ETSI TS 102 165-1 V5.3.1 (2025-02)

TECHNICAL SPECIFICATION

Cyber Security (CYBER);
Methods and protocols;
Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)

Reference

RTS/CYBER-0082

Keywords

authentication, confidentiality, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from the ETSI Search & Browse Standards application.

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format on ETSI deliver repository.

Users should be aware that the present document may be revised or have its status changed, this information is available in the Milestones listing.

If you find errors in the present document, please send your comments to the relevant service listed under Committee Support Staff.

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure (CVD) program.

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Cyber Security (CYBER).

The present document is part 1 of a multi-part deliverable covering methods and protocols for security standardization, as identified below:

Part 1: "Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)";

Part 2: "Protocol Framework Definition; Security Counter Measures"

Part 3: "Vulnerability Assessment extension for TVRA".

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document defines a method primarily for use in undertaking an analysis of the threats, risks and vulnerabilities of an Information and Communications Technology (ICT) system to identify applicable countermeasures.

NOTE 1: The method described has been tailored to apply to pre-production but can be applied to production devices with due attention given to possibility that the application of countermeasures may be unachievable for a re-design strategy.

NOTE 2: The method described in the present document builds from the Common Criteria for security assurance and evaluation defined in [i.27], [i.28], [i.29] and may be used to form part of the documentation set for the Target Of Evaluation as specified in ETSI ES 202 382 [i.24].

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found in the ETSI docbox.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

[1] Common Methodology for Information Technology Security Evaluation, CEM:2022 Revision 1: "Evaluation methodology", November 2022. .

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI EG 202 387: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method for application of Common Criteria to ETSI deliverables".

[i.2] ETSI TR 187 011: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Application of ISO-15408-2 requirements to ETSI standards - guide, method and application with examples".

[i.3] ETSI TR 187 002: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); TISPAN NGN Security (NGN-SEC); Threat, Vulnerability and Risk Analysis".

[i.4] Void.

[i.5] Void.

[i.6] Void.

[i.7] Void.

[i.8] Void.

[i.9] ETSI ETR 332 (1996): "Security Techniques Advisory Group (STAG); Security requirements capture".

[i.10] CESG: "HMG IA Standard Numbers 1 & 2 - Supplement - Technical Risk Assessment and Risk Treatment", Issue No: 1.0, April 2012.

NOTE: The above reference is not actively maintained but can be found in many locations online. Aspects of the text of the reference have been rolled into the UK's Cyber Assurance Scheme.

[i.11] Void.

[i.12] Void.

[i.13] Void.

[i.14] "Object Management Group. UML 2.0 Superstructure Specification", 2004.

[i.15] Void.

[i.16] Void.

[i.17] Void.

[i.18] Void.

[i.19] Void.

[i.20] Void.

[i.21] Void.

[i.22] ISO/IEC 27000:2018: "Information technology - Security techniques - Information security management systems - Overview and vocabulary".

[i.23] Void.

[i.24] ETSI ES 202 382: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method and proforma for defining Protection Profiles".

[i.25] Void.

[i.26] Void.

[i.27] "Common Criteria for Information Technology; Security Evaluation; Part 1: Introduction and general model", November 2022, CC:2022, Revision 1.

[i.28] "Common Criteria for Information Technology; Security Evaluation; Part 2: Security functional components", November 2022, CC:2022, Revision 1.

[i.29] "Common Criteria for Information Technology; Security Evaluation; Part 3: Security assurance components", November 2022, CC:2022, Revision 1.

[i.30] "Common Criteria for Information Technology; Security Evaluation; Part 4: Framework for the specification of evaluation methods and activities", November 2022, CC:2022, Revision 1.

NOTE: The referenced documents [i.27] to [i.30] and [i.37] are also available from ISO as ISO/IEC 15408.

[i.31] Void.

[i.32] Void.

[i.33] ETSI TR 103 305-1: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls".

[i.34] ETSI TR 104 221: "Securing Artificial Intelligence (SAI); Problem Statement".

[i.35] ETSI GR SAI 001: "Securing Artificial Intelligence (SAI); AI Threat Ontology".

[i.36] ETSI EG 203 310 (V1.1.1): "CYBER; Quantum Computing Impact on security of ICT Systems; Recommendations on Business Continuity and Algorithm Selection".

[i.37] "Common Criteria for Information Technology; Security Evaluation; Part 5: Pre-defined packages of security requirements", November 2022, CC:2022, Revision 1.

[i.38] ETSI GR SAI 006: "Securing Artificial Intelligence (SAI); The role of hardware in security of AI".

[i.39] ETSI TR 101 583: "Methods for Testing and Specification (MTS); Security Testing; Basic Terminology".

[i.40] ETSI TR 103 305-5: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 5: Privacy and personal data protection enhancement".

[i.41] ETSI TR 103 370: "Practical introductory guide to Technical Standards for Privacy".

[i.42] ETSI TS 103 485: "CYBER; Mechanisms for privacy assurance and verification".

[i.43] ETSI TR 104 102: "Cyber Security (CYBER); Encrypted Traffic Integration (ETI); ZT-Kipling methodology".

[i.44] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[i.45] Recommendation ITU-T I.130: "Method for the characterization of telecommunication services supported by an ISDN and network capabilities of an ISDN".

[i.46] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

[i.47] ETSI TS 102 165-2: "CYBER; Methods and protocols; Part 2: Protocol Framework Definition; Security Counter Measures".

[i.48] Data Protection Impact Assessment (DPIA) tool.

[i.49] ETSI TS 102 165-3: "Cyber Security (CYBER); Methods and Protocols for Security Part 3: Vulnerability Assessment extension for TVRA".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI EG 202 387 [i.1], ISO/IEC 27000 [i.22] and the following apply:

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

attack surface: user interfaces, target protocol interfaces and reachable data paths that can be attacked within the system

NOTE: As defined in ETSI TR 101 583 [i.39].

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

NOTE: As defined in ISO/IEC 27000 [i.22].

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

cyber herd immunity: form of immunity to attack wherein a critical mass of vulnerable assets are protected against a certain type of attack such that it becomes unprofitable for attackers to attempt to discover unprotected assets to attack

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

nonce: arbitrary number that is generated for security purposes (such as an initialization vector) that is used only one time in any security session

NOTE: Although random and pseudo-random numbers theoretically produce unique numbers, there is the possibility that the same number can be generated more than once.

non-repudiation: ability to prove an action or event has taken place, so that this event or action cannot be repudiated later

residual risk: risk remaining after risk treatment

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 adverse action performed by a threat agent on an asset (clause 7.1.2 of Common Criteria part 1 [i.27]).

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: entity that can adversely act on an asset

TVRA analyst: person performing the TVRA

NOTE: The TVRA analyst role may be taken by a team of people.

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

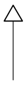
user: person or process using the system in order to gain access to some system resident or system accessible service

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 27000 [i.22], is modelled as the combination of a **weakness** that can be exploited by one or more **threats**.

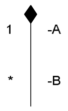
3.2 Symbols

For the purposes of the present document, the symbols given in OMG UML2 [i.14] and the following apply:



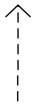
Generalization/Specialization: UML concept showing relationship between entities A and B where the two entities exhibit the property that A (top of arrow) is the general case whereas B is the specific case

EXAMPLE: A countermeasure is a specialized asset.



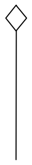
Composition: UML concept showing relationship between entities A and B where A "is composed of" B

EXAMPLE: Vulnerability "is composed of" a threat and a weakness.



Dependency: UML concept showing relationship between entities A and B where B is dependent upon A

EXAMPLE: Security requirements "depend on" security objectives.



Aggregation: UML concept showing relationship between entities A and B where A "is an aggregate of" B

EXAMPLE: System "is an aggregate of" assets.

3.3 Abbreviations

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

AI	Artificial Intelligence
CAT	CATegory (of Change Request)
CBA	Cost Benefit Analysis
CC	Common Criteria
CIA	Confidentiality Integrity Availability
CM	Configuration Management
DDDS	Dynamic Delegation Discovery System
DNS	Domain Name Service
EAL	Evaluation Assurance Level
GDPR	General Data Protection Regulation
IP	Internet Protocol
ISBN	International Standard Book Number
ISO	International Organization for Standardization
IT	Information Technology
ML	Machine Learning
MS	Mobile Station
NAPTR	Naming Authority PoinTeR
NASS	Network Attachment Sub-System
NGN	Next Generation Network
PP	Protection Profile
ST	Security Targets
TISPAN	Telecommunications and Internet converged Services and Protocols for Advanced Networking
TOE	Target Of Evaluation
TSF	TOE Security Function
TTP	Trusted Third Party
TVRA	Threat Vulnerability and Risk Analysis
UML	Unified Modelling Language

4 Introduction

4.1 Role of TVRA

It is asserted for the present document that without an understanding of the system, of the threats to the system, and a systematic cost-benefit analysis of countermeasures to the threats, that appropriate selection of those countermeasures cannot be made.

A Threat Vulnerability and Risk Analysis (TVRA) as defined in the present document should be used to identify risk to the system based upon the product of the likelihood of an attack, and the impact that such an attack will have on the system. The TVRA method described in the present document is intended to give justification for the development of security solutions, and the Cost Benefit Analysis (CBA) element of the method includes analysis of the impact on standardisation, regulation, and others (see clause 6.10 of the present document).

The method described in the present document provides a means of documenting the rationale for designing and implementing security countermeasures in a system. This is achieved by application of a systematic method, and by using part of the method to visualize the relationship of objectives, requirements, system design and system vulnerabilities.

The method requires analysts (the TVRA analyst) to systematically address ICT systems and to quantify their assets, vulnerabilities and threats. The TVRA analyst shall identify the quantitative risk to the assets of a system in order to identify mitigations that counter threats, or prevent attacks, such that the assets, and the system they form part of, can perform their primary function. The output of the TVRA shall be a quantified measure of the risks to the assets of a system, and of the system as a whole. The TVRA process, as part of the overall system design process, shall also define security requirements for the identified threat mitigations.

NOTE: The requirements may be further expanded in dedicated standards or design documentation where the referenced TVRA offers justification or rationale for each countermeasure.

For the purposes of analysis all assets shall be assumed, initially, to have weaknesses and the analyst shall verify that opening assumption.

The depth of the required analysis (using the TVRA method) changes as the system design becomes more detailed. A TVRA working from the system objectives should identify at a very coarse level the required security functionality to ensure that the objectives can be met without damage to the system.

The structure of activities in development of a TVRA is shown in figure 1. The process is shown as recursive wherein any change to any aspect of the system or its environment requires the process to be restarted, or its conclusions reviewed.

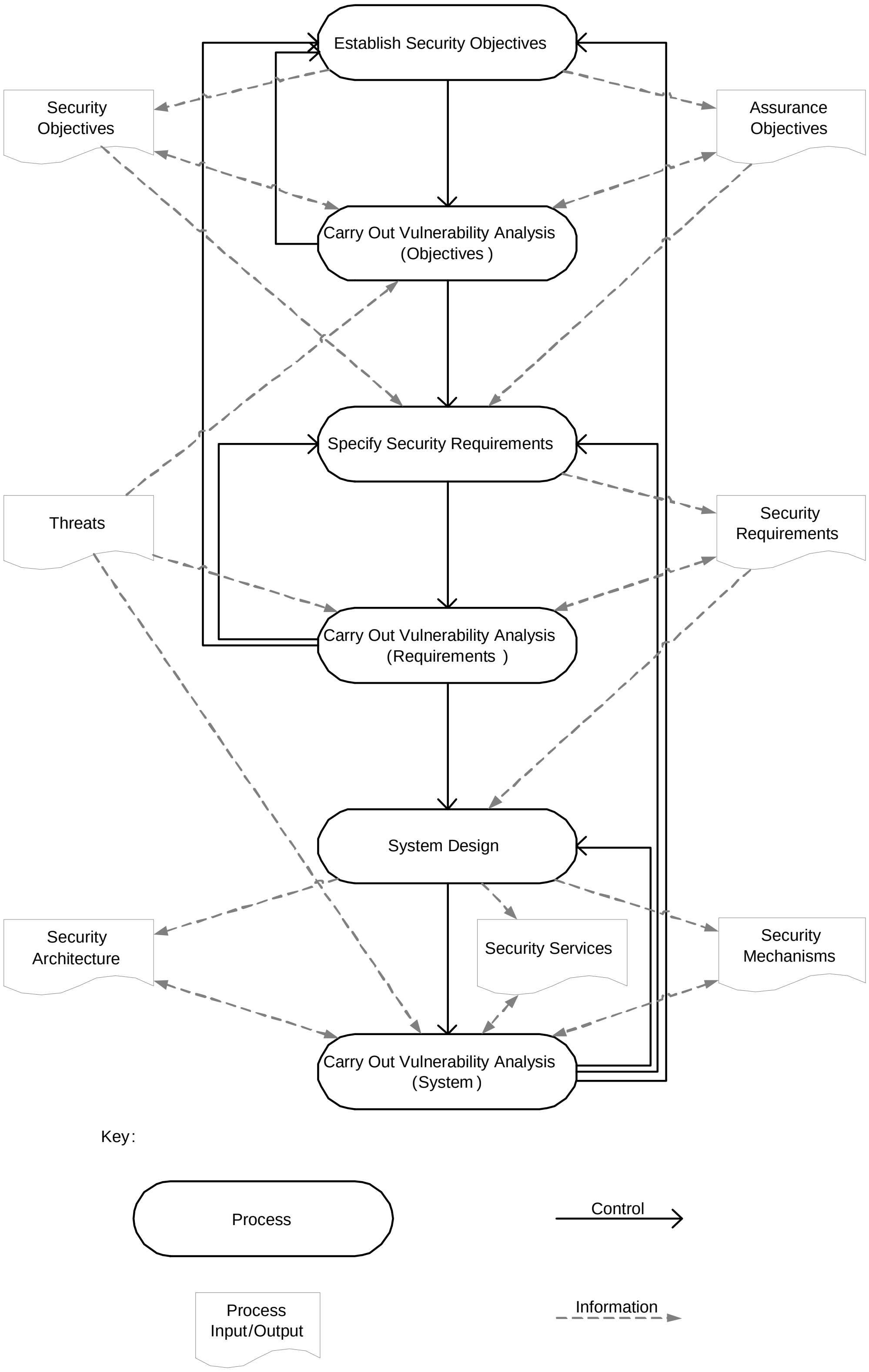

Establish Security Objectives
Security Objectives
Assurance Objectives
Carry Out Vulnerability Analysis (Objectives)
Specify Security Requirements
Threats
Security Requirements
Carry Out Vulnerability Analysis (Requirements)
System Design
Security Architecture
Security Services
Security Mechanisms
Carry Out Vulnerability Analysis (System)
Key:
Process
Control
Process Input/Output
Information

Figure 1: Structure of security analysis and development in standards documents

The purpose of the TVRA is to determine how open to attack the system, or components of the system are. A measure of openness of the system to attack is the metric "attack potential" which combines factors of expertise, availability and resources and this is explored further in clause 6.6.

An additional view of the nature of TVRA is given in figure 2 showing that any change either internal (say by application of countermeasures) or external to the system (say by an evolved attack or a change in the environment) requires that the conclusions of the TVRA process are reviewed, with the consequence in some cases that the TVRA is redone.

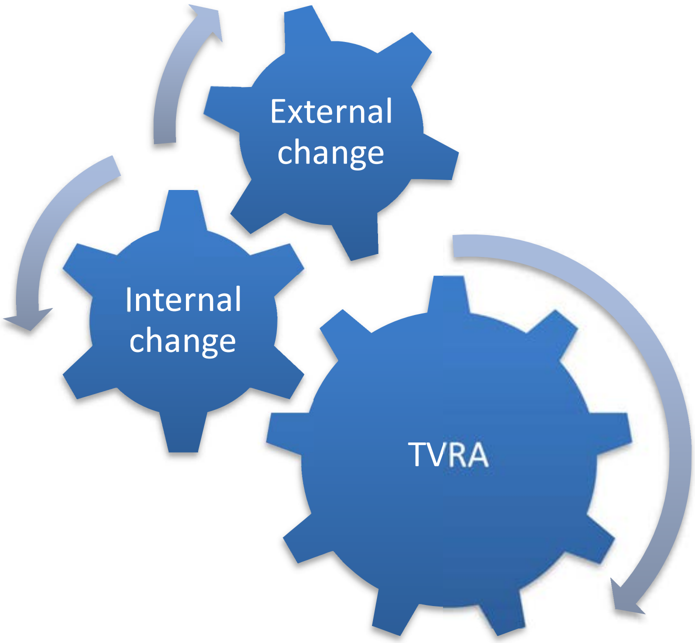


Figure 2: Cyclical nature of TVRA wherein any change requires reapplication of TVRA

In addressing the changing environment and the affect that has on risk the analyst is expected to ensure that means exist within the system and its organisation to continuously monitor for vulnerabilities. The security controls from ETSI TR 103 305-1 [i.33] apply, in particular CSC7.5 and CSC7.6 apply for continuous identification, and CSC7.1 and CSC7.2 apply to the necessary governance capabilities of the organisation.

4.2 Generic TVRA relationships

One of the keys to a successful TVRA, and also of a successful system design, is the ability to show the relationship of objectives and requirements to the system design and to the stakeholders in the system. Figure 3 shows the dependencies between system objectives, system requirements and system design highlighting the interplay of security objectives and requirements. In text format security requirements realize security objectives where the system design supports the security objectives.

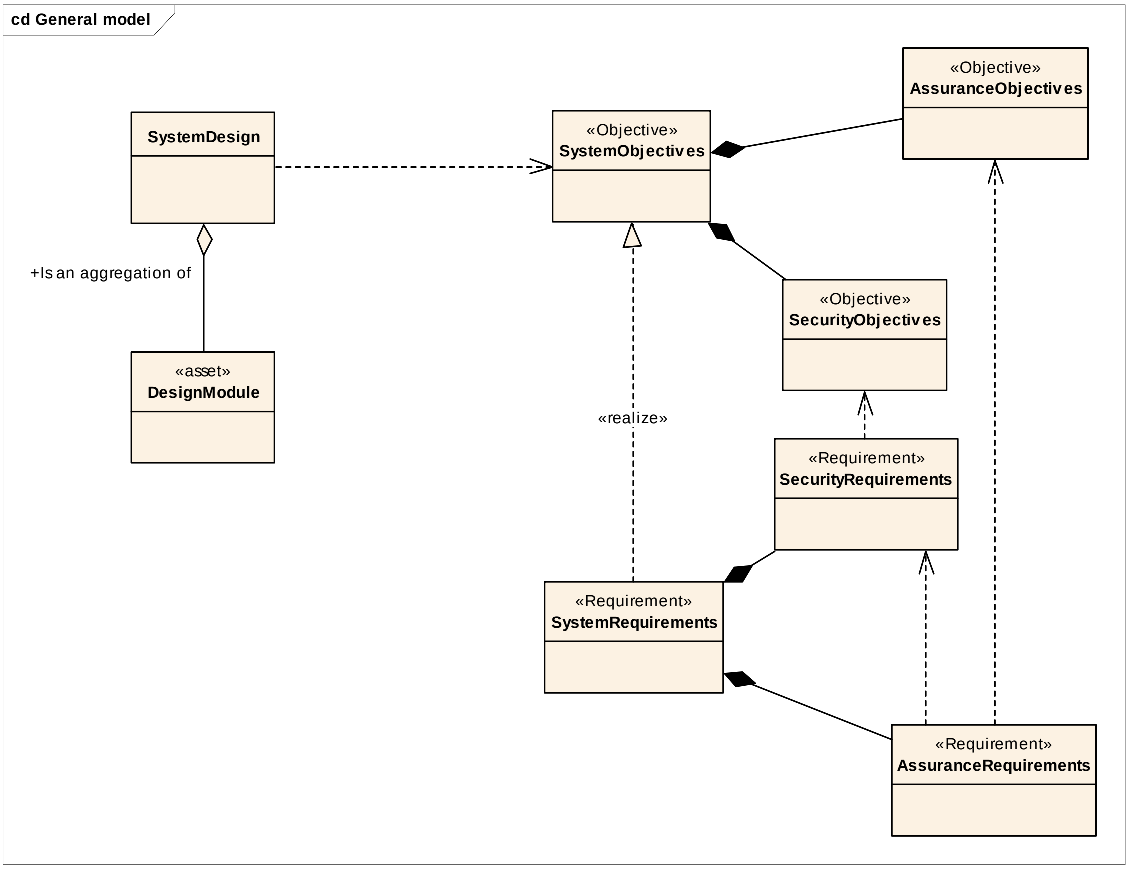


Figure 3: Relationship between system design, objectives and requirements

For most systems the development of system requirements goes far beyond just security and one concern for TVRA is to ensure that the system design is itself robust and therefore has fully documented requirements across all its aspects.

For the TVRA the system being examined (with its catalogued objectives and requirements) and the assets of the system and how it fits to its environment shall be clearly identified. The means to perform this in the TVRA method are described in clause 6 of the present document. In the context of TVRA the key relationship is that between a vulnerability and an asset and this is a weighted relationship with the weighting being defined as the risk to the asset due to the associated vulnerability. A pictorial view of the asset-threat-weakness-vulnerability-countermeasure relationship to system design is given in figure 4.

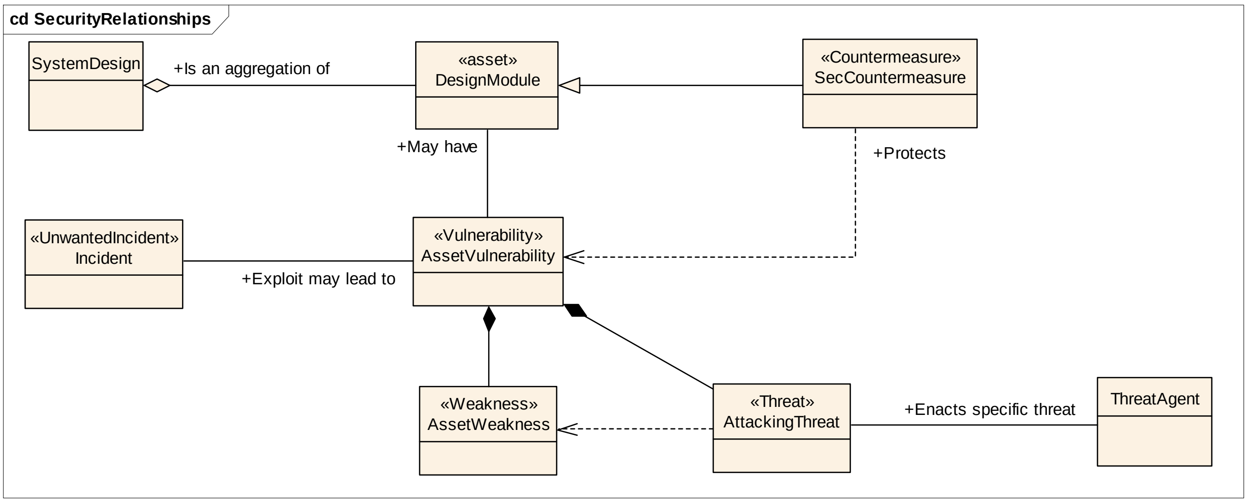


Figure 4: Generic security TVRA model

The TVRA method derives from the model shown in figure 4. The TVRA models a system consisting of assets. An asset may be physical, human or logical. **Assets** in the model may have **Weaknesses** that may be attacked by **Threats**. A **Threat** is enacted by a **Threat Agent**, and may lead to an **Unwanted Incident** breaking certain pre-defined security objectives. A **Vulnerability** is modelled as the combination of a **Weakness** that can be exploited by one or more **Threats**. When applied, **Countermeasures** protect against **Threats** to **Vulnerabilities** and reduce the **Risk**.

NOTE: The text above is consistent with the definition given in ISO/IEC 27000 [i.22].

One of the purposes of security design is to minimize the probability of any instance of the class "unwanted incident" being instantiated. It should be noted that whilst some countermeasures may themselves become system assets, and as such have their own vulnerabilities, many instances of countermeasures will be considered as policies, system guidelines and, if captured early enough, system redesign.

Threats can be classified as one of 4 types:

- Interception.
- Manipulation.
- Denial of service.
- Repudiation of an action (e.g. Repudiation of sending, and Repudiation of receiving).

NOTE: The general case for repudiation is that of involvement in an action, for communication this can be stated as repudiation of sending or receiving, but can be any other action such as editing or deleting a file (where such actions themselves are considered under manipulation threats).

Similarly, security objectives can be classified as one of 3 types (commonly referred to as "CIA" types (an expanded interpretation of the "A" in "CIA" is given)):

- Confidentiality.
- Integrity.
- Availability:
  - Authenticity.
  - Accountability.

Figure 5: Void

4.3 Countermeasure strategies

4.3.0 Overview of strategies

The goal of security design is to ensure a low likelihood of an unwanted incident arising by minimising the viable attack surface. As the likelihood of an unwanted incident is dependent upon the presence of weakness in an asset, and also the presence of both threats and threat agents that exploit the weakness, it is the purpose of security systems to remove, or mask, the weaknesses of an asset (i.e. to make that threat agent non-viable).

NOTE 1: The analyst is expected to evaluate non-technical components of security strategies such as the management of the system and its human components in determining the risk to a system or its constituent assets.

There are non-technical measures addressed by the security controls described in ETSI TR 103 305-1 [i.33] that apply across the system and the TVRA method may assist in prioritising each of the controls described there.

The following strategies are considered within the present document:

- Asset redesign.
- Asset hardening.

NOTE 2: In some cases, the TVRA analyst will recommend, or highlight, a non-system deterrent as a strategic countermeasure. Such measures can include the criminalisation under law of the attack and a sufficient judiciary penalty (e.g. interment, financial penalty), with adequate law enforcement resources to capture and prosecute the threat agent.

4.3.1 Asset redesign

The assumption made prior to analysis is that all assets have weaknesses and the analyst shall identify those weaknesses. Where weaknesses are found and have associated threats and threat agents there may be a possibility to redesign the asset in such a way as to remove the inherent weaknesses. The viability of this strategy depends on a number of factors including the maturity of the asset design and the relative cost of redesign versus the cost of weakness masking through asset hardening (see clause 4.3.2).

4.3.2 Asset hardening

An asset can have some weaknesses that cannot be removed but which can be masked or made inaccessible by the addition of features or capabilities to the vulnerable asset or to other assets in the system such that the combination of assets in the system presents a lower likelihood of attack, and hence a lower risk to the system.

NOTE: As assets in the form of asset hardening measures are added to the system the complexity of the system increases and the number of assets and inter-asset relationships to be protected is also increased. This can lead to a point where the resultant system cannot be adequately protected as the system complexity introduced as protection outweighs the set of assets defined for basic system functionality.

4.3.3 Resilience and redundancy considerations

As shown in figure 4 systems are modelled as an aggregation of assets. Many of these assets may be deployed to offer redundancy protection, or to add resilience to the system. Where an asset is duplicated it will share the same vulnerabilities as any other instance of the asset, however when subject to attack not all instances of the asset may be attacked at the same time. The use of multiple instances of the same asset does not, in general, diminish the attack likelihood, or impact, rather it offers protection against other forms of failure including site failure (e.g. loss of power or similar to a particular geographic location).

4.4 Relationship with Common Criteria evaluation

The purpose of the TVRA is to support and rationalize the provision of security countermeasures. In addition, the TVRA serves to support and rationalize system design decisions. The result of the TVRA exercise is therefore to minimize risk of exploitation and attack of the analysed system when deployed. In order to consider this fully the TVRA method described in the present document addresses the impact and likelihood of an attack on the system prior to it becoming available, whereas the Common Criteria [i.30] primarily addresses the resistance to attack of the system by assessment, in the form of a structured evaluation, of an available system. In this way the TVRA method complements the Common Criteria [i.30].

The TVRA is defined in such a way that it allows part of the descriptive text of a PP to be derived from the TVRA:

- security objectives;
- security requirements;
- rationale.

The structure of the assurance class for vulnerability analysis described in Common Criteria [i.30] is slightly different from the structure recommended for a TVRA in the present document, however the two approaches are considered complementary.

Within a final common criteria evaluation [i.30] the vulnerability analysis assurance family assumes that the system design is complete whereas the purpose of the vulnerability analysis exercise in TVRA is to be able to identify vulnerabilities that require the provision of countermeasures, and then to assess the vulnerabilities that exist in the system with the countermeasures applied. The final documented TVRA may be used in the context of common criteria evaluation [i.30] to satisfy those aspects of evaluation found in sections (a), (b) and (c) of a protection profile (see ETSI ES 202 382 [i.24], clauses 5.1.2 through to clauses 5.1.7).

Figure 6 (taken from ETSI EG 202 387 [i.1]) shows a simplified view of the relationships between the components of Common Criteria (CC), Protection Profiles (PPs), Security Targets (ST) and Targets Of Evaluation (TOE). The standardization process fits primarily in the "Consumer side" of the figure. The TVRA takes the slightly wider interpretation of attack surface as opposed to TOE, in which the intent of security design is to minimise the attack surface, where that attack surface consists of user interfaces, target protocol interfaces and reachable data paths that can be attacked within the system.

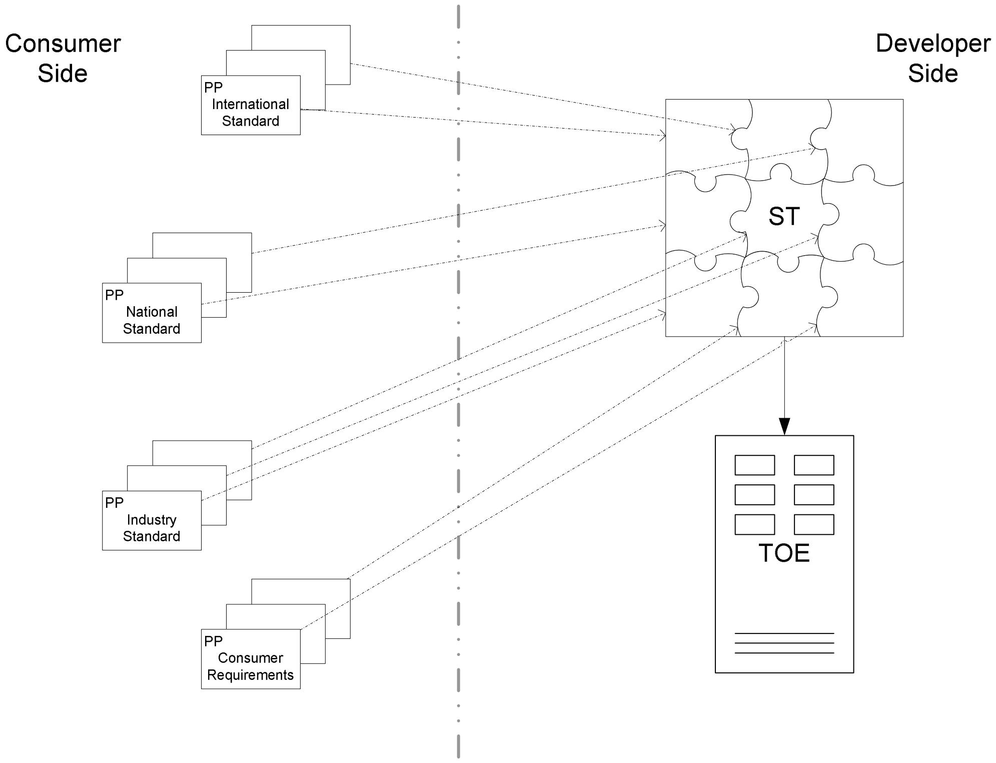


Figure 6: Relationship between PPs, STs and TOEs

4.5 Relationship to explicability and transparency

Where explicability and transparency are cited as requirements, e.g. in regulation of systems, a TVRA, in decomposing a system in order to determine risk, should be able to meet those requirements.

EXAMPLE: In very simple terms if an asset in a system has no clear role or where its role is open ended (unbounded) it can have a detrimental impact on system security that should be identified in the analysis,

The output of the TVRA process shall by default make all assets and their connections explicable and transparent. The Zero Trust approach identified in ETSI TR 104 102 [i.43], which extends the identification of assets and their relationship to each other to the dynamic establishment of services, should be adopted for live systems in order to give ongoing validation of the credentials of assets.

4.6 Relationship to testing

All requirements imposed on a system should be designed to be testable.

4.7 Relationship to cybersecurity controls

In addition to understanding of risk and in provision of a secure environment an organisation should implement security controls such as those defined in ETSI TR 103 305-1 [i.33]. Details of the application of controls relating to inventory of assets is addressed in more detail in clause 6.4 of the present document.

4.8 Relationship between privacy and security

Privacy protection is often a non-negotiable characteristic of a system where the system processes data that can be used to identify a person. The application of security controls (see clause 4.7) to privacy protection is specifically addressed in ETSI TR 103 305-5 [i.40]. In addition, ETSI TR 103 370 [i.41] and ETSI TS 103 485 [i.42] apply.

If the system gathers data that falls within the scope of the GDPR [i.44] the analyst should clearly identify data controller and data processor assets, and the relevant policy in the inventory of assets (see clause 6.4 of the present document). The analyst should also verify that where GDPR applies that the controls outlined in ETSI TR 103 305-5 [i.40] or an equivalent have been taken into account.

4.9 Relationship to security design practice

There are a number of design principles that are commonly recommended and endorsed by the present document.

- Least privilege - security principle that demands that it should be granted the minimum set of capabilities to access and use information and resources that allows to carry out those duties to which someone is expressly authorized.

- Least persistence - extends least privilege to ensure that a security association is maintained for the minimum time.

In addition, the security model of Zero Trust is endorsed, in which security associations are not assumed to be present but established on the assumption of no-memory (i.e. the existence of a previous trusted connection has no impact on the acceptance of the current connection).

The method for Zero-Trust design and implementation given in ETSI TR 104 102 [i.43] applies in general by which the role of each asset in the system is identified and justified.

5 TVRA method

5.1 Overview

5.1.0 Introduction

The TVRA method involves a systematic identification of the unwanted incidents to be prevented in the system, the means by which those unwanted incidents can be enacted, and the risk to the system when enacted. Thus, the TVRA analyst shall document the outcome of the following actions:

- The analyst shall identify the attack surface of the system (see clause 6.2).

- The analyst shall identify the assets of which a system is composed (see clause 6.5).

- The analyst shall identify the associated weaknesses of each asset and of the system as a whole (see clause 6.6).

- The analyst shall identify the threats and the threat agents that are able to attack the system (see clause 6.6).

- The analyst shall determine the risk to the system by modelling the likelihood and impact of each attack on the system's vulnerabilities (see clause 6.6).

The system description shall include the roles of stakeholders to the system as assets on the boundary of the system.

From the initial analysis documented through the investigate steps above the analyst shall identify means to reduce the risk to an acceptable level. This should address critical risks first in order to either eliminate them or to reduce the residual risk. A Cost Benefit Analysis (CBA) as defined in clause 6.10 shall be used to guide this assessment. The analysis shall be re-performed with the identified countermeasures deployed to re-assess the risks of the protected system.

NOTE 1: The role of Artificial Intelligence (AI) or Machine Learning (ML) in assessment of likelihood and impact is addressed across the present document in consideration of automation (see also Annex J).

NOTE 2: The application of the TVRA method to AI and ML systems is addressed in Annex K.

The output of the TVRA shall be a quantified measure of the risks to the assets and a set of detailed security requirements that will minimize that risk.

For the purposes of analysis, the initial view is that all assets shall be considered to have weaknesses.

Given that the TVRA identifies the assets of a system, the weaknesses of each asset and the potential threats associated with these weaknesses it may act as a weakness of the system in its own right and care should be taken in publication of the analysis as making the details of any particular weakness public can increase the risk to the system, particularly where a means of exploiting the weakness is also published unless countermeasures are implemented promptly.

NOTE 3: The term threat agent is used in the present document to refer to a specific means to enact a threat in order to exploit a weakness.

5.1.1 Scope of the analysis (TVRA) description

5.1.1.0 Introduction

As indicated in clause 4.4 the preference of the present document is to consider the entire attack surface of the system to be deployed and to ensure that reasonable steps have been taken to address the risks across the entire attack surface. It is recognised that in many cases the potential attack surface may be unwieldy and that an analyst may attempt to shrink it to a manageable scale, placing parts of the attack surface into the wider environment. This approach can only be justified if the analyst can show that the minimisation does not harm the wider environment, and that reasonable risk analysis has been conducted on the wider environment.

NOTE 1: If it is known in advance that the system will be subject to 3rd party evaluation using Common Criteria [i.27], the applicable requirement to provide a brief but clear description of the Target Of Evaluation (TOE) applies and therefore the PP pro forma defined in ETSI ES 202 382 [i.24] may be adopted.

NOTE 2: It is recognized that an attack on any asset can affect not only the asset but also the system in which the asset exists (the environment).

5.1.1.1 Security environment

The security environment describes the security aspects of the environment in which the asset is intended to be used. It shall include:

- Security assumptions:
    - the intended use of the implementation;
    - the physical, user and connection aspects of the environment in which an implementation will operate.

EXAMPLE 1: A Home Gateway (HG) is intended to be in the customer premises and connect to a CSP network externally to the premises (home), and to allow for an internal network to access the external network but for devices on the internal network to be gapped from the external network. The HG is expected to have at least one fixed connection to the external network, and to have support for fixed (e.g. Ethernet) and wireless (e.g. Wi-Fi®) connectivity on the home side of the HG.

- Assets:
    - Identified by a decomposition of the system/implementation into its discrete components;

  - the assets with which the asset under analysis will interact with;
  - the nature of the asset's interaction with other assets.

- Threats and threat agents:
  - all threats against which specific protection is required within either the implementation of the asset or its expected environment;
  - the threat agents that will be used to enact the identified threats.

- Organizational security policies:
  - any security policies or rules with which an implementation of the asset shall comply.

The description of the security environment should be documented in such a way that each element identified above is clearly identifiable. The checklist format illustrated in the example may be used by the developer.

EXAMPLE 2:

A Security Environment		
TVRA-id	**Guidance text**	**Checkbox**
a.1 Assumptions		
a.1.1	The intended use of the implementation is to allow a home user to connect to an ISP for access to the Internet.	
a.1.2		
..	..	..
a.2 Assets		
a.2.1		
a.2.2		
..	..	..
a.3 Threats		
a.3.1		
a.3.2		
..	..	..
a.4 Threat agents		
a.4.1		
a.4.2		
a.4.3		
..	..	..
a.5 Security policies (OPTIONAL)		
a.5.1		
a.5.2		

5.1.1.2 Security objectives

A TVRA shall contain a definition of the security objectives of each of the stakeholders, the system as a whole, each asset and the environment. These objectives are expected to cover the assumptions, threats and policies described in the security environment (see clause 5.1.1.1). They should be expressed in broad terms rather than in detail. The phrasing of an objective shall not contain any of the words *shall* or *should* as an objective does not state a requirement. Objectives should be segregated into two distinct groups, thus:

- Security objectives for the system under analysis (i.e. the system, assets and stakeholders):
  - It should be clear which aspects of the identified threats and policies are addressed by each objective.

NOTE 1: If the asset is defined in a standard, it is likely that the asset security objectives will be specified in the Stage 1 (or equivalent) specification.

NOTE 1a: The 3-stage approach to design mentioned above is defined in Recommendation ITU-T I.130 [i.45], where stage 1 is an overall service description from the user’s standpoint, stage 2 is an overall description of the organization of the network functions to map service requirements into network capabilities, and stage 3 is the definition of switching and signalling capabilities needed to support services defined in stage 1.

- Security objectives for the environment:
    - It should be clear which aspects of the identified threats and policies are expected to be addressed by the environment because they are not covered (either wholly or in part) by the asset security objectives.

NOTE 2: Standards rarely specify requirements for the environment, rather they react to the environment, so it is unlikely that the security objectives for the environment will be stated explicitly in the base security standard or any associated document.

EXAMPLE:

B Security Objectives		
b.1 Security objectives for the asset		
b.1.1	Ensure that only registered users can access the system	
b.1.2		
..	..	..
b.2 Security objectives for the environment		

5.1.1.3 Security requirements

5.1.1.3.1 The relationship between security objectives and security requirements

The distinction between security objectives and security requirements is an important one to make. An objective is the expression of what a security system should be able to do in very broad terms whereas a requirement is a detailed specification of how an objective is achieved. An objective is not normative and shall not use the modal verbs shall or should.

EXAMPLE 1: Ensure that only registered users can access the system.

A security requirement associated with this objective (example 1) could be as shown in example 2.

EXAMPLE 2: A user shall be successfully identified and authenticated to the asset by means of a username and password before all other interactions between the asset and that user.

NOTE: It would not be unusual for a single objective to be realized by the implementation of more than one requirement nor for a single requirement to partially implement more than one objective.

5.1.1.3.2 Security requirements statements

Security requirements should be identified for both the asset and, where applicable, its environment. The security requirements should be classified into the following groups:

- Asset security functional requirements:
    - An identification of each of the security-related functional requirements specified in the base security standard and an indication of where in the standard the detailed requirement can be found.

NOTE 1: If it is known in advance that the system will be subject to 3rd party evaluation using a known evaluation scheme, e.g. Common Criteria, the applicable functional components that the requirement represents defined by the 3rd party scheme (e.g. Common Criteria Part 2 [i.28]) may be used in the TVRA and system documentation.

- Asset security assurance and testing/verification requirements:
    - An indication of how the security claims can be tested or verified.

NOTE 2: If it is known in advance that the system will be subject to 3rd party evaluation using a known evaluation scheme, e.g. Common Criteria, the assurance scheme and the results expected (e.g. Evaluation Assurance Level (EAL) [i.37], or EUCC assurance level from the Cyber Security Act (CSA) [i.46]) form part of the system assumptions (see clause 6.2).

NOTE 3: If a 3rd party evaluation scheme is required that uses CC an identification of any specific assurance components from Common Criteria Part 3 [i.29] or which need to be specified may be given as part of the TVRA documentation.

The specification of security requirements for the environment is optional and should only be included in the analysis if security objectives for the environment are identified earlier in the analysis (see clause 5.1.1.2). If requirements for the environment are included, they should be presented in the same way as functional requirements for the asset.

EXAMPLE:

C Security Requirements			
c.1 asset security requirements			
c.1.1 asset security functional requirements			
c.1.1.1	Users shall not be allowed to access any system function prior to successful identification and authentication.		
c.1.1.2			
..	..	..	..
c.1.2 asset security assurance requirements			
c.1.2.1	The system shall be designed to be evaluated as "substantial" as defined by the CSA [i.46].		
..	..		..
c.2 Environment security requirements (OPTIONAL)			
c.2.1			

5.1.1.3.3 Interaction with Common Criteria

In the preceding clause it is recommended that where possible assurance and functional components from Common Criteria Part 2 [i.28] and Common Criteria Part 3 [i.29] should be identified. The guidance to the application of Common Criteria in ETSI deliverables, ETSI EG 202 387 [i.1], should be used as source material in this case.

EXAMPLE: A countermeasure to prevent masquerade can require that the identity is presented and validated, then authenticated, prior to system access. To implement this countermeasure with respect to Common Criteria's use of functional requirements will require a design that includes components "User identification before any action" and "User authentication before any action" (FIA_UID.2 and FIA_UAU.2 respectively in Common Criteria Part 2 [i.28]).

Common Criteria Part 5 [i.37] provides packages of security assurance and security functional requirements including groupings as Evaluation Assurance Levels (EALs), and Composed Assurance Packages (CAPs).

Table 1: Evaluation service level summary as specified in Common Criteria Part 5 [i.37]

Assurance Class	Assurance Family	Assurance Component by Evaluation Assurance Level (EAL)						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	Security architecture (ADV_ARC)		1	1	1	1	1	1
	Functional specification (ADV_FSP)	1	2	3	4	5	5	6
	Implementation representation (ADV_IMP)				1	1	2	2
	TSF internals (ADV_INT)					2	3	3
	Security policy modelling (ADV_SPM)						1	1
	TOE design (ADV_TDS)		1	2	3	4	5	6
Guidance documents	Operational user guidance (AGD_OPE)	1	1	1	1	1	1	1
	Preparative procedures (AGD_PRE	1	1	1	1	1	1	1
Life-cycle support	CM capabilities (ALC_CMC)	1	2	3	4	4	5	5
	CM scope (ALC_CMS)	1	2	3	4	5	5	5
	Delivery (ALC_DEL)		1	1	1	1	1	1
	Development security (ALC_DVS)			1	1	1	2	2
	Life-cycle definition (ALC_LCD)			1	1	1	1	2
	Tools and techniques (ALC_TAT)				1	2	3	3
Security Target evaluation	Conformance claims (ASE_CCL)	1	1	1	1	1	1	1
	Extended components definition (ASE_ECD)	1	1	1	1	1	1	1
	ST introduction (ASE_INT)	1	1	1	1	1	1	1
	Security objectives (ASE_OBJ)	1	2	2	2	2	2	2
	Security requirements (ASE_REQ)	1	2	2	2	2	2	2
	Security problem definition (ASE_SPD)		1	1	1	1	1	1
	TOE summary specification (ASE_TSS)	1	1	1	1	1	1	1
Tests	Coverage (ATE_COV)		1	2	2	2	3	3
	Depth (ATE_DPT)			1	1	3	3	4
	Functional tests (ATE_FUN)		1	1	1	1	2	2
	Independent testing (ATE_IND)	1	2	2	2	2	2	3
Vulnerability assessment	Vulnerability analysis (AVA_VAN)	1	2	2	3	4	5	5

ETSI TR 187 011 [i.2] provides guidelines and method on how to apply Common Criteria Part 2 [i.28] requirements to ETSI standards. ETSI TR 187 002 [i.3] provides examples of security functional requirements.

NOTE: The version of ETSI TR 187 011 [i.2], and of ETSI TR 187 002 [i.3] refer to an earlier version of the Common Criteria but the general principles given apply.

5.1.2 Threats and threat agents

Threats to an ICT system fall into a small set of easily identified operations. The means to enact these threats are conversely many and varied and it is the " threat agent" that will take most time to identify and that is the primary source of the risk to the system.

NOTE 0: A threat agent can take many forms including AI agents, viruses and trojans that may act in compositions of agents to achieve enactment of the threat.

Threats in ICT belong to one of the following groups (showing subclasses of each threat) as outlined in clause 4.2 and shown in a tree in figure 7:

- Interception:
  - Eavesdropping:
    - A breach of confidentiality by unauthorized monitoring of communication.
- Manipulation:
  - Masquerade ("spoofing"):
    - The pretence of an entity to be a different entity. This may be a basis for other threats like unauthorized access or forgery.

- Loss or corruption of information:
  - The integrity of data (transferred) is compromised by unauthorized deletion, insertion, modification, reordering, replay or delay.
  - Data used in processing, for example in ML or AI, is compromised by containing bias or other forms of data poisoning at source that offers risk to the user or dependent stakeholders.
- Unauthorized access:
  - An entity accesses data in violation to the security policy in force.
- Forgery:
  - An entity fabricates information and claims that such information was received from another entity or sent to another entity.

- Repudiation:
  - An entity involved in an exchange subsequently denies the fact.
- Denial of service:
  - An entity fails to perform its function or prevents other entities from performing their functions.

NOTE 1: Denial of Service can be considered as a specialism of Manipulation but is shown as a discrete threat group as it can combine elements of all groups and further is sufficiently prevalent to require such separation.

NOTE 2: There are a number of threat categories identified in ETSI TR 104 221 [i.34] for the specific domain of AI that are wide variations of manipulation, where bias may be inherent in data sources but when combined with learning algorithms may result in user manipulation, even if the integrity of the source is unaffected.

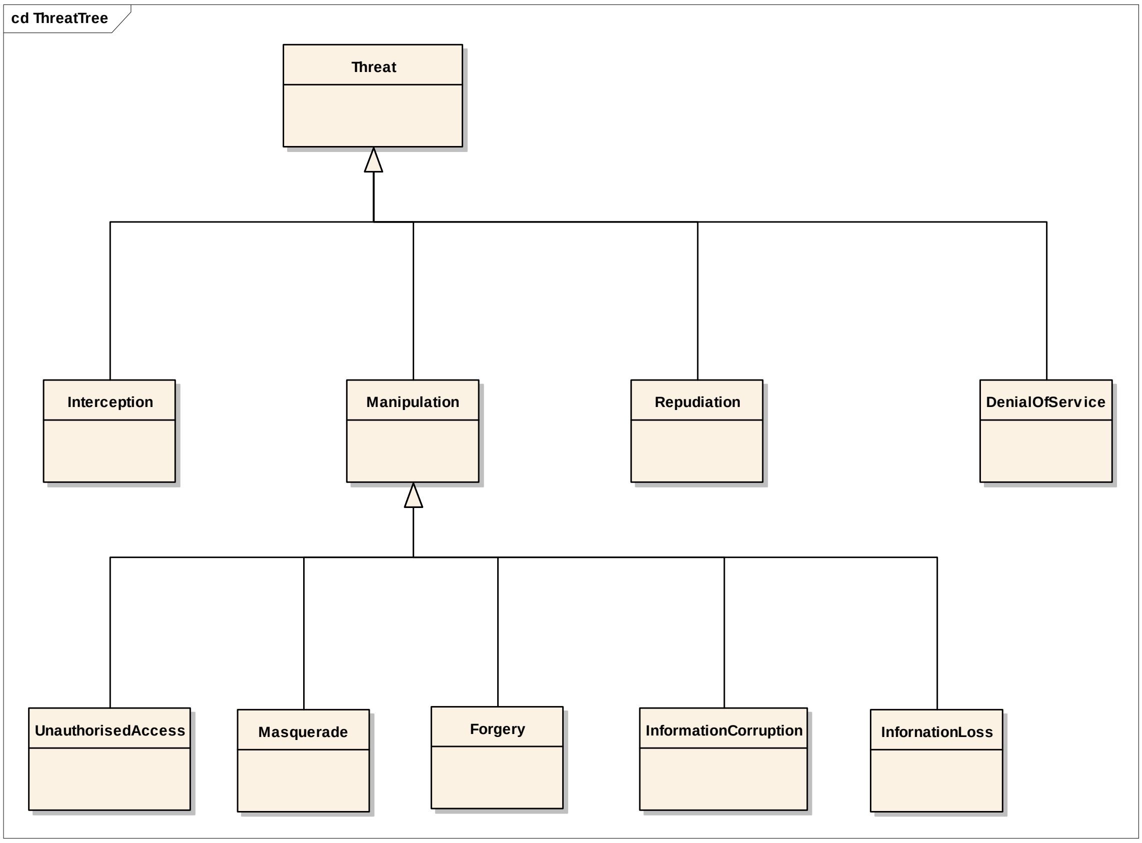


Figure 7: Threat tree

Table 2 shows how the CIA(AA) security objective classifications are vulnerable to specific types of threat.

Table 2: Threats to security objective types

Threat	Objective type				
	Confidentiality	Integrity	Availability	Authenticity	Accountability
Interception (eavesdropping)	X				
Unauthorized access	X	X		X	X
Masquerade	X	X		X	X
Forgery		X	X	X	X
Loss or corruption of information		X	X		
Repudiation		X		X	X
Denial of service			X		

5.2 Actors and roles

For the purpose of the analysis relevant actors to consider are *users*. A user is defined as a person or process using the system in order to gain access to some system resident or system accessible service. Users can further be categorized dependent on whether they belong to the organization running the services (internal users) or whether they access the services as external users.

Each time a user accesses a service, the user takes on a role. In some cases, there will be a one-to-one relationship between a user and a role, i.e. the user will always stay in the same role. In other cases, there will be a one-to-many relationship between a specific user and the possible roles the user can play. This latter case is the normal ICT case in which the same user can act as a session initiator, receiver, registrant, etc.

NOTE 1: The term session is used as a catch all to address session based, transaction based, and both persistent ad non-persistent connectivity.

Some security measures can require actors to enforce the role of a Trusted Third Party (TTP). An important security issue is how these actors should be allowed to interact with each other in the context of the service or function they are using.

NOTE 2: The role of a TTP in access control is addressed in ETSI TS 102 165-2 [i.47].

5.3 Rationale (for use in Protection Profiles)

To comply with Common Criteria Part 1 [i.27] a PP should provide a rationale, for both the security objectives and the security requirements. It should explain in detail how the security objectives and the security requirements address the threats identified in the asset's security environment. The TVRA may be used to provide this rationale and it may, therefore, be referred to in the PP as the source of the rationale. The association of objectives, requirement, threats and assets within a TVRA provides the rationale for the selection of the security architecture and the countermeasures described by the PP.

5a Risk calculation approach

5a.1 Summary of calculation

Risk shall be calculated as the product of attack impact and attack likelihood.

It is recognised that ICT deployments are open to many other forms of risk in addition to the cyber-security risks addressed by the present document. In any practical system risks have to be assessed across many dimensions: Financial risk; Environmental risk; Market risk; and so forth. The metrics outlined in the present document apply to ICT systems under some form of cyber-attack and are not intended to be applied in other risk dimensions.

It is highly likely that long term existential risks to systems can be mis-identified using the metrics from the Common Criteria Evaluation methodology [1] (see clauses 5a.3 and 6.7 of the present document). This is particularly true for assessing the long term evolution of security from one paradigm to another. In all cases the approach to evaluation of the risk derived from the equation for quantum safe development given in ETSI EG 203 310 [i.36] applies as outlined in clause 6.8.0 of the present document.

EXAMPLE: A cryptographic scheme defined by effective key length makes an assumption for immunity to brute force attack (i.e. if every key possible key is tried in sequence what is the time before the correct key is found?) which does not take into account many other factors in cryptanalysis that may weaken or invalidate the cryptographic scheme. As such attacks and cryptanalysis may take many years to develop the metrics from [1] may relegate the risk to lower than is appropriate.

5a.2 Impact metrics

The value assigned to impact shall be determined by level of harm to the asset or its stakeholders from an attack.

By default, as shown in figure 4 in clause 4.2, a system is an aggregation of assets. Therefore, any non-redundant system will fail if one system component fails, and a redundant system should only fail if multiple assets are subject to attack. Thus whilst the bulk of the TVRA method addresses the impact and attacks on a single asset due consideration should be made for the cumulative impact of attacks on multiple assets of the system, or for the cumulative impact of repeated attacks on a single asset.

Table 3: Summary of impact metric for use in risk calculation

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

5a.3 Likelihood metrics

The core technical metrics for determination of the likelihood of a particular cyber-attack are defined in clause B.6 of the Common Criteria Evaluation methodology [1] and further developed in clause 6.7 of the present document.

Table 4: Summary of likelihood metric for use in risk calculation

Value	Likelihood of occurrence	Explanation
1 (note)	Very unlikely	According to up-to-date knowledge, there are no means of solving the technical difficulties to state the threat irrespective of the motivation or resources available to the attacker.
1	Unlikely	According to up-to-date knowledge, a possible attacker needs to solve strong technical difficulties to state the threat or the motivation for an attacker is very low.
2	Possible	The technical requirements necessary to state this threat are not high and could be solved without significant effort; furthermore, there is a reasonable motivation for an attacker to perform the threat.
3	Likely	There are no sufficient mechanisms installed to counteract this threat and the motivation for an attacker is quite high.
3 (note)	Very likely	As for very likely but the threat is considered more imminent.
NOTE: The values assigned to "Very unlikely" and "Unlikely" are identical, similarly the values assigned to "Likely" and "Very likely" are identical. The rationale is that they represent extreme poles but, in each case, do not equate to risk escalation.		

6 Method process

6.1 Overview

The TVRA method systematically identifies the assets, and the relationships between assets (where the relationship can be considered as an intangible asset), and then for each asset, establishes the weaknesses this asset has, assesses how practical it is to attack this weakness and assesses the resulting likelihood of attack, which when taken alongside the impact of the attack identifies the resultant risk.

6.2 Identification of the attack surface and scope of the analysis (TVRA)

A successful TVRA depends on a clear definition of the scope, purpose and goal of the analysis and of the system being analysed. A comprehensive description of the scope of the analysis (the TVRA) and its environment shall be produced, and shall contain the following elements:

- Identification of the boundary between the system and its environment (the attack surface).
- Identification of any elements of the system that are excluded from the analysis and a justification for their exclusion.
- Identification of any decomposition of system elements (this may be necessary if an entity in the system has discrete interfaces for individual functional elements).
- Identification of the interfaces between the system and its environment.

NOTE 1: An incomplete definition of the scope of the analysis (TVRA) may mean that at least some of the security objectives specified will be impossible to meet.

There are no strict rules on how to determine what is in the system and what is in its environment but, as a guide, in communication systems it is likely that the boundary will pass through interfaces rather than entities and that human users will exist in the environment rather than the system. It is also likely that the system will comprise a number of easily identifiable assets which can be decomposed into multiple assets themselves at a later stage in the development process. The description should include a high level description of the main assets and its environment.

Figure 8: Void

It is essential to the analysis that the scope description is specific and unambiguous and that it clearly identifies the assets of both the system in scope and those it interacts with in the environment.

The use of UML use case diagrams, class diagrams, deployment diagrams, object diagrams and behavioural diagrams to model the system and its environment may be used in subsequent steps of the TVRA and may assist in other analysis activities. If such methods are used the diagrams shall be considered as part of the TVRA documentation.

The abstraction level required of the scope identification depends on the purpose of the analysis and the information available. The description may include an outline and details of the architecture, relevant applications, reference points, information flows and possible attack interfaces. Attack interfaces are specific assets in the environment, or the interfaces between the system and the environment, that a threat agent can use to launch an attack against one or more weaknesses in the assets.

NOTE 2: Attack interfaces may also be procedural (exploiting a weakness in a security procedure).

NOTE 3: The term Target of Evaluation (ToE) is used in Common Criteria Part 1 [i.27] and is equivalent to the scope of the analysis (TVRA). Common Criteria Part 1 [i.27] provides guidelines on producing TOE and TOE environment descriptions that should be considered by the analyst. ETSI TR 187 002 [i.3] provides further examples of TOE descriptions.

6.3 Identification of objectives

Security objectives identify the broad aims of a standard or system in terms of the protection to be given to users and information within the framework of the CIA paradigm and its underlying attributes. Without such objectives it is difficult to develop a coherent set of security requirements and, therefore, complete a meaningful TVRA. Security objectives should be specific to the target system and clearly specify the CIA attributes affected. The following gives a demonstration of security objectives identification and specification for the CIA attribute availability.

The objectives should be classified against the relevant CIA paradigm's attribute. Examples include the following technical security issues that arise for most ICT services:

- charging fraud;
- protection of privacy; and
- ensuring availability of the offered services.

The goals for ICT services should therefore aim to reduce these risks by reducing the ability to mount attacks that prevent the achievement of these objectives.

NOTE 1: As discussed later in the present document risk is calculated as the product of impact and likelihood of an attack occurring. As impact is considered to be mostly immutable (without changing the design or purpose of the underlying system) the security design can really only affect the likelihood of attack.

The following technical objectives for ICT services security hold:

- Prevention of masquerade:
  - being able to determine that a user claiming to be Alice is always Alice, Bob is always Bob, and where Bob cannot pretend to be Alice;
  - applies to each of masquerade of the user, of the system, and of the service.
- Ensure availability of the ICT services:
  - the service is accessible and usable on demand by an authorized entity.

NOTE 2: In general, a user expects to be able to engage a service, and complete the service without being disconnected from the service whilst the service is in progress.

- Maintain privacy of data used to enable, and in the content of, a service:
  - where the parties to a service communicate across public networks mechanisms exist to prevent eavesdropping;
  - the only delivery points for communication are the legitimate parties to the service.

6.4 Identification of functional security requirements

The system requirements are dependent on the system objectives identified in clause 6.3 and have two specialisms shown in figure 8a identifying security and assurance requirement specialisms.

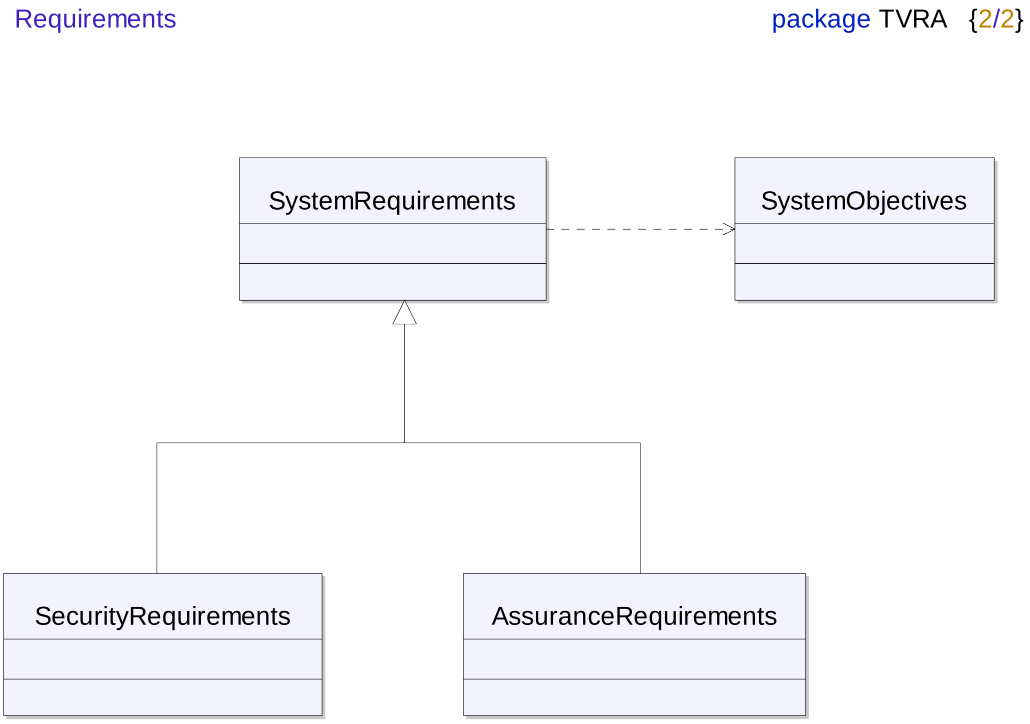


Figure 8a: Dependency relationship between requirements and objectives

When building systems the guiding principles for the content of ETSI deliverables as listed below apply:

- **Necessary:** it (a standard) should specify only what is required to meet its objectives, and not impose a particular approach to implementation.
- **Unambiguous:** it should be impossible to interpret the normative parts of the standard in more than one way.
- **Complete:** the requirement should contain all the information necessary to understand that requirement, either directly or by reference to other documents. The reader of a standard should not need to make assumptions about the implementation of any requirement.
- **Precise:** the requirement should be worded clearly and exactly, without unnecessary detail that might confuse the reader.
- **Well-structured:** the individual elements of the requirement should all be included in an appropriate and easy-to-read manner.
- **Consistent:** there should be no contradiction between different requirements within the standard, nor with other related standards.
- **Testable:** there should be clear and obvious means of demonstrating that an implementation complies with the requirement.

If using the functional capabilities from Common Criteria Part 2 [i.28] to state requirements each selected Security Functional Requirement (SFR) from [i.28] should conform to the listed principles. ETSI TR 187 011 [i.2] provides guidelines and method on how to apply Common Criteria Part 2 [i.28] requirements to ETSI standards.

The assurance requirements of the system may be determined by a number of instruments including those set for market access. An overview of the role of assurance criteria can be found in [i.2] and in ETSI TS 102 165-3 [i.49].

6.5 Systematic inventory of the assets

The Cyber Security Controls defined in ETSI TR 103 305-1 [i.33] that address the building of an inventory of hardware and software assets in the system should be used. Specifically, CSC1.1 and CSC2.1 from [i.33] should be applied.

NOTE 0: If the controls from ETSI TR 103 305-1 [i.33] (or its direct derivatives) are not applied the analyst is expected to clearly identify the means used to build the inventory of assets.

The life expectancy of the asset is used in consideration of the time taken to develop and run an attack (develop a threat agent for a specific attack type). This can be affected by aspects such as the frequency with which a key or password is updated, and the duration in which the asset is expected to be in operational use.

NOTE 1: If an asset is protected by a key or password and the attack is based on key or password guessing then the frequency of key or password update can be a countermeasure.

Three kinds of **assets** are defined:

- physical assets (i.e. equipment);
- human assets; and
- logical assets (i.e. the information stored in and handled by the physical assets).

An asset is at **risk** when a weakness exists and a **viable threat** is present. The seriousness of the **vulnerability** depends on the **value** of the **asset** and the **likelihood** of the **weakness** to be exploited by the threat.

The use of UML use case diagrams, class diagrams and object diagrams may assist in the analysis of the system to identify the assets. If such methods are used the diagrams should be used in the analysis documentation.

In order to catalogue an asset, the following attributes and relationships shall be identified:

- The system in which the asset resides.

NOTE 2: An asset can exist in more than one system and a system can contain many assets (a many-to-many relationship).

- The asset parent-child-sibling relationships if any exist.

NOTE 3: An asset can be a parent to one or more other assets and such relationships are captured. Similarly, an asset can be a peer (sibling) to another asset and such relationships are captured.

It is the impact on the system from a successful attack on a specific asset that is particularly important to identify from the TVRA. Table 5 identifies the three levels of impact used to evaluate assets in the TVRA process.

Table 5: Asset impact

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

If the analyst determines that it is unreasonable to address all possible scenarios, or determines that a reasonable understanding of the risk is not possible, the analyst may decompose the system into a system of systems. The rationale for the decomposition shall be documented and the interfaces between each decomposed sub-system clearly identified.

6.6 Systematic identification of vulnerabilities and threat level

6.6.0 Overview

In order to identify potential vulnerabilities to the system or asset and its environment it is first necessary to determine where its weaknesses exist, what, if any, viable threats could exploit those weaknesses and what harm could be caused by an attack on each weakness. A weakness with a corresponding viable threat and threat actor is considered to be a vulnerability within the system.

It may be possible to use an AI or ML system to assist in identifying weaknesses and assessing if those weaknesses map to vulnerabilities. An overview of the role of AI/ML in system vulnerability analysis is given in Annex J.

6.6.1 Identification of weakness

A weakness within a system offers a potential point of attack for a threat agent. However, viable attacks will not necessarily be possible against all weaknesses.

6.6.2 Identification of a vulnerability

Possible attack interfaces need to be identified and all possible attacks need to be elaborated. This is in addition to those already identified and involves a further analysis of such.

6.6.3 Identification of attack method

6.6.3.0 Introduction

The difficulty of mounting a successful attack is determined by a number of factors that are defined and described in detail in the remainder of this clause.

6.6.3.1 Assessment of the practicality

6.6.3.1.0 Core assessment

An evaluator shall determine the attack potential associated with each of the vulnerabilities identified and shall consider the effect of the vulnerability becoming publicly known. That is, an attacker would not have to repeat the analysis to identify the vulnerability, but would only have to perform the exploitation.

The approach defined in clause B.6 of the Common Criteria Evaluation methodology [1] applies for the assessment of the likelihood of an attack.

In direct attacks against probabilistic or permutational mechanisms, the issue of exploitation will normally be the most important, since potential vulnerabilities in these mechanisms will often be self-evident, however this may not always be the case. With cryptographic mechanisms, for example, knowledge of subtle potential vulnerabilities can considerably affect the effectiveness of a brute force attack. Knowledge that users of a system tend to choose first names as passwords will have a similar effect. The initial identification of potential vulnerabilities will become a much more important consideration, since the existence of difficult to uncover potential vulnerabilities can be promulgated, often rendering exploitation trivial.

6.6.3.1.1 Knowledge factor

The knowledge factor is defined in clause B.6 of the Common Criteria Evaluation methodology [1] with the following notes to be taken into account.

The knowledge of the asset may graduate according to design abstraction, although this can only be done on an asset by asset basis. Some asset designs can be public sources (or heavily based on public sources) and therefore even the design representation would be classified as public or at most restricted, while the implementation representation for other assets is very closely controlled as it would give an attacker information that would aid an attack and is therefore considered to be sensitive or even critical.

NOTE 1: Open source software is an example of asset design or implementation that is wholly in the public domain, however the level of risk represented by open source is tempered by the level of vulnerability it exhibits. There is some evidence that open source software is open to greater scrutiny to resolve errors but it is stressed that the weighting here is only intended to be on the asset itself.

NOTE 2: Public vulnerability databases may be used by the attacker to gain knowledge of particular implementations and as such where a deployed product has not been updated to mitigate any such publicly declared vulnerability it should be considered as high risk by default.

Care should be taken here to ensure the highest level of knowledge of the asset required during identification, development and running of the potential vulnerability is identified.

6.6.3.1.2 Time factor

The time factor is defined in clause B.6 of the Common Criteria Evaluation methodology [1] with the following notes to be taken into account.

The time factor suggests that anything greater than a few months, when added to the other factors, suggests an unlikely attack. This should be addressed with care as there are several scenarios where a conceptual attack may be possible only given years of development that would suggest a low risk, but when the mitigation is taken into account, and particularly the time to develop or implement a mitigation, the delta time becomes important (i.e. the time between an attack being viable and a mitigation being viable), and may be sufficient to make the risk critical. This is addressed in more detail in clause 6.8.0 below.

EXAMPLE: The time taken to identify a potential vulnerability can be the time taken to locate the potential vulnerability from information that is publicly available or can be the time required to analyse the design information to identify a potential vulnerability.

In addition to this time taken for identification, consideration of the time required to develop an attack method (which can also be publicly available) and to successfully mount the attack on the asset to exploit the vulnerability shall be included in this factor.

6.6.3.1.3 Expertise factor

The expertise factor is defined in clause B.6 of the Common Criteria Evaluation methodology [1] with the following notes to be taken into account.

When describing the expertise required, the total number of experts required shall be included; the number of people for each type of expertise required and access to the expertise (dissemination) shall be considered when describing the expertise required. Therefore, if expertise in both techniques for types of attack applicable to the asset and underlying algorithms and protocols is required, then the highest level of Multiple Specialist Expertise characterization should be assumed.

6.6.3.1.4 Opportunity factor

The opportunity factor is defined in clause B.6 of the Common Criteria Evaluation methodology [1] with the following notes to be taken into account.

For the purposes of this clause unnecessary/unlimited access means that the attack does not need any kind of opportunity to be realized; easy means that access is required for less than a day or that the number of asset samples required to perform the attack is less than ten; moderate means that access is required for less than a month or that the number of asset samples required to perform the attack is less than fifty; difficult means that access is required for at least a month or that the number of asset samples required to perform the attack is less than one hundred; none means that the opportunity window is not sufficient to perform the attack (the length for which the asset to be exploited is available or is sensitive is less than the opportunity length needed to perform the attack - for example, if the asset key is changed each week and the attack needs two weeks).

The actual number of samples of an asset should not be considered fixed but rather should be considered against what would be a normal supply amount.

EXAMPLE: If a normal residential consumer attempts to hold more than a reasonable number of samples for residential use it can be characterized as the precursor to an attack.

Consideration of this factor can result in determining that it is not possible to complete the exploit, due to requirements for time availability that are greater than the opportunity time.

6.6.3.1.5 Equipment factor

The equipment factor is defined in clause B.6 of the Common Criteria Evaluation methodology [1] with the following notes to be taken into account.

Specialist expertise and knowledge of the asset are concerned with the information required for persons to be able to attack an asset. There is an implicit relationship between an attacker's expertise (where the attacker can be one or more persons with complementary areas of knowledge) and the ability to effectively make use of equipment in an attack. The weaker the attacker's expertise, the lower the potential to use equipment (IT hardware/software or other equipment). Likewise, the greater the expertise, the greater the potential for equipment to be used in the attack. Although implicit, this relationship between expertise and the use of equipment does not always apply, for instance, when environmental measures prevent an expert attacker's use of equipment, or when, through the efforts of others, attack tools requiring little expertise to be effectively used are created and freely distributed (e.g. via the Internet).

In applying specialist software such as AI and ML (see also Annex J) the requirements for developing training data and applying it to the active system should be considered as bespoke even if that software will run on standard equipment.

6.6.3.1.6 Intensity factor

The intensity of an attack can be a factor in determining risk to the system or asset under attack. Table 6 identifies three possible levels of attack intensity and assigns values to each for use in the subsequent threat analysis.

Table 6: Attack intensity levels

Attack intensity	Value
Single instance of attack	0
Moderate level of multiple instances	1
Heavy level of multiple instances	2

The intensity of an attack can be modified by use of:

- distributed threat agents (many sources of attack);
- reducing the time interval between attacks; or
- by combining these two.

In the simplest case a threat agent is assumed to operate at one place for one instance of an attack in any one time period (where even if the attack is repeated the interval between attacks is greater than the asset recovery time such that the attacks can be considered as discrete). For many attacks where manual processes need to be executed at a particular location (such as intercepting a physical line) this is an adequate point of view. In many practical implementations or deployments, including those considered in standards development, consideration only of the discrete attack can be insufficient for risk analysis. Assets are often automated and accessible via networks, and as threat agents are also assets, then so can the attacks be automated and network accessible.

A particular instance of the impact of intensity is that of a Distributed Denial of Service attack (see also Annex C of ETSI TS 102 165-2 [i.47]).

6.6.4 Identification of threat agents

A *threat agent* is an entity that can adversely act on assets. There exist different types of threat agents. The objective and the extent to which a threat agent is motivated and capable to successfully mount an attack on an asset differs per threat agent.

NOTE 1: Capability and motivation are treated separately in the application of the method but are then combined to determine the risk of a threat being enacted.

An evaluator shall identify threat agents that potentially want to launch an attack, and shall determine the threat level represented by each of these threat agents. The threat level is a value attributed to the combination of the capability and motivation of a threat agent to attack an asset. Capability is a characteristic of a threat agent that defines the level of technical sophistication of the threat. Motivation is a measure of how much a threat agent desires to attack and compromise an asset or group of assets. See Annex B for more information.

It may be beneficial for the analysis to distinguish between the threat source and the threat actor. A *threat source* is a person or organization that desires to breach security and ultimately will benefit from a compromise in some way (e.g. nation state, criminal organization, activist) [i.10].

A *Threat Actor* is a person, or group of persons, who actually performs the attack (e.g. hackers, script kiddy, insider (e.g. employee), physical intruders) [i.10]. A threat source can recruit, influence or coerce a threat actor to mount an attack on their behalf. In the simplest case the *threat source* and the *threat agent* are the same entity and are treated as synonyms in the remainder of the present document.

NOTE 2: An AI or ML entity can act as a proxy for the threat actor (see also Annex J), and can be conceived as being both the threat source and the threat actor (see also Annex K).

In considering the role of motivation as it influences threat level, table 7 categorizes motivation levels. Table 8 presents a measure of the capability of the attacker. The motivation level and capability level are mapped to identify the threat level (see table 9).

Table 7: Motivation levels

Motivation levels	Description
Very low (indifferent)	The system is considered to have limited to no value to the threat agent, thus the threat agent is very unlikely to attempt any attack on the system.
Low (curious)	The system is considered to have minimal value to the threat agent. Threat agents can attempt to attack the system out of curiosity or opportunistic motivation. Non system deterrents (see note 1) can be sufficient to deter the threat agent from initiating the attack (e.g. due to potential ramifications if the agent can be linked to the attack).
Medium (interested)	The system is considered to have moderate value to the threat agent. The threat agent will attempt to attack the system on a frequent basis. It is also considered unlikely that the threat agent can be deterred from initiating the attack by the existence of non-system deterrents.
High (committed)	The system is considered to have significant value to the threat agent. The threat agent will attempt to attack the system on a persistent and frequent basis. It is considered highly unlikely that the threat agent can be deterred from initiating the attack by the existence of non-system deterrents.
Very high (focused)	Threat agent has a primary aim to attack the system (see note 2).
NOTE 1: A non-system deterrent can include the criminalisation under law of the attack and a sufficient judiciary penalty (e.g. interment, financial penalty), with adequate law enforcement resources to capture and prosecute the threat agent. NOTE 2: In a fully automated attack including those driven by AI/ML (see Annex J) the motivation can be considered to default to very high (as the sole purpose of the AI/ML software is to attack the system), although the intent to develop such an attack can be assigned to any of the motivation levels.	

The determination of motivation, as discussed in Annex B, is not generally considered as deterministic. However, where sufficient resources can be applied to determine the level of motivation tables 8 and 9 consider the combination of threat agent capability and threat agent motivation to map a value for threat level.

Table 8: Capability levels

Capability levels	Description
Very little	Threat agent has almost no capabilities or resources. Matches an attack potential of Basic.
Little	Threat agent has very modest capabilities and resources. Matches an attack potential of Enhanced-Basic.
Limited	Threat agent has modest capabilities and resources. Matches an attack potential of Moderate.
Significant	Threat agent is capable and has significant resources. Matches an attack potential of High.
Formidable	Threat agent is extremely capable and well-resourced. Matches an attack potential of Beyond High.

Table 9: Mapping of motivation with capability to identify threat level

Motivation	Capability				
	Very little	Little	Limited	Significant	Formidable
Very low (indifferent)	Negligible	Negligible	Low	Low	Low
Low (curious)	Negligible	Negligible	Low	Low	Moderate
Medium (interested)	Negligible	Low	Moderate	Severe	Severe
High (committed)	Low	Low	Moderate	Severe	Critical
Very high (focused)	Low	Moderate	Severe	Critical	Critical

6.7 Calculation of the likelihood of the attack and its impact

The weighted summation approach defined in clause B.6 of the Common Criteria Evaluation methodology [1] (and summarised in table 10) applies in order to determine the attack potential with the following deviations.

Each of the attack factors shall be summed (i.e. Time + Expertise + Knowledge + Opportunity + Equipment) to give an overall attack potential rating as shown in table 10. The attack potential value shall then be mapped to a vulnerability rating (table 11). The vulnerability rating shall then be combined with the threat level using table 12 to obtain the Occurrence likelihood. The computation template is given in Annex G.

Where an attack is carried out with an AI or ML enabled threat agent there are several distinct stages in development of the attack which are addressed in Annexes J and K for the machine learning cycle.

Table 10: Attack potential

Factor	Range	Value
Time (elapsed time)	≤ 1 day	0
	≤ 1 week	1
	≤ 2 weeks	2
	≤ 1 month	4
	≤ 2 months	7
	≤ 3 months	10
	≤ 4 months	13
	≤ 5 months	15
	≤ 6 months	17
	> 6 months (see note 1)	19
Expertise	Layman	0
	Proficient	3
	Expert	6
	Multiple experts	8
Knowledge	Public	0
	Restricted	3
	Sensitive	7
	Critical	11
Opportunity	Unnecessary/ unlimited access	0
	Easy	1
	Moderate	4
	Difficult	10
	None (see note 2)	999
Equipment	Standard	0
	Specialized (see note 3)	4
	Bespoke	7
	Multiple bespoke	9
NOTE 1: A successful attack requires in excess of 6 months. NOTE 2: None means that the window of opportunity is not sufficient to perform the attack. NOTE 3: If clearly different groups of specialized equipment are required for distinct steps of an attack, this should be rated as bespoke.		

Table 11: Vulnerability rating

Attack potential values	Attack potential required to exploit attack	Resistant to attacker with attack potential of
0 to 9	Basic	No rating
10 to 13	Enhanced-basic	Basic
14 to 19	Moderate	Enhanced basic
20 to 24	High	Moderate
> 24	Beyond High	High

The method for threat analysis defined in ETSI ETR 332 [i.9] combines the likelihood with the impact of the attack in determining if a countermeasure should be applied. The form of countermeasures can include redesign of the element at risk in the system to remove the vulnerability that is to be attacked, and application of a defensive system component that masks the vulnerability. The vulnerability rating and threat level can be mapped to the likelihood of attack as shown in table 12.

Table 12: Mapping of vulnerability rating with Threat level to identify likelihood of attack

Vulnerability rating	**Threat level**				
	Negligible	**Low**	**Moderate**	**Severe**	**Critical**
Basic	Possible	Likely	Very Likely	Very Likely	Very Likely
Enhanced Basic	Unlikely	Possible	Likely	Very Likely	Very Likely
Moderate	Very Unlikely	Unlikely	Possible	Likely	Very Likely
High	Very Unlikely	Very Unlikely	Unlikely	Possible	Likely
Beyond High	Very Unlikely	Very Unlikely	Very Unlikely	Unlikely	Possible

6.8 Determination of the risks

6.8.0 Overview

For each of the assets in the system under study one can identify their vulnerabilities and corresponding threats and weaknesses. For each vulnerability the likelihood should be computed as described in clause 6.7 above. For each asset the risk associated with each vulnerability should be computed. The computation template to support the calculation of risk is given in Annex H.

It is highly likely that long term existential risks to systems can be mis-identified using the metrics from the Common Criteria Evaluation methodology [1]. This is particularly true for assessing the long term evolution of security from one paradigm to another. In all cases the following approach to evaluation of the risk shall be derived from the equation for quantum safe development given in ETSI EG 203 310 [i.36] as below:

- X = the time that the asset needs to remain secure (against violation of any of the CIA attributes of its protection scheme).
- Y = the time it will take to replace the current protection system with one that is safe against new attacks.
- Z = the time it will take to break the security (i.e. any of the CIA attributes) of the protection mechanisms of the asset.
- T = the time it will take to develop trust in the new security mechanism.

If "X + Y + T > Z" any data protected by an existing scheme is at risk and for the purposes of the present document shall be classified as critical risk (often this should be considered as an existential risk as the current methods of protection will be made null and void against the new attacks).

The Y factor is very dependent on the nature of the cryptographic deployment. Similarly, the X factor is dependent on the nature of the data being protected with some data (e.g. eHealth records) requiring protection for decades, whereas signalling data (e.g. DHCP derived IP addresses) may only require protection for a few minutes (e.g. the lease period of a DNCP derived IP address). Where justified assessments of each of the factors above (X, Y, Z, T) can be made and where the calculation "X+Y+T>Z" is true then the time factor should be assessed at a level equivalent to a zero day attack (i.e. where an attack is considered viable and likely as soon as the asset is deployed).

If the "X + Y + T > Z" as above is true then the metric based analysis defined in the Common Criteria Evaluation methodology [1] does not apply.

EXAMPLE: In the quantum safe cryptography arena, the existence of Shor's algorithm identifies a valid conceptual threat to conventional asymmetric key cryptography even if the existence of a relevant quantum computer remains some years distant. However, the factors Y and T above then become significant and may result in the "X + Y + T > Z" assessment being true almost irrespective of the value assigned to Z if the realisation of relevant quantum computer is reassigned from a theoretical problem to an engineering problem.

6.8.1 Impact of intensity

The overall impact on a system of a particular threat can vary with the intensity with which the attack is mounted. The resulting impact, shown in table 13, is determined by summing the asset impact value (from table 5) and the attack intensity value (from table 6).

Table 13: Result on overall Impact of varying attack intensity

Asset Impact	Attack Intensity	Resulting Impact
1	0	1
1	1	2
1	2	3
2	0	2
2	1	3
2	2	3 (see note)
3	0	3
3	1	3 (see note)
3	2	3 (see note)
NOTE: The Asset Impact is assigned a value in the range of 1 to 3. Consequently, any Resulting Impact value calculated to be greater than 3 is given the value of 3.		

6.8.2 Classification of risk

6.8.2.1 Overview

Risk is defined as the product of the likelihood of an attack (occurrence likelihood) and the impact of the attack on the system.

The likelihood of a threat occurring (occurrence likelihood) may be estimated with values from 1 to 3 as explained in table 14 (Occurrence likelihood). Capability and motivation are each taken into account in the calculation of likelihood. A highly motivated and capable threat agent (e.g. a nation state with a cyber division) will be able to attack successfully even if the vulnerability rating is "beyond high" which results in a likelihood evaluation of possible.

Table 14: Occurrence likelihood

Value	Likelihood of occurrence	Explanation
1 (note 1)	Very unlikely	According to up-to-date knowledge, there are no means of solving the technical difficulties to state the threat irrespective of the motivation or resources available to the attacker.
1	Unlikely	According to up-to-date knowledge, a possible attacker needs to solve strong technical difficulties to state the threat or the motivation for an attacker is very low.
2	Possible	The technical requirements necessary to state this threat are not high and could be solved without significant effort; furthermore, there is a reasonable motivation for an attacker to perform the threat.
3	Likely	There are no sufficient mechanisms installed to counteract this threat and the motivation for an attacker is quite high.
3 (note 1)	Very likely	As for very likely but the threat is considered more imminent.
NOTE 1: The values assigned to "Very unlikely" and "Unlikely" are identical, similarly the values assigned to "Likely" and "Very likely" are identical. The rationale is that they represent extreme poles but, in each case, do not equate to risk escalation. NOTE 2: As noted in clause 6.8.0 for special cases such as that of a quantum computer attacking systems based on conventional asymmetric cryptography the likelihood should be considered as "Likely" irrespective of the current state of the art of development of quantum computers.		

The impact of a threat is also estimated with values from 1 to 3 as explained in table 3 in clause 5a.2 and extended in table 10 when attack intensity is considered.

The product of occurrence likelihood (from table 15) and impact value (from table 14) as defined in clause 6.6 gives the risk which serves as a measurement for the risk that the concerned asset is compromised. The result is classified into three categories of risk as shown in table 16.

Table 15: Risk

Value	Risk	Explanation
1, 2	Minor	No essential assets are concerned, or the attack is unlikely. Threats causing minor risks have no primary need for counter measures.
3, 4	Major	Threats on relevant assets are likely to occur although their impact is unlikely to be fatal. Major risks should be handled seriously and should be minimized by the appropriate use of countermeasures.
6, 9	Critical	The primary interests of the providers and/or subscribers are threatened and the effort required from a potential attacker's to implement the threat(s) is not high. Critical risks should be minimized with highest priority.
NOTE: Because risk is calculated as the product of likelihood and impact the values 5, 7 and 8 cannot occur.		

6.9 Security countermeasure identification

6.9.0 Introduction

Security Countermeasures are assets that are added to the system to reduce the weighted risk to the system. The purpose of countermeasures is to reduce either the likelihood of an attack or to the attack impact. Security countermeasures are modelled in the TVRA as instances of assets and whilst primarily logical can also be human or physical. The general security model can be summarised in the triplets shown below for each of the model and its implementation:

- Model: {threat, security-dimension, countermeasure}
- Implementation: {interception, confidentiality, encryption}

Thus, it should be clear which threat is addressed and by what measure.

NOTE 0: A framework of security countermeasures is described in ETSI TS 102 165-2 [i.47].

There might be several alternative countermeasures and these should first be identified, then evaluated and compared to identify the costs and benefits of each so that an informed decision can be made of which countermeasures to select.

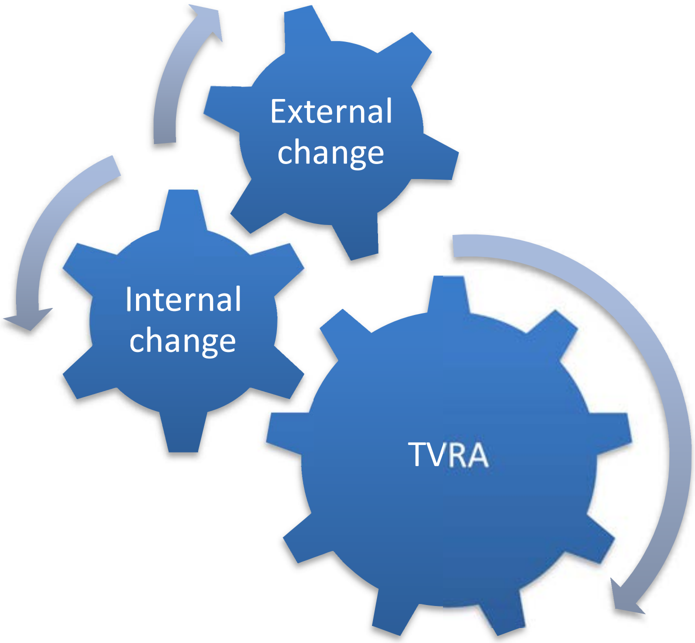


Figure 9: Cyclical nature of TVRA

Figure 9 shows that countermeasures are added as internal changes to the system and thus for change to the system the TVRA process shall be repeated. This should continue either until no further countermeasures can be applied (indicating stability in the system) or until the level of risk identified is considered as acceptable (residual risk).

NOTE: Some countermeasures can be inferred by inspection of the security requirements.

6.9.1 Countermeasures in the system

Where a countermeasure has been defined, or is implemented, as a logical asset it will require to be deployed in a corresponding physical assets (e.g. a firewall rule requires a firewall). The countermeasures and their supporting physical assets bring their own vulnerabilities and as noted above the TVRA shall be re-applied with the countermeasures included in the scope of the TOE.

6.9.2 Composite countermeasures applied to the system

More than one countermeasure may be applied against a single threat agent, or to protect a single asset. In such case the residual risk is only identified by re-performing the TVRA.

6.9.3 Impact of composite countermeasures applied to the system

The impact of countermeasures on the overall risks analysis takes a similar approach as the automated threat agents. In this case the least likely of the two values is taken for each of the likelihood parameters. The impact of the countermeasures on the impact is similarly calculated by taking the least impact. This calculation shall be applied after assessing the impact of automated threat agents.

6.10 Countermeasure Cost-benefit analysis

6.10.0 Introduction

More than one countermeasure can be effective in reducing particular risks or the overall set of risks. The TVRA method specifies a countermeasure cost-benefit analysis for this purpose. The goal of the analysis is to identify the most cost-effective countermeasure of the alternatives. The main benefit of any countermeasure is the mitigation of attack measures that results in both added security and in the introduction of explicit attack protection. Other benefits can be increased market acceptance and improved regulatory compliance. Costs are not merely economical aspects, but affect standardization, implementation and operation. The countermeasure cost-benefit template and tool are given in Annex H.

6.10.1 Standards design

Introducing countermeasures to a standard under development or an existing standard (published) can impose changes affecting the time schedule and resulting in additional effort and cost. The level to which a countermeasure affects the standard design is measured according to the scale in table 16.

Table 16: Standards design evaluation

Scale	Description	Assigned value
No Impact	No effect on the time schedule and resources needed of standards under development or no changes needed on existing and published standards.	0
Low Impact	No significant time delay or additional resource demand for standards under development or changes needed on existing and published standards.	1
Medium Impact	Significant time delay and additional resource demand for standards under development and significant changes needed on existing and published standards.	4
Major Impact	Unacceptable time delay and additional resource demand for standards under development and unacceptable changes needed on existing and published standards.	9

6.10.2 Implementation

Adding countermeasures to standards can affect its adoption and implementation in the targeted user community. This is an important aspect of standards adoption and crucial for countermeasure cost-benefit analysis. The level to which a countermeasure affects implementation of the standard is measured according to the scale in table 17.

Table 17: Implementation evaluation

Scale	Description	Assigned value
No Impact	No effect on standards adoption in the targeted user community.	0
Low Impact	No significant effect on standards adoption in the targeted user community.	1
Medium Impact	Significant effect on standards adoption in the targeted user community.	4
Major Impact	Unacceptable effect on standards adoption in the targeted user community.	9

6.10.3 Operation

Countermeasures can impact the ongoing operation of standardized products or systems once they have been deployed into an operational environment. The level to which a countermeasure affects the operation of standardized products is measured according to the scale in table 18.

Table 18: Operation evaluation

Scale	Description	Assigned value
No Impact	No effect on operation of realized standards design and targeted operational environment.	0
Low Impact	No significant effect on operation of realized standards design or targeted operational environment.	1
Medium Impact	Significant effect on operation of realized standards design and targeted operational environment.	4
Major Impact	Unacceptable effect on operation of realized standards design and targeted operational environment.	9

6.10.4 Regulatory impact

Regulatory impacts concern the influence that the countermeasure can have on ensuring regulatory compliance. Regulatory impact is evaluated according to the scale in table 19.

Table 19: Regulatory impact evaluation

Scale	Description	Assigned value
Severe Negative Impact	Unacceptable effect on regulatory compliance requirements.	-9
Negative Impact	Significant negative effect on regulatory compliance requirements.	-4
No Impact	No effect on regulatory compliance requirements.	0
Positive Impact	Significant positive effect on regulatory compliance requirements.	4
Severe Positive Impact	Very favourable effect on regulatory compliance requirements.	9

In addition to the role of regulatory impact evaluation it is also essential to consider the regulatory environment when assessing the environment as it can be necessary to meet certain regulatory constraints that will require security measures even if the risk calculation would suggest otherwise.

EXAMPLE: In the EU context any processing of personal data is considered with respect to the GDPR [i.44] and the necessary assets built into the system. Thus, data may need to be stored in encrypted form with strict access controls even if that data can only be accessed programmatically and no viable attack is identified as there is a regulatory constraint where if no action is taken and data does leak the organisation is at significant financial risk. In such cases in addition to the core TVRA method defined in the present document additional analysis such as that covered by a Data Protection Impact Assessment [i.48] is undertaken.

6.10.5 Market acceptance

Adoption of a standard into industrial products and its acceptance by the targeted user community determine the success of a standard. Therefore, countermeasures with negative predicted effect on market acceptance should be carefully analysed. The level to which a countermeasure affects market acceptance of the standard is measured according to the scale in table 20.

Table 20: Market acceptance evaluation

Scale	Description	Assigned value
Severe Negative Impact	Unacceptable effect on market acceptance.	-9
Negative Impact	Significant negative effect on market acceptance.	-4
No Impact	No effect on market acceptance.	0
Positive Impact	Significant positive effect on market acceptance.	4
Severe Positive Impact	Very favourable effect on market acceptance.	9

6.11 Specification of detailed requirements

Security requirements should be identified for both the asset and, where applicable, its environment. Detailed requirements are refined from the functional security requirements and the security services and capabilities of the countermeasures and security requirements identified as the result of the application of the TVRA method. Guidelines for the specification of detailed requirements are given in ETSI TR 187 011 [i.2].

Annex A (normative): TVRA pro forma

Notwithstanding the provisions of the copyright clause related to the text of the present document, ETSI grants that users of the present document may freely reproduce the TVRA definition pro forma in this annex so that it can be used for its intended purposes and may further publish the completed TVRA definition.

A Security Environment			
a.1 Assumptions			
a.1.1	*Text of assumption*		*Citation for full text*
a.1.2			
a.2 Assets			
a.2.1	*Short text describing asset*		*Citation for full text*
a.2.2			
a.3 Threat agents			
a.3.1	*Short text describing threat agent*		*Citation for full text*
a.3.2			
a.4 Threats			
a.4.1	*Short text describing threat*		*Citation for full text*
a.4.2			
a.5 Security policies (OPTIONAL)			
a.5.1	*Short text describing security policy*		*Citation for full text*
a.5.2			
B Security Objectives			
b.1 Security objectives for the asset			
b.1.1	*Short text describing objective for the asset*		*Citation for full text*
b.1.2			
b.2 Security objectives for the environment			
b.2.1	*Short text describing objective for the requirement*		*Citation for full text*
b.2.2			
C IT Security Requirements			
c.1 Asset security requirements			
c.1.1 Asset security functional requirements			
c.1.1.1	*Short text describing security functional requirement*	*CC class*	*Citation for full text*
c.1.1.2			
c.1.2 Asset security assurance requirements			
c.1.2.1	*Short text describing security assurance requirement*	*CC class*	*Citation for full text*
c.1.2.2			
c.2 Environment security requirements (OPTIONAL)			
c.2.1	*Short text describing security environment requirement*	*CC class*	*Citation for full text*
c.2.2			
D Application notes (OPTIONAL)			
E Rationale			
The eTVRA should define the full rational, if this is true only a citation (reference) to the full text is required			

Annex B (informative): The role of motivation

A full critique of the role of motivation in attacking a system when viewed in the context of Common Criteria evaluation can be found in clause B.6.1.2 of the Common Criteria Evaluation methodology [1]. In the present document motivation is addressed in broadly similar terms as a factor in determining attack potential.

Motivation can be used to describe aspects both of the attacker, and of the system (assets) he is attacking. The following key criteria may be considered when evaluating motivation:

- The likelihood of an attack:
  - If a threat is highly motivated an attack can be considered imminent, with a corollary of.
  - If a threat is unmotivated no attack can be anticipated.
- The value of the asset, monetarily or otherwise, to either the attacker or the asset holder:
  - An asset of very high value is likely to motivate an attack, with a corollary of.
  - An asset of little value is unlikely to motivate an attack.
- The expertise and resources with which an attacker is willing to effect an attack:
  - A highly motivated attacker is likely to acquire sufficient expertise and resources to defeat the measures protecting an asset, with a corollary of.
  - An attacker with significant expertise and resources is not willing to effect an attack using them if the attacker's motivation is low.

In each case there is no probabilistic means of determining the role of motivation in mounting an attack. However, in assessing threat potential it is essential to consider motivation in order to minimize the effect of motivation on the attacker.

Whilst it can be attested that mitigation of common attacks against known vulnerabilities can be reduced by the development of a degree of cyber-herd immunity by the encouragement of a significant proportion of the community to implement a proven countermeasure there is a corollary that attackers can be motivated by similar herd behaviour. Thus, it can be that attack and countermeasures move in and out of fashion and a visibly successful attack can motivate similar, copycat attacks. The role of cyber-herd immunity in such cases requires that a countermeasure is spread across all potentially vulnerable systems with an associated impact of reducing the likelihood of an exploit finding an attack surface. This herd immunity is particularly effective in demotivating those seeking to use simple attack vectors across multiple targets.

NOTE: For common platforms the attack surface can be, for example, an operating system vulnerability but if there are millions or 10 s or 100 s of millions of instances of the vulnerable code then only herd immunity will work to demotivate an attacker.

Annex C:
Void

Annex D: Void

Annex E:
Void

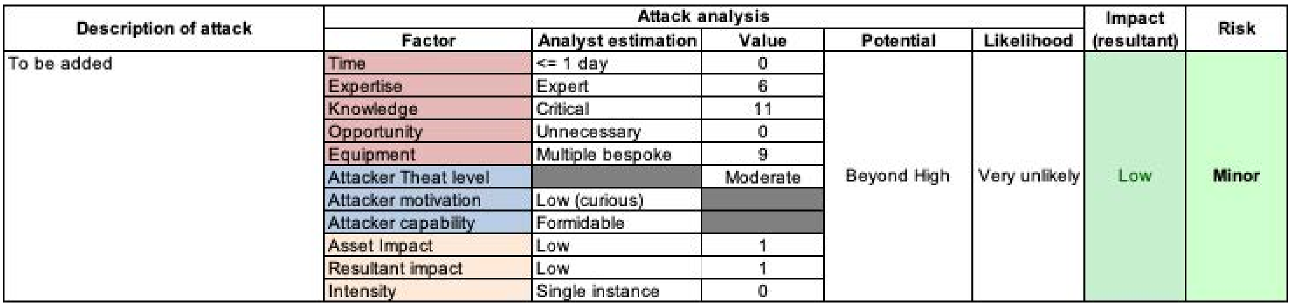
Annex F:
Void

Annex G (informative): TVRA Risk Calculation Template and Tool

The evaluation and calculation of the factors that affect the risks posed by particular threat groups (as defined in clause 6 of the present document) have been consolidated into a MS Excel® spreadsheet available as an electronic attachment in ts_10216501v050301p0.zip which accompanies the present document. An example entry in this spreadsheet is shown in table G.1.

NOTE: Excel® is the trade name of a product supplied by Microsoft. This information is given for the convenience of users of the present document and does not constitute an endorsement by ETSI of the product named. Equivalent products may be used if they can be shown to lead to the same results.

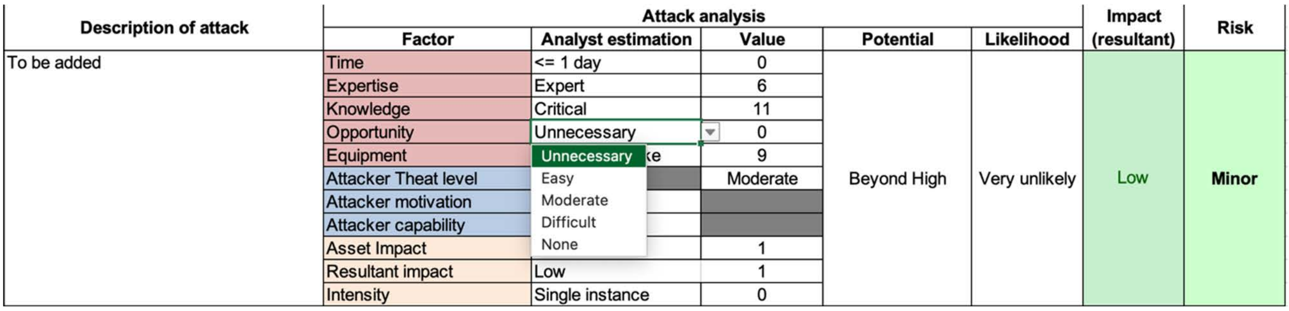
Table G.1: Example row entry in the TVRA risk calculation spreadsheet



Description of attack	Attack analysis					Impact (resultant)	Risk
	Factor	Analyst estimation	Value	Potential	Likelihood		
To be added	Time	<= 1 day	0	Beyond High	Very unlikely	Low	Minor
	Expertise	Expert	6				
	Knowledge	Critical	11				
	Opportunity	Unnecessary	0				
	Equipment	Multiple bespoke	9				
	Attacker Theat level		Moderate				
	Attacker motivation	Low (curious)					
	Attacker capability	Formidable					
	Asset Impact	Low	1				
	Resultant impact	Low	1				
	Intensity	Single instance	0				

Each of the values in the "Analyst estimation" column can be selected from drop-down lists which limit the entry to legitimate values only as shown in table G.2.

Table G.2: Entering data into the risk calculation spreadsheet



Description of attack	Attack analysis					Impact (resultant)	Risk
	Factor	Analyst estimation	Value	Potential	Likelihood		
To be added	Time	<= 1 day	0	Beyond High	Very unlikely	Low	Minor
	Expertise	Expert	6				
	Knowledge	Critical	11				
	Opportunity	Unnecessary	0				
	Equipment	ke	9				
	Attacker Theat level		Moderate				
	Attacker motivation						
	Attacker capability						
	Asset Impact		1				
	Resultant impact	Low	1				
	Intensity	Single instance	0				

The attached spreadsheet provides for auto-calculation of the content of the Potential, Likelihood, Impact and Risk columns.

Annex H (informative): TVRA Countermeasure Cost-Benefit Analysis Template and Tool

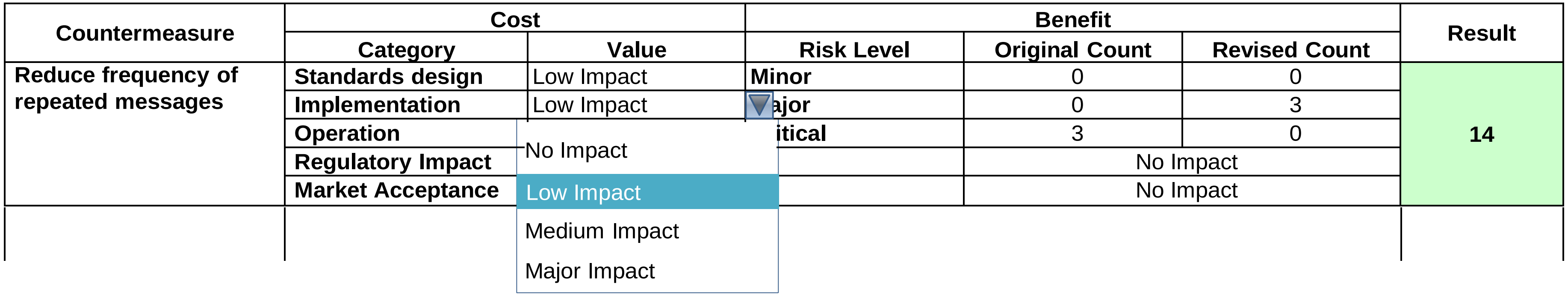
The calculations described in clause 6 of the present document for analysing the costs and benefits of specific countermeasure solutions have been consolidated into a MS Excel® spreadsheet that is available as an electronic attachment in ts_10216501v050301p0.zip which accompanies the present document. An example entry in this spreadsheet is shown in table H.1.

Each of the values in the "Cost/Value" column and the "Regulatory Impact" and "Market Acceptance" can be selected from drop-down lists which limit the entry to legitimate values only as shown in table H.2. The "Original Count" column in the "Benefits" section of the sheet should show number of critical, major and minor risks related to the countermeasure calculated before its implementation. The "Revised Count" column shows the appropriate numbers of risks calculated after the countermeasure has been implemented.

Table H.1: Example row entry in the Countermeasures Cost-Benefit Analysis table

Countermeasure	Cost		Benefit			Result
	Category	Value	Risk Level	Original Count	Revised Count	
Reduce frequency of repeated messages	Standards design	Low Impact	Minor	0	0	14
	Implementation	No Impact	Major	0	3	
	Operation	No Impact	Critical	3	0	
	Regulatory Impact			No Impact		
	Market Acceptance			No Impact		

Table H.2: Entering data into the cost/benefit calculation spreadsheet



Countermeasure	Cost		Benefit			Result
	Category	Value	Risk Level	Original Count	Revised Count	
Reduce frequency of repeated messages	Standards design	Low Impact	Minor	0	0	14
	Implementation	Low Impact	ajor	0	3	
	Operation		itical	3	0	
	Regulatory Impact			No Impact		
	Market Acceptance			No Impact		

Annex I (informative): Bibliography

I.1 UML

The following sources may give the reader a deeper understanding of the use and application of UML and of UML2 in particular.

[UML2-Style] "The elements of UML™ 2.0 style", Scott W. Ambler, Cambridge University Press, 2005. ISBN 0-521-61678-6.

[UML2-Doldi] "UML 2 illustrated: Developing real-time & communications systems", Laurent Doldi, TMSO 2003. ISBN 2-9516600-1-4.

[UML2-OReilly] "UML 2.0 in a nutshell", Dan Pilone with Neil Pitman, O'Reilly. ISBN 0-596-00795-7.

I.2 Others

- ETSI ES 282 004: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture; Network Attachment Sub-System (NASS)".
- IETF RFC 2535: "Domain Name System Security Extensions".
- IETF RFC 3403: "Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database".
- IETF RFC 2915: "The Naming Authority Pointer (NAPTR) DNS Resource Record".
- Draft-ietf-dnsext-dnssec-protocol-06 (2004): "Protocol Modifications for the DNS Security Extensions".
- Draft-ietf-dnsext-dnssec-records-08 (2004): "Resource Records for DNS Security Extensions".
- Draft-ietf-dnsext-dnssec-intro-11 (2004): "DNS Security Introduction and Requirements".
- ETSI TR 102 420: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Review of activity on security".
- Fishburn, P.C. (1967): "Additive Utilities with Incomplete Product Set: Applications to Priorities and Assignments". Journal of the Operations Research Society of America. doi:10.1287/opre.15.3.537.

Annex J (informative): AI and ML application to TVRA process

J.1 Overview

The software tools identified in the class of Artificial Intelligence (AI), or Machine Learning (ML), may be used to perform some of the tasks of analysis or of attack. In general, in all models AI and ML there are 3 broad steps:

1) Data gathering.

2) Data processing.

3) Applying insights gained from the data processing.

It is stated in ETSI GR SAI 001 [i.35] that the use of AI is unlikely to change the impact of a successful exploitation. However, it can increase the likelihood of an organization being targeted and/or of attack attempts being successful, and hence can increase the overall risk.

The relative novelty of AI and ML over other software processing is that they allow inference from data to determine outputs, meaning that programs have a dependence on the training data that they are constructed from, which can be exploited in several ways. Datasets in an AI system hence represent significant assets with a different type of relationship to other components. It is also noted that an AI asset is mutable in that how it behaves is dependent on the logic of the AI/ML component and on the nature of the inputs.

Thus, in the specific system model identified for the application of the TVRA given in in figure 4 of clause 4.2 of the present document the role of AI can be seen at least as follows:

- AI acting in lieu of a (human) threat agent;
- AI as a specific asset of the system (i.e. as a designed in element) and integral to the system design;
- AI as an instance of a countermeasure to protect specific assets in the system;
- AI as an instance of a specific threat against known weaknesses in the system.

The data dependence in AI and ML processing also means that for any given input, one cannot expect a single, testable expected output, as one might from a traditional software system. This means that small variations in the system outputs could be hiding a deliberate alteration made by an attacker and adds an additional level of complexity to assessing risks and assuring the security of systems.

It is stated in [i.35] that acquired intelligence, i.e. intelligence from learning, requires knowledge of data semantics (i.e. what data elements mean) and data context (i.e. how data elements are related), and conventional domain ontologies offer this form of data labelling. The richer the ontology of the input data, i.e. the more that data is labelled, the closer the ontology is to the world model required by the AI to represent the world view for the intelligence in the machine. In other words, semantic labelling is a major step forward in gaining an understanding of data. Data semantic labelling can give more insight to the attacker that can be exploited, i.e. the semantic labels are themselves assets. In the example from ETSI GR SAI 001 [i.35] it is stated that "simple semantic labels can be seen in the names given by programmers to constants and variables, but in the wider context semantics have to be transferred with the data in order that the receiver has knowledge of what the value means, or is associated to" and that transfer of semantics has to be protected from exploit.

The typical ML cycle is illustrated in figure J.1 (from ETSI TR 104 221 [i.34]).

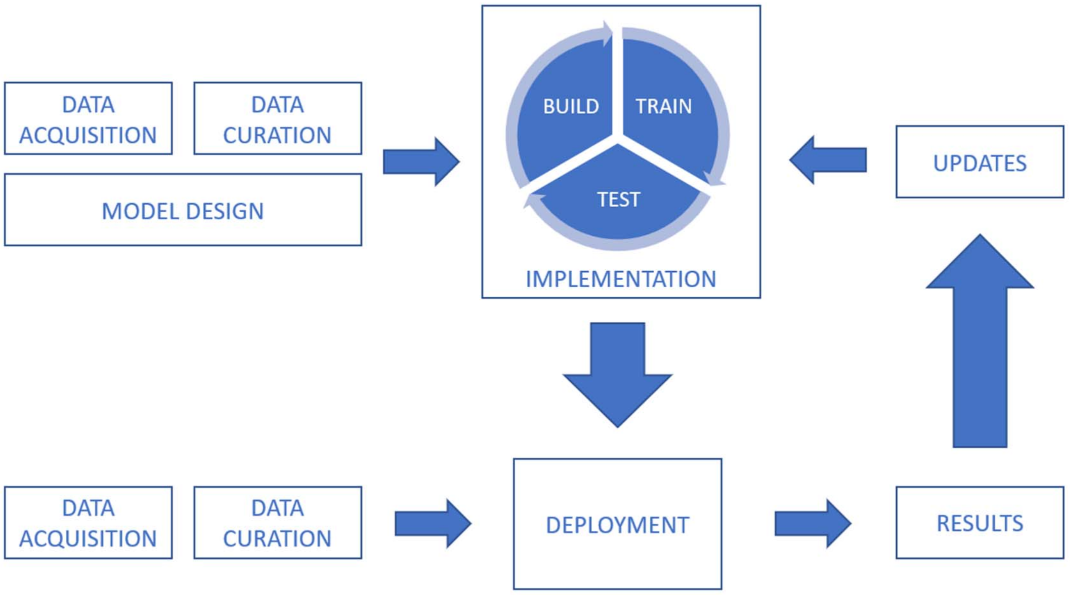


Figure J.1: Typical machine learning lifecycle (from ETSI TR 104 221 [i.34])

Data that is acquired and curated is used to develop and refine the model - where the model describes the purpose of the ML system. In the TVRA environment the intent of the model can be to identify weaknesses and exploits, therefore the data used as input will generally be based on the system to be analysed.

J.2 ML as an adversary to identify weaknesses and vulnerabilities

One common application of ML is to identify correlations in random data and from those correlations to determine if there is an identifiable causation for them. The more data available to the adversary the higher the likelihood of finding such a causation and then exploiting that causation as an attack vector.

As stated in ETSI GR SAI 001 [i.35] attacks on AI systems can be thought of as aiming to force a model to do, learn or reveal the wrong things:

- **Do** - the actor aims to engineer an input to a model such that the output will be incorrect. The actor has control over the input but not the model itself. This class of attack is known as *evasion*. An example would be a malware author manipulating an executable binary so that an ML-based security product classifies that binary as benign software.

    - **Do** attacks are variants of the manipulation attack classification shown in figure 7 of the present document.

- **Learn** - the actor wishes to *poison* a model such that it will fail to operate as intended, in a targeted or indiscriminate way. The actor has control over the data and/or model. The actor may be looking to degrade the overall performance of a model (functionally a denial-of-service attack), or to introduce a backdoor or trojan. In the former case, the degradation or disruption can be the actor's ultimate aim, or they wish to use the reliably poor performance of a model to achieve a downstream effect. In the backdoor case, while overall model performance will remain consistent, the actor will be able to reliably conduct an evasion attack as above.

    - **Learn** attacks are, as suggested above, also a manipulation attack.

- **Reveal** - the actor aims to uncover information about the model and/or the data used to train it. This can be for espionage or theft purposes: actors wish to steal the model itself, reveal sensitive training data or learn if particular examples have been used for training. Many of the evasion and poisoning attacks above are enabled by access to the model or an approximation of it: as such, an actor may wish to steal a model as a preparatory step in conducting another type of attack.

An adversary's objective in using AI for offensive purposes is likely to be similar to any organization's: increased efficiency, speed and scale; automation; and easier exploitation of large amounts of data. If attacks using AI fail, a sufficiently motivated attacker may still be able to perform the attack manually.

J.3 ML/AI as determinants of an attack

In making an assessment of risk, and likelihood in particular, the analyst may use AI/ML techniques to assist in the analysis. The role of AI/ML in such scenarios is to determine if an attack is viable by collating data on the system and developing a knowledge base for making evaluations.

Existing vulnerability databases may be used as data sources in identifying weaknesses in systems (in this mode the ML/AI data sources act as accelerants to the knowledge factor identified in clause 6.6.3.1.1 and in Annex B of [1]).

Annex K (informative): Application of TVRA to AI and ML systems

An AI or ML system is decomposed in like manner to any other system to identify its assets, and the relationships that exist between those assets. In this regard the method described in the main body of the present document applies. The analyst has to take due consideration that the operational AI/ML system may modify its behaviour and thus the analyst should assess the likelihood of change of the system over time and the impact that any such learned behaviour modifies risk.

Annex L (informative):
Change history

L.1 Updates prior to V5.2.5

Date	WG Doc.	CR	Rev	CAT	Title / Comment	Current Version	New Version
19-10-2010	TISPAN07(10)0139R1	1	-	F/D	ETSI TS 102 165-1 CR to introduce requirements and countermeasure cost-benefit analysis and to make minor editorial changes to clause 4.	4.2.1	4.2.2
19-10-2010	TISPAN07(10)0140R2	2	-	B	ETSI TS 102 165-1 CR to revise title of eTVRA method to TVRA method and to add three new steps to the TVRA method based on experience from TVRA exercises in TISPAN and ITS and to make minor editorial changes to clause 5.	4.2.1	4.2.2
19-10-2010	TISPAN07(10)0141R1	3	-	B	ETSI TS 102 165-1 CR to add three new steps to the TVRA method based on experience from TVRA exercises in TISPAN and ITS and to make minor editorial changes to clause 6.	4.2.1	4.2.2
2-12-2010	TISPAN07(10)0164	4	-	D	Removal of ENUM analysis.	4.2.2	4.2.3
16-9-2017	CYBER(16)008022				Transfer to ETSI CYBER for maintenance.	4.2.3	5.0.1
5-1-2017	CYBER(16)008021r1	1		B	Modification to the mapping of vulnerability rating to likelihood of attack.	5.0.1	5.2.1
7-8-2017	CYBER(17)011009	2		B	Revision addressing removal of bulk of Common Criteria text and replacement by simple example and reference.	5.2.1	5.2.2
8-8-2017	CYBER(17)011010	3		B	Revision of Annex E adding database tables for new motivation treatment.	5.2.2	5.2.3
22-11-2021	CYBER(21)026011	1	-	F	TVRA method fix of spreadsheet and method description in Annex G.	5.2.3	5.2.4
01-2022					Publication with removal of outdated introduction.	5.2.4	5.2.5
04-2022	CYBER(22)29a004	-	-	-	Removal of Annex D (to be moved to ETSI TS 102 165-2). Clarification that the 10 steps are not sequential Extension of the role of AI in the metrics.	5.2.5	5.2.6 (5.3.0)

History

Document history		
V4.1.1	February 2003	Publication
V4.2.1	December 2006	Publication
V4.2.3	March 2011	Publication
V5.2.3	October 2017	Publication
V5.2.5	January 2022	Publication
V5.3.1	February 2025	Publication