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

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

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

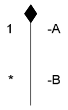
NOTE: A **vulnerability**, consistent with the definition given in ISO/IEC 27000 [i.22], is modelled as the combination of a **weakness** that can be exploited by one or more **threats**.

3.2 Symbols

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

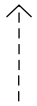
Generalization/Specialization: UML concept showing relationship between entities A and B where the two entities exhibit the property that A (top of arrow) is the general case whereas B is the specific case

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.

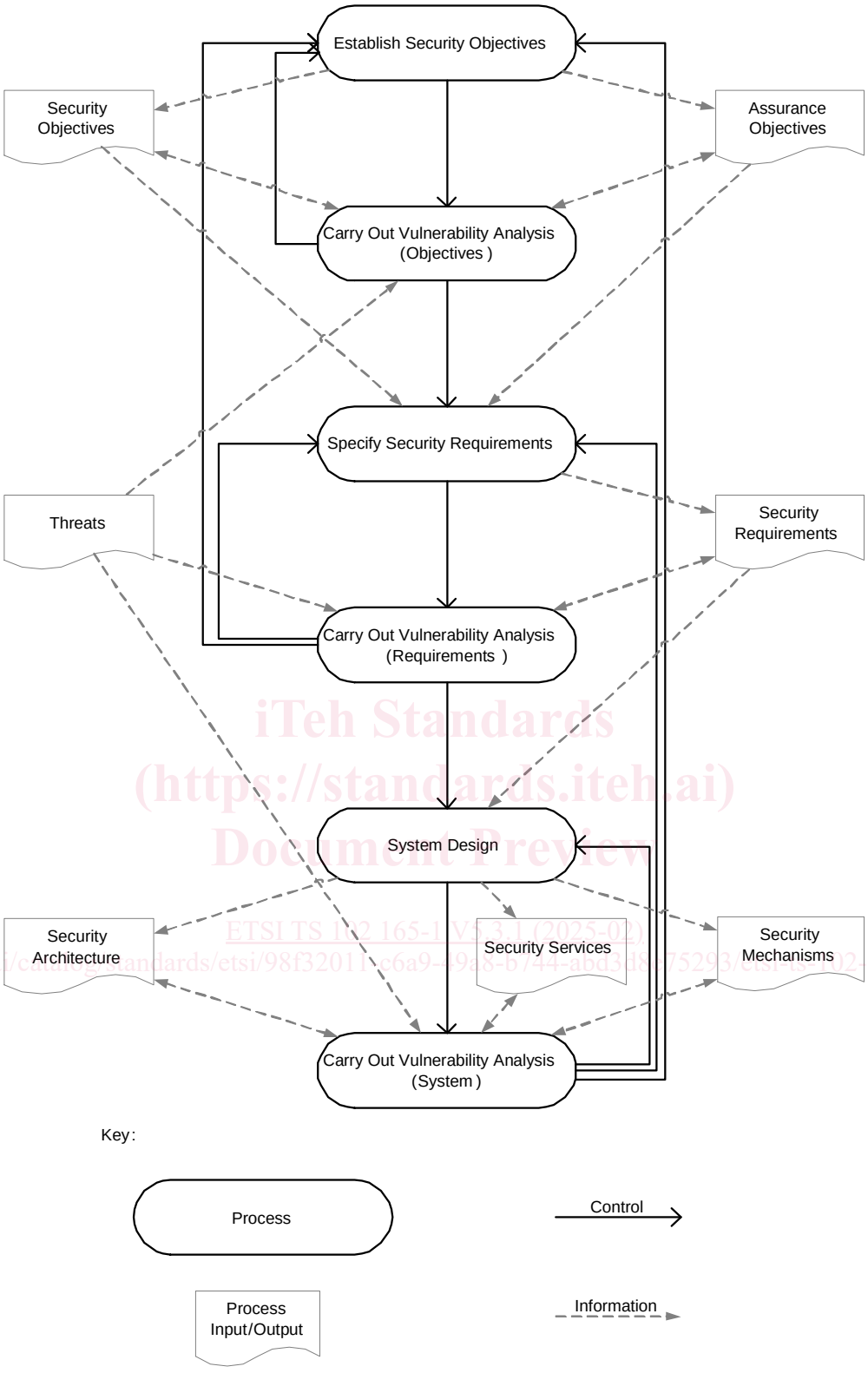


Figure 1: Structure of security analysis and development in standards documents

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.

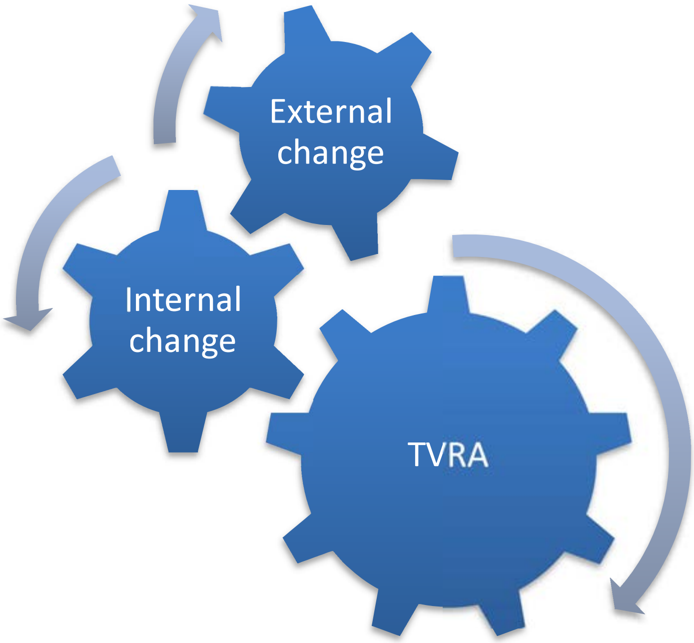


Figure 2: Cyclical nature of TVRA wherein any change requires reapplication of TVRA

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.