes and relationships (without the intervention of class "Resilience")

Using the classes and relationships defined so far, an attempt will be made to combine them and see how they interact in an end-to-end resilience concept. By this way, interactions can be built such as the following examples:

- "Cognitive and Self-Management" **confronts** "changes" (e.g. context changes, traffic changes, KPI degradation) which **are performed by** "Human" (e.g. mobility, profile change) and which ("changes") **attack** "Network".
- "Risk Management" **confronts** "changes" (e.g. outstanding business plans) which **are performed by** "Human" (e.g. competition) and which ("changes") **attack** "Business".
- "Security Mechanisms" (e.g. protocols, DNSSEC) **confronts** "Security threats" which **are performed by** "Human" (e.g. malicious user) and which ("Security threats") **threaten** "Service" (e.g. DNS application) BUT "Security Mechanisms" (e.g. protocols, DNSSEC) **are threatened by** other "Security threats".

In order to build all these interactions, an analysis per domain will be followed.

6.2 Ontological examination of the Business Domain

NOTE: In this study, "Customer" is treated as a member of "Business" domain.

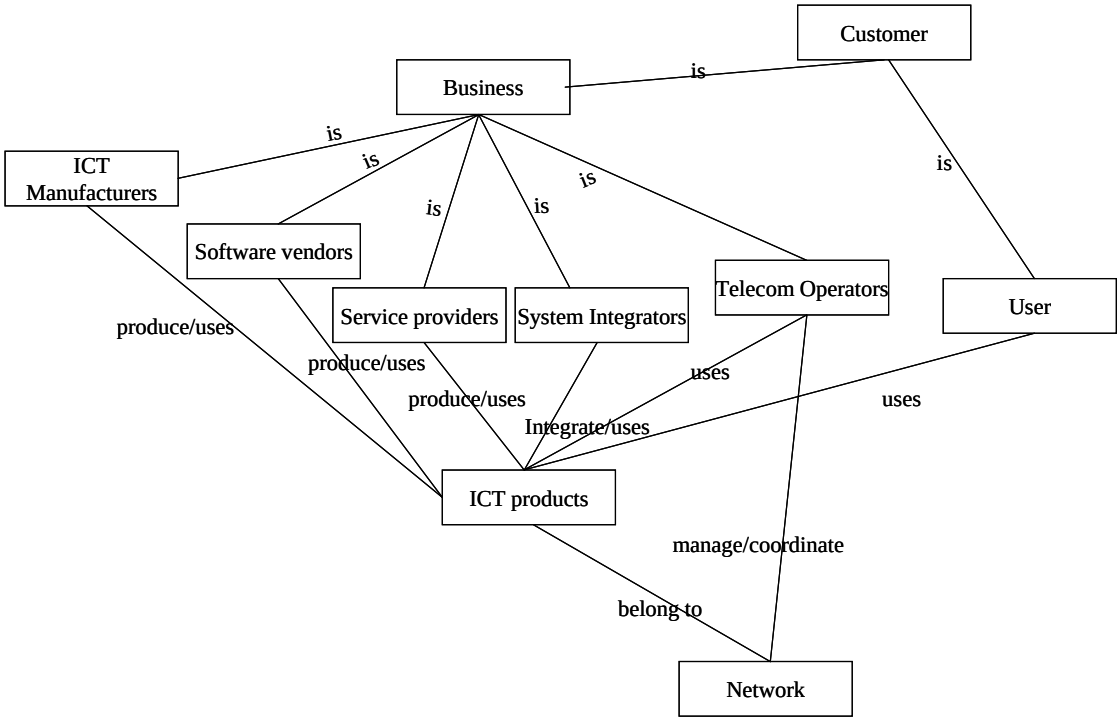


Figure 19: Business domain

First, the definition of business with respect to network resilience is investigated. As depicted in Figure 19, a business could be one of "ICT manufacturers", "Software vendors", "Service providers", "System integrators" or "Telecom operators". This set comprises the target audience of the derived resilience ontology, since they are the main stakeholders affected by resilience. Furthermore, the "Customer" domain may be a business and "User" is an instantiation of "Customer". The relationships of these businesses with the "ICT products" and "Network" domain are also presented.

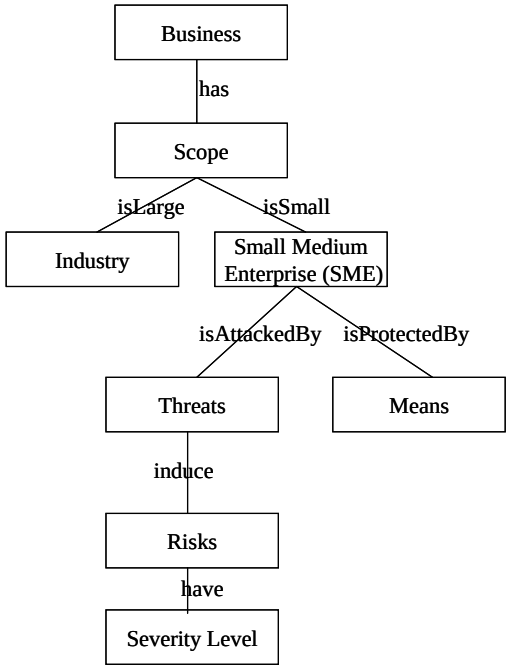


Figure 20: Business scope and risks

A business may have either a large or a small/medium scope (Figure 20). By this criterion, it may be distinguished to "Industry" and "Small Medium Enterprises" (SME). The relative impact of an attack will always depend to an extent on the defences of the thing under attack. As organisations grow and particularly as they diversify in their behaviour the risk presented by any one attack to the whole is reduced, whereas an organisation that remains small and focussed is much more susceptible to a focussed attack. Thus SMEs, when under attack would tend to exhibit higher risk than larger or more diversified industries.

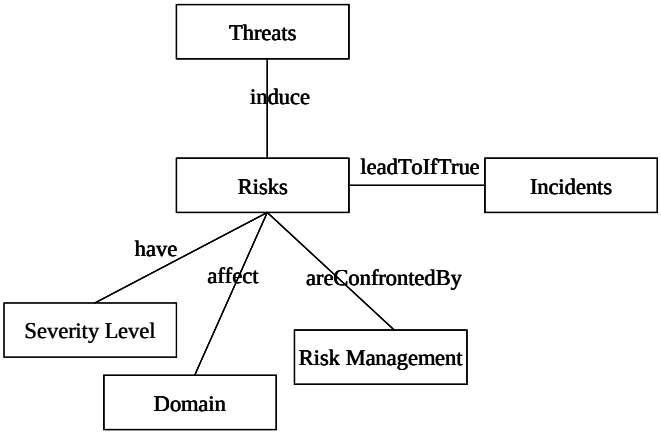


Figure 21: "Threats" and "Risks"

The "Risks" and the relationship with "Threats" are depicted in Figure 21 and "ICT products" are presented in Figure 22.

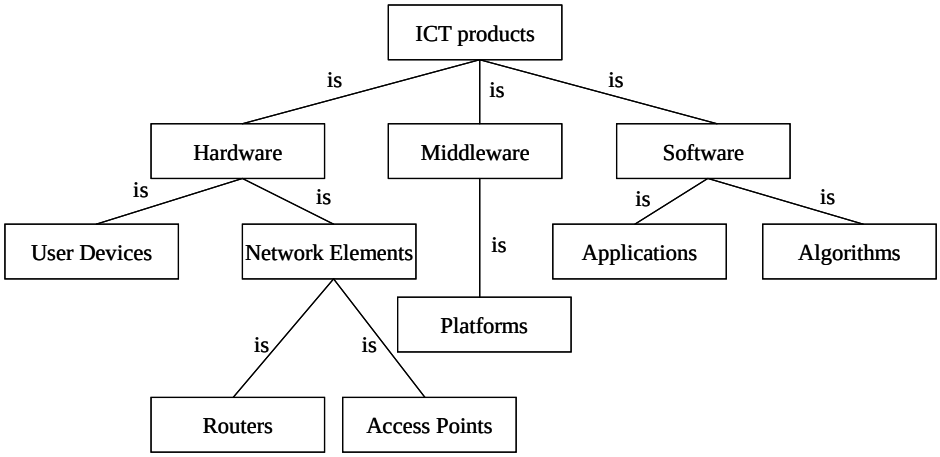


Figure 22: ICT products

The "Business" domain has mainly three kinds of "Threats", namely "Supply Chain Attacks", "Changes" in the business environment and "Interaction Conflicts" in the synergy with other businesses (Figure 23). "Supply Chain Integrity Means" confront "Supply Chain Attacks", while "Cooperation" between businesses helps confronting all these three kind of "Threats". "Cooperation" is a kind of "Means", which protects both "Business" and "Network" domain, since it confronts "Threats" corresponding to conflicting businesses and network assets, relatively.

NOTE: In the area of business development where a large market can only be served by many different manufacturers or operators cooperation through standardisation is often used to allow a market to develop. In some cases regulatory constraints also encourage standardisation such as for use of licensed radio spectrum or to prevent markets being dominated to the detriment of customers by single corporations.

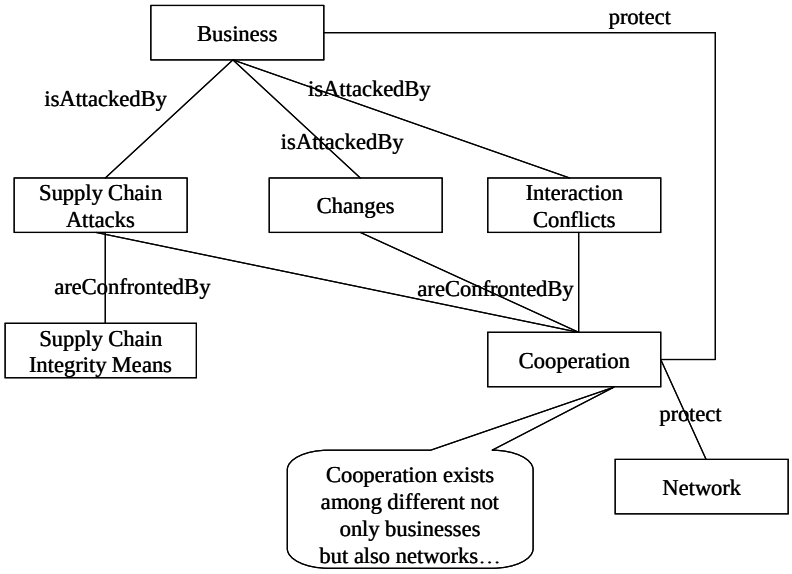


Figure 23: "Business" domain "Threats" and "Means"

6.3 *Ontological examination of the Network Domain*

"Network" is described in Figure 5. However, in Figure 24, the network domain is depicted according to Operator organization levels. First, in the top of the hierarchy, there is the Operational Support System (OSS) and the Business Support System (BSS). Then, Network Management System (NMS) follows, which controls one or more management domains. Each management domain has its Element Management System (EMS) that has the responsibility for some Network Elements. However, an NMS can directly control a Network Element with an incorporated EMS, that is with embedded capabilities. Network Elements were described in Figure 22.

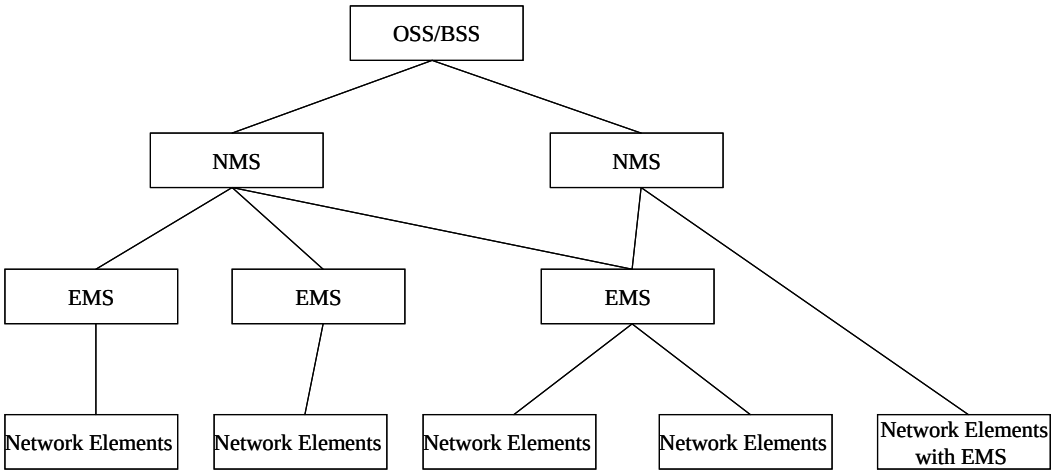
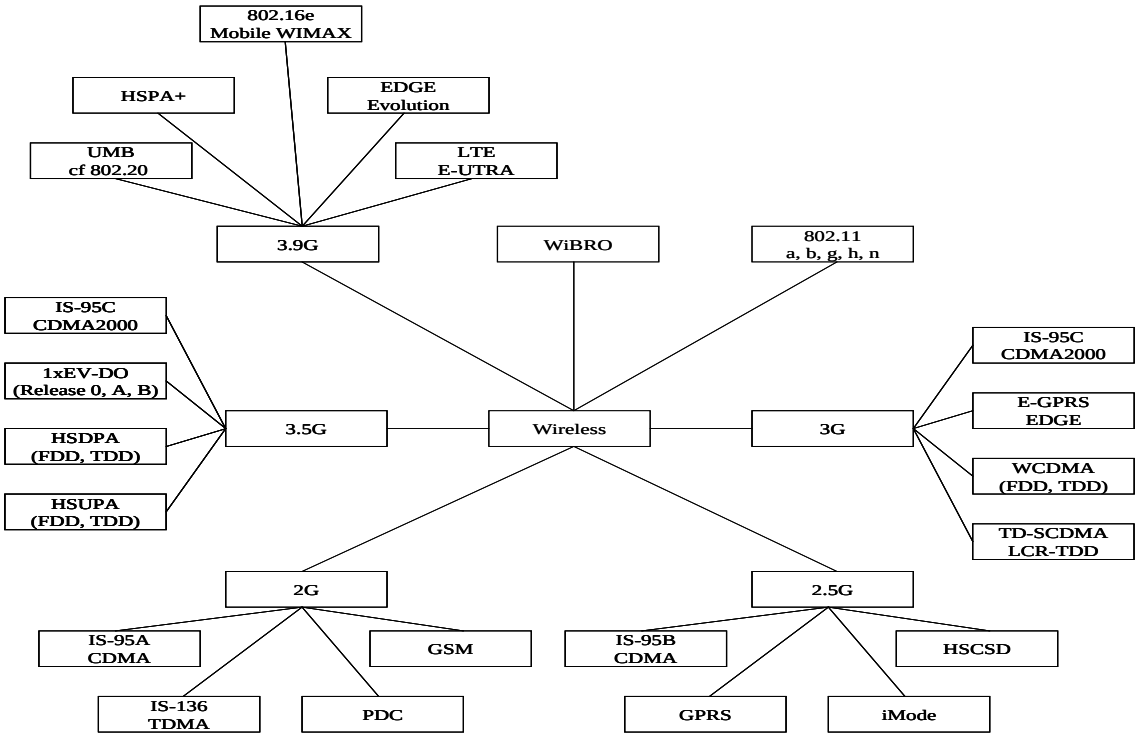


Figure 24: "Network" domain w.r.t. Operator organization levels

Another interesting aspect is presented in Figure 25, where all the wireless technologies used so far are depicted.



NOTE: The terms 2G, 2.5G, 3G, 3.5G and 3.9G are in common use but only 2G and 3G are officially recognised. 2G refers to those cellular networks that use digital transmission and that replaced the first generation of analogue cellular technologies (i.e. the AMPS and TACS systems) introducing security features including terminal authentication and encryption of the speech channel. 3G refers to the succeeding generation offering wider bandwidth than necessary for solely voice communication. The interim generations such as 2.5G by introducing GPRS to the GSM model moved from voice centric cellular communication to a model supporting data transmission. The interim extensions of 3G have in like manner extended the data carrying capacity of cellular networks by extensions of frequency band, channel bandwidth, and by extending the data encoding of bits per symbol increased the available data transmission rate.

Figure 25: "Wireless" access technologies

Figure 26 presents an example of a heterogeneous network and the role of "Cooperation" as the mean to federate and negotiate among the different networks.

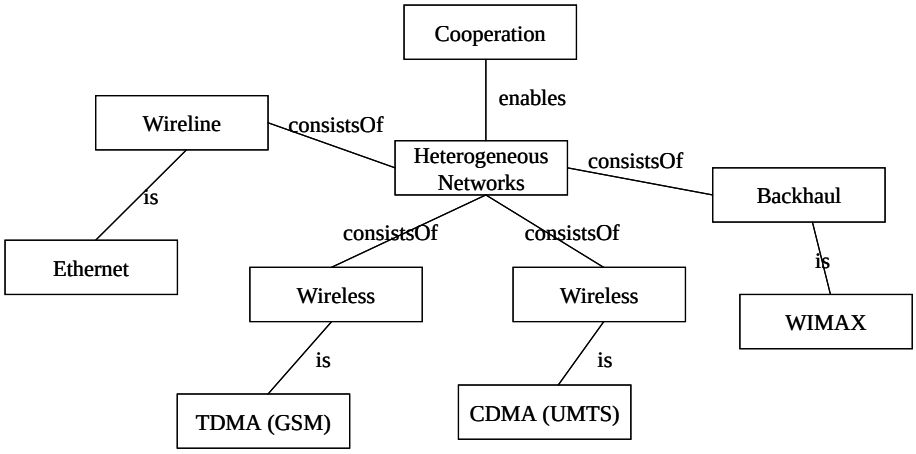


Figure 26: "Heterogeneous Networks"

In Figure 27, a description of "Network" domain "Threats" and "Means" is presented. The main "Threats" of "Network" are "Changes" (e.g. traffic changes, mobility pattern changes, KPI degradation, user profile changes) and "Interaction Conflicts" between network assets. The current and future trend of networks will be to have different network segments and even different networks (heterogeneous networks) to interact with each other. Moreover, some management functions, located into different network assets, may be conflicting. This case is enforced when autonomic functions are spread over the network layout (Self-Organizing Networks (SON)) but also over all the Operator organization levels. "Governance", "Cooperation" and "Cognitive and Self-Management" are the "Means" to confront both "Interaction Conflicts" and "Changes". "Governance" provides rules and policies to fix network instabilities caused by either "Changes" or "Interaction Conflicts". "Cooperation" resolves "Interaction Conflicts", but also helps confronting "Changes". Finally, "Cognitive and Self-Management" monitors the network, identifies any instability and triggers the appropriate actions. Therefore, it is the main self-diagnosis and self-healing mechanism. Furthermore, the learning capability enables to acquire knowledge, so that the next time similar trigger events will be confronted more immediately. "Trust Management" is a more horizontal process, encompassing all these means, although it is not included in Figure 27. This is because in such an environment with autonomic and self-x processes, there is an urgent need to build trust (trust in autonomics).

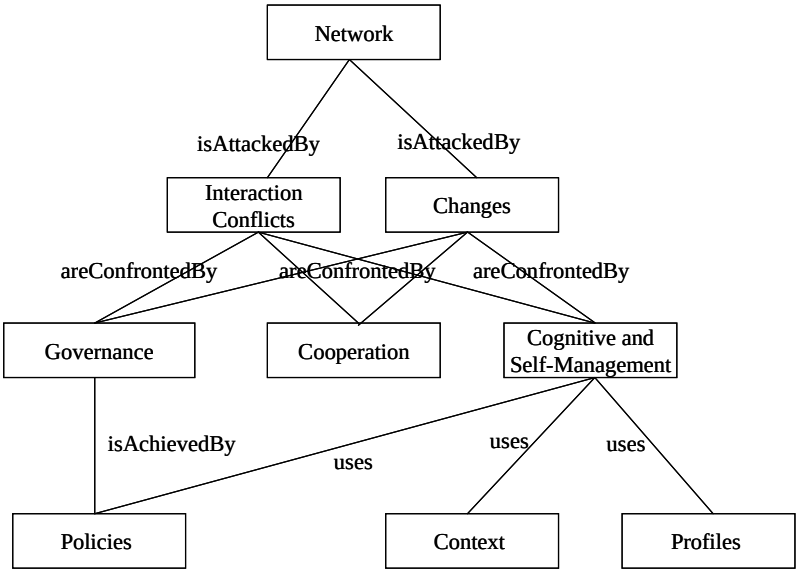


Figure 27: "Network" domain "Threats" and "Means"

"Cognitive and Self-Management" has some instruments, namely "Policies", "Context" and "Profiles" and "Governance" is achieved by "Policies". "Policies", "Context" and "Profiles" will be analyzed later. However, in Figure 28, the relationships among the functions of "Cognitive and Self-Management" (Figure 15) and "Policies", "Context" and "Profiles" are presented. In the functions of MAPE cycle, arrows are used to identify the direction of the information, that is when a relationship exists without an inverse relationship. "Monitor" feeds "Analyze" and "Learning" with data, acquired through the use of "Policies", "Context" and "Profiles". "Learning" builds knowledge, while "Analyze" analyzes/diagnoses the situation, derives the specific configuration policies and feeds "Plan". "Plan" is the decision making function, which decides also based on the knowledge, acquired so far by "Learning". "Plan" also feeds "Learning" with the decision, in order to build knowledge on what solution has been given to which problem for future use. Then, "Plan" orders the enforcement of the decision to "Execute". Finally, "Execute" feeds "Learning" about the enforcement result.

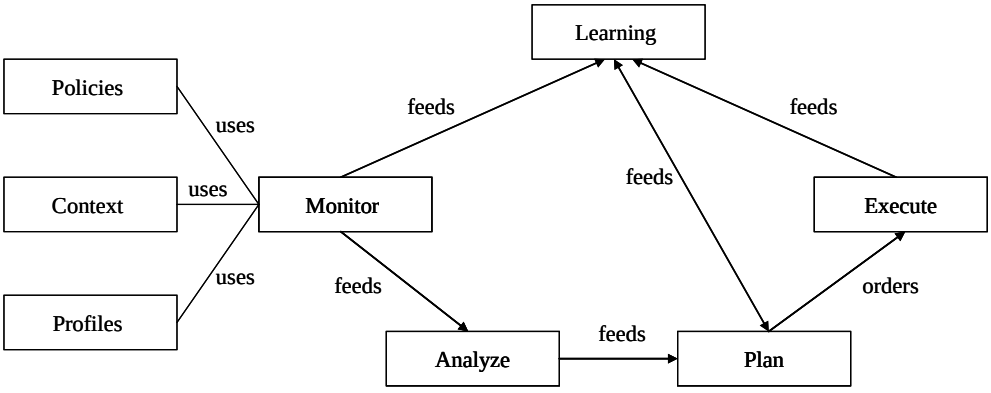


Figure 28: MAPE cycle functions and Policies, Context, Profiles

6.4 Ontological examination of the Service Domain

In Figure 29, the "Service" domain "Threats" and "Means" are presented.

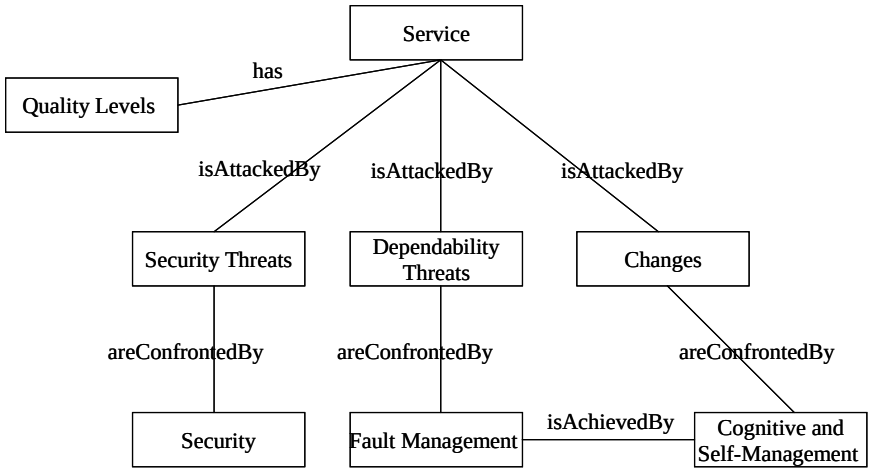


Figure 29: "Service" domain "Threats" and "Means"

"Service" domain has mainly three kinds of "Threats", namely "Security Threats", "Dependability Threats" and "Changes". The first two are depicted in Figures 12 and 13. "Security Threats" are confronted by "Security", using the instruments described in Figure 17. "Dependability Threats" are confronted by "Fault Management", which is depicted in Figure 14. "Changes" are confronted by "Cognitive and Self-Management", which is depicted in Figure 15 and achieves in an automatic way "Fault Management".

6.5 Ontological examination of the domain Information Exchange

This section describes in some detail the information exchanged between various components of a wireless communication network (WCN), i.e. user devices, Access Points and the Network Management System. The type of information exchanged between the components is first presented, followed by an overview of indicative interactions among the WCN components. This is categorised in Profiles, Context and Policies. The first two categories allow for the perception/awareness of users, devices, infrastructure elements and the networks status, while the third category facilitates governance of the network according to certain requirements or goals.

6.5.1 Profiles

NOTE: The material presented in this clause has close relationships with the work published by ETSI in the domain of User Profile Management (UPM) and in the domain of Universal Communications Identifier (UCI).

6.5.1.1 User Profile

The User Profile (Figure 30(a)) comprises information on the user subscription and user preferences regarding service provisioning. Such information includes the services that the user has subscribed to and the corresponding Quality of Service (QoS) levels for each of these

services. Moreover, the User Profile contains information on user preferences per Service and QoS level in the form of a so-called Utility value. This information is obtained and updated dynamically, following a process such as the one described in [i.13].

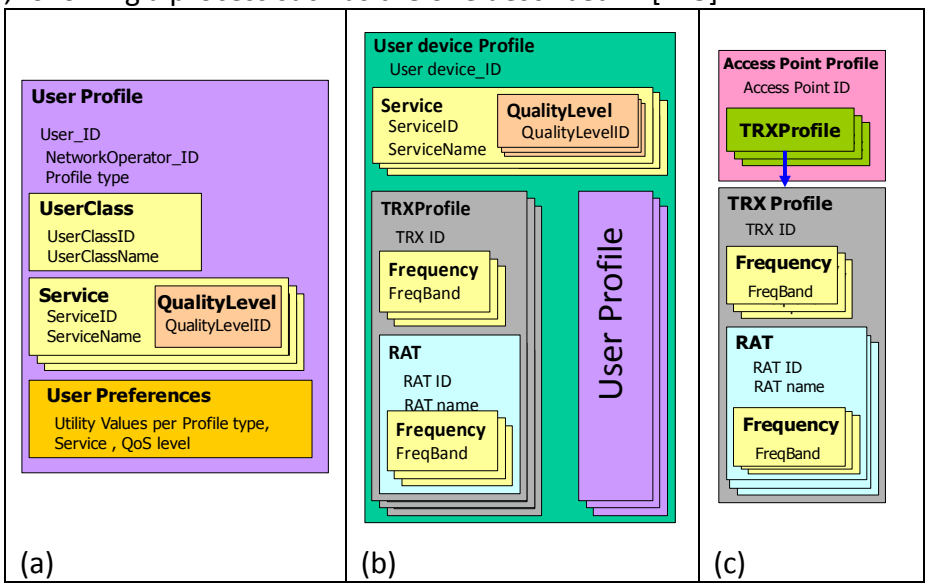


Figure 30: Profile information

6.5.1.2 User device Profile

The user device Profile (Figure 30(b)) comprises information regarding the capabilities of the device and is associated with a specific User Profile, i.e. of the user currently using the device. More specifically, the user device Profile includes the set of services that are supported by a specific device. Furthermore, it includes information on the number of transceivers (denoted as TRX in Figure 30) that the device can operate. Each transceiver (TRX) can operate at a set of RATs, at various frequencies.

6.5.1.3 Access Point Profile

This is similar to the user device Profile. An Access Point can comprise one or more reconfigurable Transceivers (TRXs) which can operate at various frequency bands and sets of RATs. Therefore the Access Point Profile (Figure 30(c)) comprises one or more TRX Profiles, which in turn include the details of a specific transceiver, i.e. its ID and information on the frequency bands and the RATs at which it can operate.

6.5.2 Context

6.5.2.1 User device Status

The user device functionality for deciding on the optimal device configuration takes into account policies as well as the information obtained through learning on context and user preferences and selects the optimal device configuration. In case this decision results in a modification of the configuration of the device (e.g. in terms of RAT, QoS level, Services, etc) the user device informs the network side (Access Point and/or CNMS) by sending a user

device Status message. The user device Status (Figure 31 (a)) contains information on the current configuration of the device, the running services, the active user profile and the most recently acquired preferences of the user of the device. Essentially, this is a sub-set of the user device Profile.

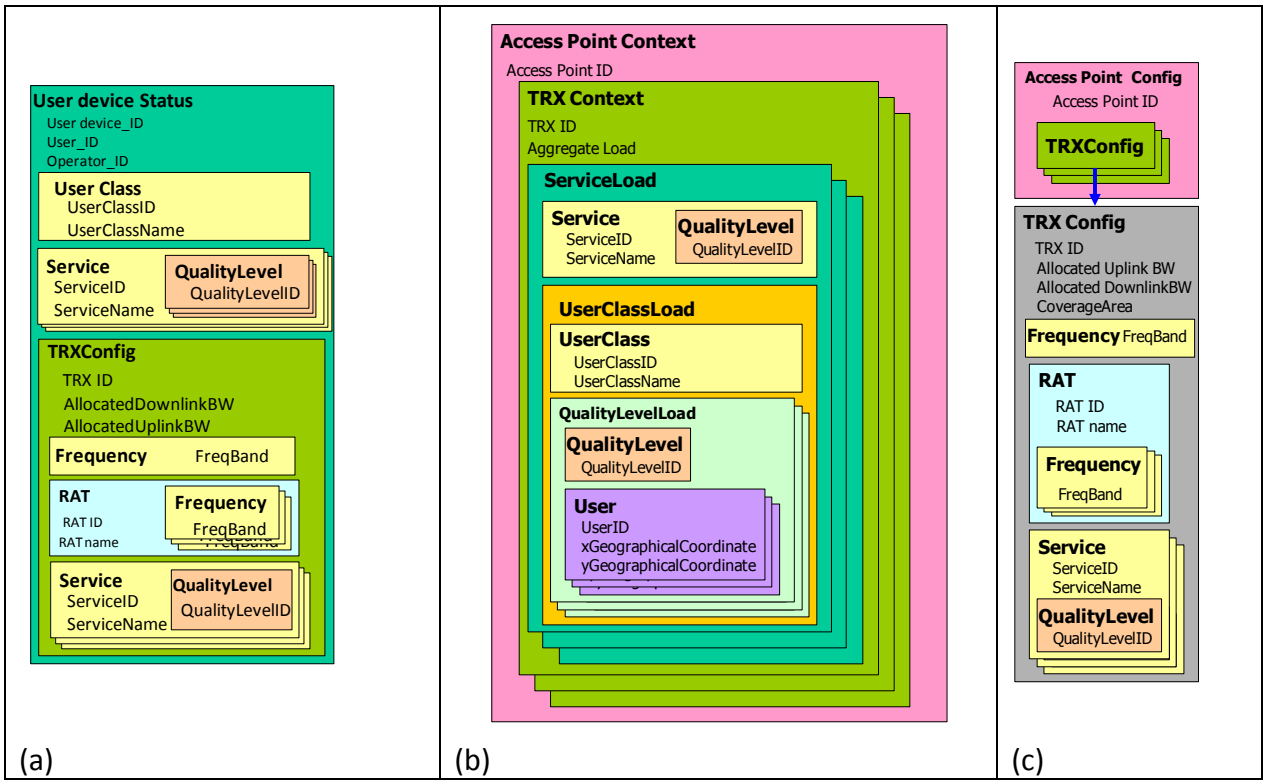


Figure 31: Context information

6.5.2.2 Access Point Context

This represents the context encountered by a specific Access Point. More specifically, it comprises information on the current load of each active transceiver of an Access Point (TRX Context in Figure 31 (b)), per User Class, Service and QoS level. This information is exploited for the decision making on the optimal configuration of a specific Access Point or a certain service area of the network.

6.5.2.3 Access Point Configuration

This information specifies the current configuration of an Access Point (Figure 31 (c)). In a way it represents a part of the Access Point profile that is currently activated. More specifically, the Access Point Configuration holds information on the transceivers that are (or should be) activated on a specific Access Point, the corresponding RATs and Frequency bands, and the services and QoS levels that can be supported (TRX Config).

6.5.3 Governance policies

6.5.3.1 Business level entries

Business level entries are information provided at the business level related to the number of users anticipated for an application, user class, in a certain location and time zone. In more detail, as can be observed in **Figure 32**, business level entries comprise information on the Number of users, the Traffic percentage, i.e. the number of concurrently active users anticipated, the Location (e.g. Piraeus, Athens-center, …), the Time Zone (e.g. 08:00-11:00, 21:00-22:00, …), the Application (e.g. IPTV, …), User Class (e.g. Gold, Silver, Bronze, …), Quality Level (e.g. High, Medium, Low), Quality level parameters (e.g. Bit rate, delay, jitter, …) and the Mobility pattern (e.g. High, low, train, car, …).

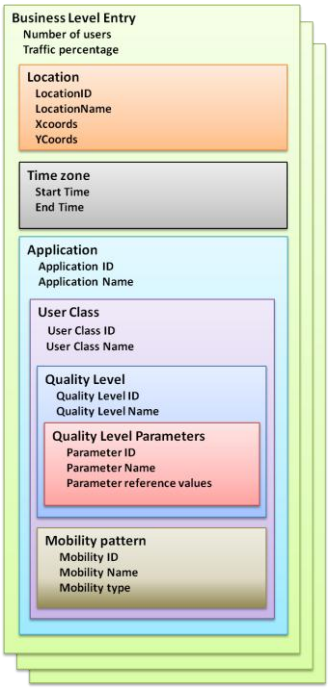


Figure 32: Business level entry structure

6.5.3.2 High-level policies (associations)

High-level policies/Associations specify rules related to the relationship of applications with user classes and quality levels, the relation of a certain application with other applications and the relations between user classes. As can be observed in Figure 33 an association comprises information on a set of applications. Each application may be associated with one or more User Classes. Each User Class may be associated with one or more QoS levels. Each QoS level is associated with one or more QoS parameters.

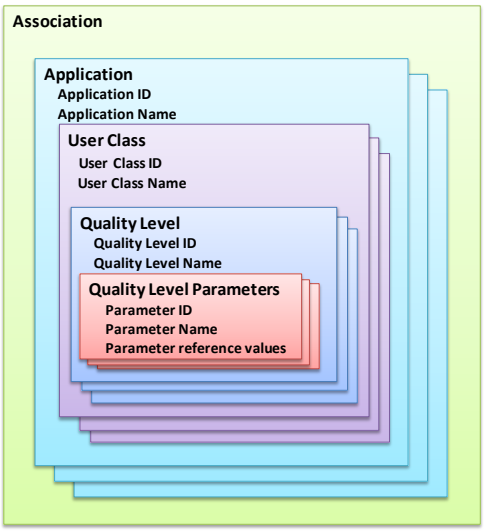


Figure 33: Structure of high-level policies (associations)

6.5.3.3 Configuration Policies

Configuration policies specify rules or constraints that should be taken into account for the selection of the optimal configuration of a service area, Access Point or Device. In this sense, configuration policies refine the set of information comprised in the Profiles and Context information. Configuration policies should be derived from business level entries and high-level policies/associations. A policy is formulated as a set of a Compound Policy Condition and a Policy configuration (Figure 34). A Compound Policy Condition comprises a Logical Expression (e.g. AND, OR, XOR) and one or more Compound Policy Conditions or Policy Conditions. A Policy Condition encompasses a Policy Expression (e.g. "equals", "greater than", "greater equal", and "less than", "less equal", etc) and a Policy Argument. A Policy Argument includes User Class, Location, and Time zone information and basically indicates the devices that are affected by the specific policy. A Policy Configuration indicates the RATs that can be operated by transceivers of Access Points, as well as certain frequency bands per RAT in a certain service area. Moreover it also may specify the services and corresponding QoS levels that can be provided over certain RATs.

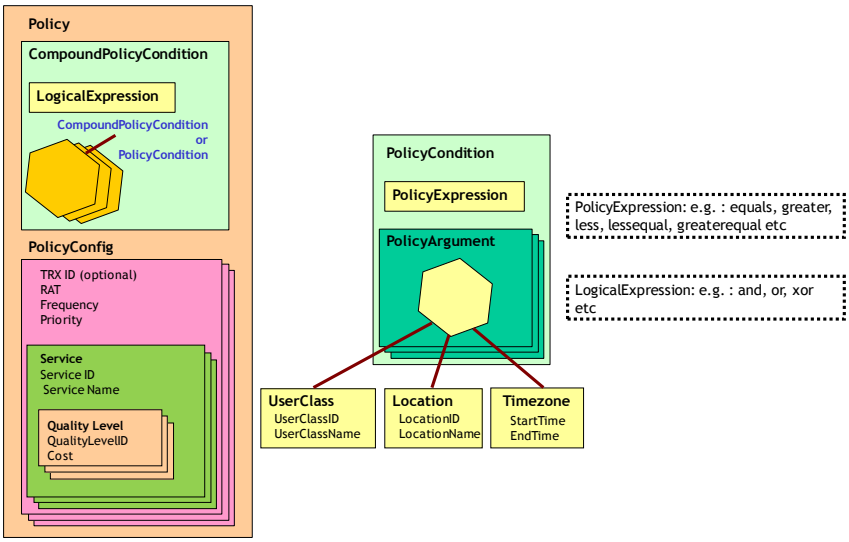


Figure 34: Configuration Policies structure

7 Next steps

7.1 Standardisation

It has been suggested that a goal of this document is to encourage the use of ontologies in standards development and in particular for the definition of approaches in standards to provide resilience as a core attribute of a system. It is not suggested that ontologies and taxonomies replace the existing approaches to developing standards but rather that the approach outlined in this report is used to augment existing best practices.

The aim of standards developed in most SDOs is to achieve interoperability and interworking of many different approaches to implementation. The approach defined in TR 187 011 is indicative of best practice in this regard but when extended by use of tools such as message sequence charts, validated state machines, formally specified data objects (say by using ASN.1) many of the aims of ontologies and taxonomies to achieve shared understanding will already have been met.

Where ontologies and taxonomies have greatest impact is in the specification of shared understanding where the context is unclear and it has been shown that these tools may be used as a stepping stone to achieving that shared understanding. Therefore it is recommended that further work is done to ensure that the methods for standardisation are extended to include the use of taxonomy and ontology. This should address the work of ETSI's Methods for Testing and Specification (MTS) group in particular.

In terms of standardisation it is not clear if either a taxonomy or an ontology will become normative as its purpose is to gain shared understanding as such it is proposed that such techniques are used primarily in the context of informative or guidance documents (i.e. ETSI Technical Reports, ETSI Guides).

7.2 Other ontologies and taxonomies in support of resilience

The bulk of this report has examined and decomposed the ontology of resilience and has along the way had to consider ontologies and taxonomies for security analysis, and the interaction of business with ICT but in order to address resilience some of these avenues have been uncovered but not explored. It is therefore recommended that rather than leaving these incomplete and unexplored that further work is undertaken (for example by standardisation bodies) to complete these with a view to closing the gaps in ontological understanding.

Annex A: References and bibliography

The following referenced documents are cited in the main body of the text or have been added by the authors as essential background for readers in interpretation or achieving further insight to the topics raised in the main body of the text.

Cited references

[1] 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/

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

[3] ENISA study: "Gaps in standardisation related to resilience of communication networks", 2009. http://www.enisa.europa.eu/act/it/library/deliverables/gapsstd

[4] ENISA study: "Priorities for Research on Current and Emerging Network Technologies ", 2010. http://www.enisa.europa.eu/act/it/library/deliverables/procent

[5] ENISA study: "Enabling and managing end-to-end resilience", 2011. http://www.enisa.europa.eu/act/it/library/deliverables/e2eres

[6] ENISA study: "Resilience Metrics and Measurements: Technical Report", 2011. http://www.enisa.europa.eu/act/res/other-areas/metrics/reports/metrics-tech-report

[7] Flynn MJ, Very High-Speed Computing Systems, Proceeding of the IEEE, 54(12), December 1966, p1901-1909

[8] Lee W Lacy: "Owl: Representing Information Using the Web Ontology Language", ISBN-10: 9781412034487, ISBN-13: 978-1412034487, ASIN: 1412034485; ASIN: B000PY45UW

[9] Andrew Cox, Fynnwin Prager, Adam Rose: "Transportation security and the role of resilience: A foundation for operational metrics" Transport Policy Volume 18, Issue 2, March 2011, Pages 307-317

[10] Mike Uschold and Michael Gruninger, "Ontologies: principles, methods and applications", *The Knowledge Engineering Review,* Vol. 11:2, 1996, 93-136.

[11] J. Li, S. Liu, Z. Lin, C. Wen, "A Real-Time Information Gathering Agent Based on Ontology", Advances in Web-Age Information Management, Lecture Notes in Computer Science, 2004, Springer, pp. 696-701

[12] J.O. Kephart and D.M. Chess, "The Vision of Autonomic Computing", In: IEEE Computer 36 (2003), No 1, pp. 41-50

[13] Ganek AG and Corbi TA, "The dawning of the autonomic computing era", IBM System Journal 2003; 42(1).

[14] IBM Corporation, "Automating problem determination: a first step towards self-healing computer systems", www.research.ibm.com/autonomic, 2003

Bibliography

[i.1] Algirdas Avižienis, Jean-Claude Laprie, Brian Randell and Carl Landwehr, "Basic concepts and taxonomy of dependable and secure computing", *IEEE Transactions of Dependable and Secure Computing*, Vol. 1, No. 1, Jan-Mar 2004, pp. 11–33.

[i.2] Jean-Claude Laprie, "From Dependability to Resilience", *LAAS-CNRS — Université de Toulouse — 7, Avenue Colonel Roche 31077 Toulouse, France* laprie@laas.fr.

[i.3] T. Anderson (Ed.), "Resilient Computing Systems", Collins, 1985.

[i.4] Jean-Claude Laprie, "Resilience for the Scalability of Dependability", in *Proceedings of the 2005 Fourth IEEE International Symposium on Network Computing and Applications (NCA'05)*, 2005.

[i.5] ReSIST project website, http://www.resist-noe.org/overview/summary.html.

[i.6] ReSIST project, Deliverable D34: Resilience ontology: final, December 2008.

[i.7] V. Stavroulaki, N. Koutsouris, K. Tsagkaris, P. Demestichas, "A Platform for the Integration and Management of Cognitive Systems in Future Networks", in *Proc. IEEE International Workshop on Management of Emerging Networks and Services (MENS) – IEEE GLOBECOM 2010 Workshop on Management of Emerging Networks and Services,* Miami, Florida, USA, 6th -10th Dec 2010.

[i.8] Rubén Darío Franco, Guillermo Prats, Rubén de Juan-Marín, "An Ontology Proposal for Resilient Multi-plant Networks", *Enterprise Interoperability IV*, Part III, pp. 169-178, Springer 2010.

[i.9] REMPLANET project website, http://www.remplanet.eu/web/

[i.10] Xiangyang Li, Charu Chandra, Jiun-Yan Shiau, "Developing Taxonomy and Model for Security Centric Supply Chain Management", *International Journal of Manufacturing Technology and Management*, Vol. 17, No.1/2, pp. 184 - 212, 2009

[i.11] V. Stavroulaki, Y. Kritikou, P. Demestichas, "Acquiring and learning user information in the context of cognitive device management", In Proc. IEEE International Conference on Communications 2009 (ICC 2009), Dresden Germany, June 2009

[i.12] Cox, A., Prager, F., & Rose, A. (2011). Transportation security and the role of resilience: A foundation for operational metrics Transport Policy, 18 (2), 307-317 DOI:10.1016/j.tranpol.2010.09.004

[i.13] http://www.greenchameleon.com/gc/blog_detail/defining_taxonomy/

NOTE: The Taxonomies & Controlled Vocabularies Special Interest Group (SIG) is a networking and educational forum for those in the indexing profession who are involved in creating or editing taxonomies, thesauri, or controlled vocabularies used for indexing. The Taxonomies & Controlled Vocabularies SIG is an affiliate of the American Society for Indexing.

[i.14] G.C. Bowker and S.L. Star. *Sorting things out: classification and its consequences*. Cambridge, MA: MIT Press, 1999. Role of categories and standards in shaping the modern world.

[i.15] J. Bryar. "The Value of organized knowledge." *CMS Watch* (January 1, 2002) Last checked 11/16/08.

[i.16] R. Cover. "Resource description and classification." OASIS, last modified February 12, 2003. Last checked 11/16/08. Collection of references on matters of Subject Classification, Taxonomies, Ontologies, Indexing, Metadata, Metadata Registries, Controlled Vocabularies, Terminology, Thesauri, Business Semantics. Part of the XML Cover Pages.

[i.17] T. Craven. "Thesaurus Construction." London: University of Western Ontario, last updated January 25, 2008.

[i.18] M. Denny. "Ontology Tools Survey, Revisited." XML.com (July 14, 2004)

[i.19] B. Doyle. "TaxoTips: Resources to help with your taxonomies and controlled vocabularies."

[i.20] S. Dumais and H. Chen. "Hierarchical classification of web content." *Proceedings of SIGIR 2000*, pp. 256-263.

[i.21] "Information intelligence: Content classification and enterprise taxonomy practice." Delphi Group. 2004.

[i.22] H. Hedden. *The Accidental taxonomist*. Medford, NJ: Information Today, 2010.

[i.23] P. Lambe. *Organising knowledge: Taxonomies, knowledge and organisational effectiveness*. Oxford: Chandos Publishing, 2007.

[i.24] B. Lutes. "Web thesaurus compendium." Last modified June 1999. Last checked 11/16/08.

[i.25] L. Ramos. "Taxonomy, thesaurus, tagging: Balancing automation and editorial review." Giga Information Group, March 2002. Provides excellent definitions of these terms.

[i.26] S.L. Roberts-Witt. "Practical taxonomies." *Knowledge Management* (January 1999) p. 46-54.

[i.27] "Taxonomy & content classification: market milestone report." Delphi Group. 2002.

[i.28] "Ten taxonomy myths." The Montague Group. (Nov. 2002)

[i.29] A. Warner. "A taxonomy primer." Ann Arbor, Mich: Lexonomy, 2002.

Annex B: Definitions and abbreviations

Definitions

For the purposes of the present document, the following terms and definitions apply:

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 (from ISO/IEC 13335-1)

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

Identifier: series of digits, characters and symbols used to identify uniquely subscriber, user, network element, function or network entity providing services/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 to the loss of capacity of a failure or foreseen overload, optimizing the availability and quality of service of telecommunications systems and support resources 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.

NOTE 2: A **Threat** is enacted by a **Threat Agent**, and may lead to an **Unwanted Incident** breaking 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

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, is modelled as the combination of a **Weakness** that can be exploited by one or more **Threats**.

Abbreviations

For the purposes of the present document, the following abbreviations apply:

BSS	Base Station Subsystem
CDMA	Code Division Media Access
DNSSEC	Domain Name System Security
ECN&S	Electronic Communication Networks and Services
ENISA	European Network and Information Security Agency
ETSI	European Telecommunications Standardisation Institute
FDMA	Frequency Division Media Access
ICT	Information and Communication Technology
IPTV	Internet Protocol Television
IPv6	Internet Protocol version 6
MIMD	Multiple Instruction Multiple Data
MISD	Multiple Instruction Single Data
MPLS	Multi-Protocol Label Switching
NGN	Next Generation Networks
NO	Network Operator
OFDMA	Orthogonal Frequency Division Media Access
QoS	Quality of Service
RAT	Radio Access Technology
SDH	Synchronous Digital Hierarchy
SDO	Standards Development Organisation
SIMD	Single Instruction Multiple Data
SISD	Single Instruction Single Data
SM	Shared Memory
SME	Small or Medium Enterprise
SM-R	Shared Memory - Read
SM-RW	Shared Memory – Read Write
SM-W	Shared Memory - Write
SRKB	Shared Re-usable Knowledge Bases
TDMA	Time Division Media Access
TETRA	Terrestrial Trunked Radio
TRX	Transceiver
TVRA	Threat Vulnerability and Risk Analysis

Annex C: Existing taxonomies in resilience

This annex contains the results of a routine search of existing papers in the field with a view to find the terms "taxonomy" and "resilience".

NOTE: The references are shown in annex A that came out of a simple search.

The development of taxonomies has been the source of much debate and many instances has led to scientists falling out for many years. Traditionally taxonomy development has been on the basis of shared characteristics with more modern taxonomy development, particularly in biology, development has been based by classification based on evolutionary descent. The latter approach is best characterised by modern biological classification and shown in Table C1 with examples of using the classification schema.

Table C.1: Classification examples from biology

Taxon	Example – Modern man		Example – domestic horse	
Kingdom	Animalia	Animals	Animalia	Animals
Phylum	Chordata (subphylum Vertebrata)	Animals with a backbone	Chordata (subphylum Vertebrata)	Animals with a backbone
Class	Mammalia	Mammals	Mammalia	Mammals
Order	Primates	Primates	Perissodactyla	Odd-toed ungulates
Family	Hominidae	Hominids	Equidae	Horse-like mammals
Genus	Homo	Humans	Equuus	Horses and their kin
Species	Homo sapiens.	Modern human	Equus ferus caballus	Domestic horse

In computing the first major taxonomical classification was made by Flynn [] and consisted of 4 categories following the rule of classification by shared characteristics:

- SISD: Single Instruction Single Data
- SIMD: Single Instruction Multiple Data
- MISD: Multiple Instruction Single Data
- MIMD: Multiple Instruction Multiple Data

These have been extended for each of the MIMD and SIMD classes with the additional categories listed below:

- SM-R: shared memory multiple reads to same location allowed
- SM-W: shared memory multiple writes to same location allowed
- SM-RW: shared memory, both multiple reads and writes allowed
- SM: shared memory, both multiple reads and writes disallowed
- TC: tightly coupled

- LC: loosely coupled
- UC: uncoupled

This approach reinforces a classification of shared characteristics.

In the area of transport a number of taxonomies have been written with a view to improvement of response to terrorist threats as considered by Cox et al [9]. Resilience is considered in this area as having two dimensions: Static; and, Dynamic.

Annex D: Existing ontologies in resilience

This annex contains the results of a routine search of existing papers in the field.

NOTE: The references are shown in annex A that came out of a simple search.

In [i.3], the main definitions relating to dependability and security are first given. Dependability is examined with regard to such attributes as reliability, availability, safety, integrity, maintainability, etc., while security brings in concerns for confidentiality. After these basic definitions, the threats to dependability and security (faults, errors, failures), their attributes, and the means for their achievement (fault prevention, fault tolerance, fault removal, fault forecasting) are addressed. The major part of this analysis is given in the form of ontologies. These dependability and security ontologies intend to explicate a set of general concepts, of relevance across a wide range of situations and, therefore, helping communication and cooperation among a number of scientific and technical communities, including ones that are concentrating on particular types of system, of system failures, or of causes of system failures. In this concept, the defined ontologies are also concerning resilience, since dependability and security are prerequisites for resilience.

The major new contributions of [i.3] with regard to existing literature, as summarised by the authors, are:

- The relationship between dependability and security is clarified.
- A quantitative definition of dependability is introduced.
- The criterion of capability is introduced in the classification of human-made nonmalicious faults, enabling the consideration of competence.
- The discussion of malicious faults is extensively updated.
- Service failures are distinguished from dependability failures: The latter are recognized when service failures over a period of time are too frequent or too severe.
- Dependability issues of the development process are explicitly incorporated into the taxonomy, including partial and complete development failures.
- The concept of dependability is related to dependence and trust, and compared with three recently introduced similar concepts, including survivability, trustworthiness, high-confidence systems.

Moreover, the authors state that the major strength of the concept formulated in [i.3] is its integrative nature, which enables the more classical notions of reliability, availability, safety, confidentiality, integrity, and maintainability to be put into perspective. The fault-error-failure model is central to the understanding and mastering of the various threats that may affect a system, and it enables a unified presentation of these threats, while preserving their specificities via the various fault classes that can be defined. The model provided for the

means for achieving dependability and security is extremely useful, as those means are much more orthogonal to each other than the more classical classification according to the attributes of dependability, with respect to which the development of any real system has to perform tradeoffs since these attributes tend to conflict with each other. Finally, the refinement of the basic definitions leads to a refined dependability and security tree.

Concerning what is intended to be done as future elaboration of [i.3], the authors identify six main points:

- Expanding the discussion of security, for example to cover techniques for protecting confidentiality, establishing authenticity, etc.
- Analyzing issues of trust and the allied topic of risk management.
- Searching for unified measures of dependability and security.
- New technologies (nanosystems, biochips, chemical and quantum computing, etc.) and new concepts of man-machine systems (ambient computing, nomadic computing, grid computing, etc.) will require continued attention to their specific dependability issues.
- The problems of complex human-machine interactions (including user interfaces) remain a challenge that is becoming very critical—the means to improve their dependability and security need to be identified and incorporated.
- The dark side of human nature causes to anticipate new forms of maliciousness that will lead to more forms of malicious faults and, hence, requirements for new defences as well.

In [i.4], the definitions of resilience and the technologies for resilience are introduced. According to the authors' view, the adjective "resilient" has been in use for decades in the field of dependable computing systems, essentially as a synonym of "fault-tolerant", thus generally ignoring the unexpected aspect of the phenomena the systems may have to face. A noteworthy exception is the preface of [i.5], which says: "The two key attributes here are dependability and robustness. […] A computing system can be said to be robust if it retains its ability to deliver service in conditions which are beyond its normal domain of operation". Fault-tolerant computing systems are known for exhibiting some robustness with respect to fault and error handling, in the above sense, i.e., for situations exceeding their specification.

A total change of scale is needed when moving to the future large, networked, evolving systems constituting complex information infrastructures — perhaps involving everything from super-computers and huge server "farms" to myriads of small mobile computers and tiny embedded devices. Such systems are in fact the dawning of *ubiquitous systems*, with which, what is at stake is to maintain dependability, i.e., the ability to deliver service that can justifiably be trusted, in spite of continuous changes.

In this concept, [i.4] intends to make the step from dependability to resilience by considering not only the fault but also the change tolerance and adaptation. Therefore, the definition of resilience builds on the definition of dependability with the insertion of facing changes in addition to faults and errors confrontation. So, briefly, resilience is seen as the persistence of dependability when facing changes. A classification of changes and a respective diagram is given. It is also emphasized, in the context of dependability that the changes can concern, or induce changes in the threats the system is facing. Moreover, the changes can themselves turn into threats, as in the case of mismatches between the modifications that implement the changes and the former status of the system. Finally, the relationship between the technologies for resilience, namely evolvability, assessability, usability, diversity, and the means for dependability, that means fault prevention, fault tolerance, fault removal, fault forecasting, is depicted.

Furthermore, in [i.6], the relationships among the changes, resilience scalability properties and resilience scaling technologies, i.e. technologies for resilience, are depicted through an ontology diagram. The concept is as follows. Accommodating functional, environmental and technological changes at a satisfactory level of dependability and security induces the need for scalability, which in turn drives the requirement for resilience policies, algorithms and mechanisms to be extensible, composable, adaptive, and consistent with respect to the assumed threats. The satisfaction of these scalability properties clearly requires that the resilience policies, algorithms and mechanisms are evolvable, assessable, usable and diverse.

The work reported previously in [i.4] has been performed in the framework of the European Network of Excellence ReSIST (Resilience for Survivability in Information Society Technologies). ReSIST [i.7] addresses the strategic objective "Towards a global dependability and security framework" of the 6th Work Programme, and responds to the stated "need for resilience, self-healing, dynamic content and volatile environments". It has integrated leading researchers active in the multidisciplinary domains of Dependability, Security, and Human Factors, in order that Europe has a well-focused coherent set of research activities aimed at ensuring that future "ubiquitous computing systems", the immense systems of ever-evolving networks of computers and mobile devices which are needed to support and provide Ambient Intelligence (AmI), have the necessary resilience and survivability, despite any residual development and physical faults, interaction mistakes, or malicious attacks and disruptions.

The objective of ReSIST project, as denoted in [i.8], a public document of ReSIST, named "Resilience ontology: final", intends to create a structured representation of the resilience concepts, in the form of a thesaurus and an ontology, which is to be able to use natural language processing tools to perform computer-aided identification and classification of existing documents concerned with resilience and to classify new documents as they are generated. More explicitly, a hierarchical thesaurus is first created based on the terminology extraction, then the thesaurus is employed to do automatic indexing of documents, followed by the identification of a number of clusters by means of automatic clustering analysis, and finally the resulting from the thesaurus final ontology will be compared with the ontology existing in [i.3]. Resilience in [i.8] is defined as "the persistence of dependability in the

presence of changes" in consistency with [i.4]. However, the term "dependability" is used as an abbreviation for the definition given above, that is, for "resilience".

With respect to resilience ontology, an effort to create an ontology corresponding to [i.3], within the ReSIST activity, is initially carried out in [i.8]. The first analysis of the ontology in [i.3] dealing with the various types of faults, conducted by ReSIST, has instantly revealed that this hierarchy contained almost no multiple inheritance, i.e., that the sub-fault relationship spanned a tree rather than a graph. This results in an inappropriate and sometimes misleading categorization of faults. Concerning the categorization of faults, [i.3] accounts for eight basic viewpoints (whose possible combinations lead to 31 fault classes), which lead to various overlapping groupings. A more detailed investigation of the distribution of potential faults with respect to their viewpoints showed that this ontology implicitly encodes several subsets, that is sub-fault relationships. Therefore, a new resulting fraction of the fault hierarchy is proposed in [i.8], which explicitly considers some of the sub-fault relationships that [i.3] misses. Since every knowledge-aware processing method can only take explicitly modelled (or implicit but entailed) facts into account, it is important to represent even the supposedly obvious.

The ENISA report on gaps in standardisation related to resilience of communication networks [3] summarises and presents the following key elements:

- the definition applied to resilience in the context of standardisation,
- the identification and presentation of the major activities undertaken in the standards developing organizations (SDOs) in either security or architecture that have a focus on resilience,
- 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, in light of the current lack of specific activity on resilience as identified in the SDOs,
- the provision of recommendations for future standardisation activities.

In this context, several isolated ontologies for resilience are introduced in the report. The first ontology is given when discussing resilience against a network model, which derives from the security analysis of systems under attack. Therefore, the electronic communications networks and services (ECN&S) model is considered alongside the model of systems under attack, i.e. the generic system security and attack model, 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. 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 the report to explicitly consider only those aspects that impact resilience as a composite of the typical security objectives. Thus, the ITU-T

ontological model of cyber security stressing resilience is depicted, where a resilient infrastructure is one of the protection measures in the cyber security model.

Other resilience ontologies are given when identifying the requirements for a taxonomy covering metrics and risk categorisation to be applied to resilience. Firstly, an illustration of a threat hierarchy is presented as an alternative model for considering both ontologies and taxonomies. Then, an ontology of cyber-security, identified by the ITU-T and ETSI in TR 187 010, is illustrated and simplified, 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. 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. In this scope, a model illustrating the metrics, used to express system resilience, is presented. Finally, when referring to the theory of network resilience and basically identifying the areas of interest for the SDOs, a hierarchical taxonomy of Hazards is given.

Another report for ENISA [2] is evaluating the effectiveness of three key technologies, namely IPv6, DNSSEC, and MPLS, in improving the resilience of public eCommunication networks. This study analyses the characteristics of those technologies and highlights their effect on the resilience of the network. An overview of the characteristics of IPv6, DNSSEC, and MPLS is given, and the resilience assisting features, as well as other properties that one has to aware of to make an educated decision about their deployment are enumerated. When studying resilience provided by DNSSEC, an ontology model presents the main threats against DNS. The points shown on the left side of the model are discussed in more detail, while security issues on the right side cannot be addressed by DNSSEC.

At a network level, [i.9] presents an open, scalable platform for the integration and management of cognitive systems (IMaCS) that aims at both comprising various cognitive management schemes, thus enabling efficient end-to-end operation, and abstracting the complexity of the underlying infrastructure. The success of future generation networks will be driven by the provision of ubiquitous, personalized services that can offer an enhanced user experience. In order to support the provision of more and better services to users, and at the same time deal with the complexity of the infrastructure of network operators (NOs), advanced management functionality needs to be introduced in wireless systems, both on the network as well as on the user device side, which will enable optimum, end-to-end operation.

In this direction, the IMACS platform introduces cognitive and self-management features in the B3G world, with the aim of evolving current heterogeneous wireless system infrastructures into an integrated, efficiently managed and scalable framework. Based on the features of cognitive systems, cognitive systems can determine and configure their operation not only in a reactive manner, i.e. responding to the detection of problematic situations, but also proactively, so as to prevent issues undermining the optimal system function. In this manner, cognitive management is an ideal mechanism in order to achieve network resilience.

The information flow, presented in [i.9], has been formulated as ontology. This ontology gives many advantages. Firstly, it offers interoperability and a shared vocabulary, which is crucial for the integration of the different, proprietary, implemented platforms and test beds and for smoothing the progress of introducing various cognitive schemes in future networks. This possibility is enforced since the implementation of a ubiquitous communications environment entails a great complexity of the underlying infrastructure that increases as networking technologies continue to evolve and new ones emerge. Secondly, the ontology can be easily extended or modified, which facilitates the integration of various software and hardware components and thus allows the realization of validation, exploitation and demonstration activities in a wide range of test cases and application areas. Future work plans include the refinement and extension of the information flow ontology as well as the enhancement of "plug and play" features.

In [i.10], an ontology proposal for the REMPLANET FP7 project [i.11], which aims at developing methods, guidelines and tools for the implementation of the Resilient Multi-Plant Networks in non-hierarchical manufacturing networks, characterized by non-centralized decision making, is presented. In manufacturing and distribution networks, the traditional concept of static Supply Chains is changing towards the operation and management (O&M) of heterogeneous, dynamic and, geographically distributed partners. This new environment is making enterprises changing the way they manage their trading relationships. Interoperability is a critical issue to take into consideration when such collaboration needs appear due to the importance of information exchange and distributed coordination needs.

The European Project REMPLANET is intended to create methods and tools in supporting resilient organizational models. The project defines the concept of a resilient organization as the capacity to respond rapidly to **unforeseen** change, even chaotic disruption. It is the ability to bounce back — and, in fact, to bounce forward — with speed, determination and precision. A resilient organization effectively aligns its strategy, operations, management systems, governance structure, and decision-support capabilities so that it can uncover and adjust to continually changing risks, endure disruptions to its primary earnings drivers, and create advantages over less adaptive competitors.

Due to structural heterogeneity of REMPLANET integration scenarios, an ontological approach is provided, intended to define a unified and commonly agreed understanding of main domain concepts, and their relationships. This ontology will facilitate partners to understand how concepts are interrelated and the information sharing, and to avoid interoperability problems identified in an inter-operational environment such as conceptual barriers. The ontology has been divided into three simpler views in order to facilitate understanding, namely *Resilient Organization, ICT Platform and Members and its related processes.* The ICT platform incorporates interoperability functionalities, to facilitate the supply network member's systems integration and allow each new member a fast connection to the network. Moreover, this platform is considered a basis for the non-centralized decision making and allows facilitating communication, achieving flexibility and preparedness to environments changes. The ontology also allows the knowledge to be reused, shared, and enriched with more

knowledge using templates and automated procedures. The authors also identify some issues for further discussion, mainly concerning members and relationships.

The study of existing bibliography on resilience ontology has identified the following key elements:

- There is need for an ontology which will address the end-2-end resilience. This ontology will cover issues at different implementation levels (hardware, middleware, software), network layers (network, application layers) including human factors, both on the network as well as on the user side.
- There are several areas of interest, which are pointed in [4], namely cloud computing, real time detection and diagnosis systems, sensor networks, future wireless networks and integrity of supply chain. The derived ontology should be applicable to the aggregation of them as much as possible.
- The ontology will bridge the gap existing in standardization. Actually, it intends to be a form of guidelines for stakeholders, e.g. operators, policy makers etc., drawing the direction for resilience and moreover for quality except availability.
- This ontology and the corresponding taxonomy will address also the metrics for resilience.
- The ontology should offer an open, interoperable and scalable framework, which is desirable to lead to standardization. The target audience consists of all the involved in resilience stakeholders and mainly the industry stakeholders.

Annex E: Ontology language files

The ontology examined in the core of the document is presented in an electronic attachment to the document.

P.O. Box 1309, 71001 Heraklion, Greece
www.enisa.europa.eu