ETSI TR 103 087 V1.1.1 (2016-06)

TECHNICAL REPORT

Reconfigurable Radio Systems (RRS); Security related use cases and threats in Reconfigurable Radio Systems

Reference

DTR/RRS-03010

Keywords

radio, safety, 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 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

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 only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is 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 Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, 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.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Reconfigurable Radio Systems (RRS).

Modal verbs terminology

In the present document "**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.

Introduction

The present document presents a security threat analysis of RRS networks and devices for a set of specific use cases and operational scenarios defined in ETSI TC RRS.

It is recommended to consider [i.1], [i.2], [i.3], [i.5], [i.6], [i.7], [i.8] and [i.18] for further information on the framework related to the solutions in the present document.

1 Scope

The present document provides an analysis of the risk of security attacks on the operation of reconfigurable radio systems. It identifies which security threats can disrupt RRS networks and devices or can induce negative impacts on other radio communication services operating in the same radio spectrum. The present document also identifies stakeholder and assets, which can be potentially impacted by the security threats.

2 References

2.1 Normative references

As informative publications shall not contain normative references this clause shall remain empty.

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] Recommendation ITU-T E.408: "Security in Telecommunications and Information Technology. An overview of issues and the deployment of existing ITU-T Recommendations for secure telecommunications. Telecommunication networks security requirements".

[i.2] L. B. Michael, M. J. Mihaljevic, S. Haruyama: and R. Kohno: "A framework for secure download for software-defined radio.", IEEE Communications Magazine, July 2002.

[i.3] A. N. Mody, R. Reddy, T. Kiernan and T.X. Brown: "Security in cognitive radio networks: An example using the commercial IEEE 802.22 standard," Military Communications Conference, 2009. MILCOM 2009. IEEE, vol., no., pp.1-7, 18-21 Oct. 2009, Boston, MA, USA.

[i.4] "Wireless Innovation Forum's Security Working Group. Securing Software Reconfigurable Communications Devices", Document Id: WINNF-08-P-0013.

[i.5] ETSI TR 103 062: "Reconfigurable Radio Systems (RRS); Use Cases and Scenarios for Software Defined Radio (SDR) Reference Architecture for Mobile Device".

[i.6] ETSI TR 102 907: "Reconfigurable Radio Systems (RRS); Use Cases for Operation in White Space Frequency Bands".

[i.7] ETSI TR 103 063: "Reconfigurable Radio Systems (RRS); Use Cases for Reconfigurable Radio Systems operating in IMT bands and GSM bands for intra-operator scenarios".

[i.8] ETSI TR 102 944: "Reconfigurable Radio Systems (RRS); Use Cases for Baseband Interfaces for Unified Radio Applications of Mobile Device".

[i.9] ETSI TS 102 165-1: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis".

[i.10] 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.11] ETSI EN 302 969: "Reconfigurable Radio Systems (RRS); Radio Reconfiguration related Requirements for Mobile Devices".

[i.12] ETSI TS 103 436: "Reconfigurable Radio Systems (RRS); Security requirements for reconfigurable radios".

[i.13] ETSI EN 303 095: "Reconfigurable Radio Systems (RRS); Radio Reconfiguration related Architecture for Mobile Devices".

[i.14] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC.

[i.15] Directive 2014/35/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of electrical equipment designed for use within certain voltage limits Text with EEA relevance.

[i.16] Directive 2014/30/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to electromagnetic compatibility (recast) (Text with EEA relevance).

[i.17] Regulation (EC) No 765/2008 of the European Paliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relatiing to the marketing of products and repealing Regulation (EEC) No 339/93 (Text with EEA relevance).

NOTE: European Directives and Regulations are available at http://eur-lex.europa.eu/.

[i.18] ETSI TR 102 967: "Reconfigurable Radio Systems (RRS); Use Cases for dynamic equipment reconfiguration".

[i.19] ETSI EN 303 146-2: "Reconfigurable Radio Systems (RRS); Mobile Device (MD) information models and protocols; Part 2: Reconfigurable Radio Frequency Interface (RRFI)".

[i.20] ETSI TS 103 146-3: "Reconfigurable Radio Systems (RRS); Mobile Device Information Models and Protocols Part 3: Unified Radio Application Interface (URAI)".

[i.21] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive).

[i.22] ETSI GS NFV-SEC 003: "Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance".

3 Definitions and abbreviations

3.1 Definitions

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

assigned frequency band: frequency band or sub-band within which the device is authorized to operate and to perform the intended function of the equipment

National Regulatory Authority (NRA): body or bodies charged by a Member State with any of the regulatory tasks assigned in this Directive and the Specific Directives (Framework Directive 2002/21/EC [i.21])

radio system: system capable to communicate some user information by using electromagnetic waves

NOTE: Radio system is typically designed to use certain radio frequency band(s) and it includes agreed schemes for multiple access, modulation, channel and data coding as well as control protocols for all radio layers needed to maintain user data links between adjacent radio devices.

Reconfigurable Radio System (RRS): radio system using reconfigurable radio technology

security threat: potential violation of security

NOTE: Examples of security threats are loss or disclosure of information or modification/destruction of assets. A security threat can be intentional like a deliberate attack or unintentional due to an internal failure or malfunctions.

use case: description of a system from a user's perspective

NOTE 1: Use cases treat a system as a black box, and the interactions with the system, including system responses, are perceived as from outside the system. Use cases typically avoid technical jargon, preferring instead the language of the end user or domain expert.

NOTE 2: Use cases should not be confused with the features/requirements of the system under consideration. A use case may be related to one or more features/requirements; a feature/requirement may be related to one or more use cases.

NOTE 3: A brief use case consists of a few sentences summarizing the use case

user: user of the Mobile Network

3.2 Abbreviations

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

ASF	Administrator Security Function
CA	Certificate Authority
CCE	Conformity Contact Entity
CE	Conformité Européenne
CM	Configuration Manager
ComSec	Communication Security
CPC	Cognitive Pilot Channel
CR	Cognitive Radio
CSL	Communication Service Layer
CSP	Communication Service Provider
DAA	Download Authorization Authority
DEF	DoC Endorsement Function
DMA	Direct Memory Access
DoC	Declaration of Conformity
EU	European Union
FCC	Federal Communications Commission
GSM	Global System for Mobile Communications
HAL	Hardware Abstraction Layer
HW	Hardware
IMEI	International Mobile Equipment Identity
IR	Intermediate Representation
IT	Information Technology
JTAG	Joint Test Action Group
LTE	Long Term Evolution
MAC	Medium Access Control
MD	Mobile Device
MDRC	Mobile Device Reconfiguration Class
MURI	MUltiRadio Interface
NFV	Network Function Virtualisation
NRA	National Regulatory Authority
OEM	Original Equipment Manufacturer
OS	Operating System
PKC	Public Key Certificate
PKI	Public Key Infrastructure
QA	Quality Assurance
RA	Radio Application
RAP	Radio Application Package
RAT	Radio Access Technology

RC	Radio Controller
RCF	Radio Controller Framework
RE	Reconfigurable Equipment
RED	Radio Equipment Directive
REF	RAP Endorsement Function
RF	Radio Frequency
RPI	Radio Programming Interface
RPOE	Radio Platform Operating Environment
RRFI	Reconfigurable Radio Frequency Interface
RRS	Reconfigurable Radio System
RVM	Radio Virtual Machine
SCA	Software Communication Architecture
SCP	Software/Content Provider
SD	Software Distributor
SDR	Software Defined Radio
SDRD	Software Defined and Reconfigurable Devices
SFB	Standard Functional Block
SPA	Service Provider Application
SW	Software
TOE	Target Of Evaluation
TR	Technical Report
TV	Television
TVRA	Threat Vulnerability Risk Analysis
UA	User Application
UDFB	User Defined Functional Block
UE	User Equipment
UML	Unified Model Language
URA	Unified Radio Application
URAI	Unified Radio Application Interface
URL	Uniform Resource Locator
URN	Unique Reference Number
USB	Universal SErial Bus
VNFCI	Virtual Network Function Component Instance

4 Method of analysis

The approach to security analysis given in ETSI TS 102 165-1 [i.9] is a multi-step process that is intended to identify, in its first steps, system objectives and the target of evaluation - in other words to clearly identify what is the thing being analysed in order to identify where its points of attack are. The method applied in the present document is derived from that described in ETSI TS 102 165-1 [i.9] in order to provide the rationale to identify and design the security countermeasures for RRS by application of a systematic method, and to allow users to visualize the relationship of objectives, requirements, system design and system vulnerabilities.

In order to assist the reader a short overview of the role and purpose of the TVRA method is given, although for complete details the reader is advised to consult the reference document. The depth of the TVRA changes as the system design becomes more detailed. A TVRA working from the system objectives will 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 in any change to any aspect of the system or its environment requires the process to restarted.

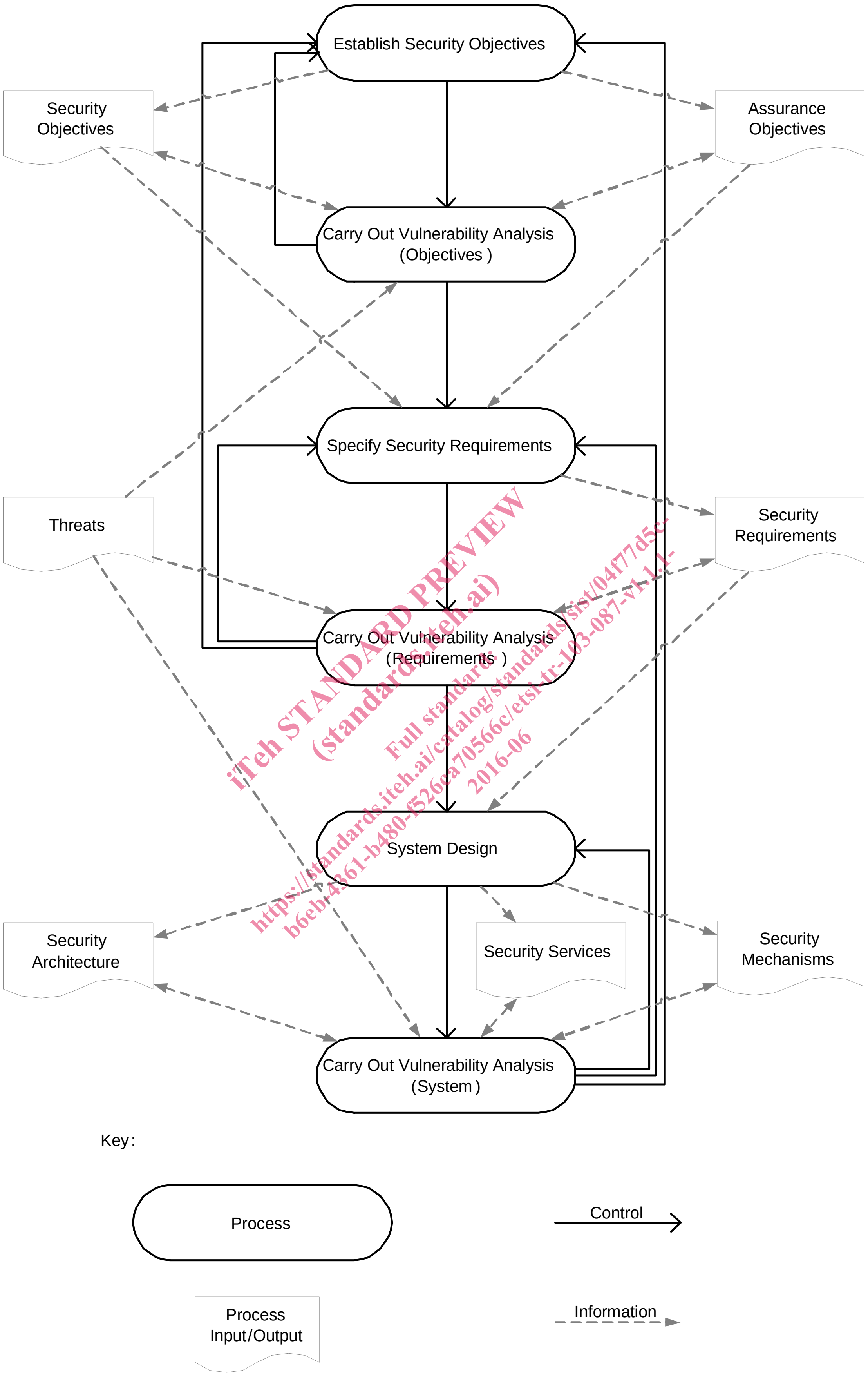
Establish Security Objectives
Security Objectives
Assurance Objectives
Carry Out Vulnerability Analysis (Objectives)
Specify Security Requirements
Threats
Security Requirements
Carry Out Vulnerability Analysis (Requirements)
System Design
Security Architecture
Security Services
Security Mechanisms
Carry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

Figure 1: Structure of security analysis and development (from ETSI TS 102 165-1 [i.9])

The purpose of the TVRA is to determine how open to attack the system, or components of the system are. The TVRA method 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**.

The TVRA method process consists of the following steps:

1) Identification of the Target of Evaluation (TOE) resulting in a high level description of the main assets of the TOE and the TOE environment and a specification of the goal, purpose and scope of the TVRA.

NOTE 1: For the present document the ToE is defined in clause 7.

2) Identification of the objectives resulting in a high level statement of the security aims and issues to be resolved.

NOTE 2: For the present document the objectives and the resultant high level statement of security provisions for RRS in the context of the ToE can be found in clause 5.

3) Identification of the functional security requirements, derived from the objectives from step 2.

4) Inventory of the assets as refinements of the high level asset descriptions from step 1 and additional assets as a result of steps 2 and 3.

5) Identification and classification of the vulnerabilities in the system, the threats that can exploit them, and the unwanted incidents that may result.

6) Quantifying the occurrence likelihood and impact of the threats.

7) Establishment of the risks.

8) Identification of countermeasures framework (conceptual) resulting in a list of alternative security services and capabilities needed to reduce the risk.

NOTE 3: The output of steps 3 through 7 are presented in clauses 6 and 7 with the conceptual framework given at the end of clause 7.

9) Countermeasure cost-benefit analysis (including security requirements cost-benefit analysis depending on the scope and purpose of the TVRA) to identify the best fit security services and capabilities amongst alternatives from step 8. The cost-benefit analysis should take account of the impact on each of standards design, implementation, operation, regulatory impact and market acceptance

NOTE 4: An indicative cost benefit analysis for a selected set of measures is given in ETSI TS 103 436 [i.12], clause A.1.

10) Specification of detailed requirements for the security services and capabilities from step 9.

NOTE 5: For RRS the output of step 10 is to be found in ETSI TS 103 436 [i.12].

The application of countermeasures adds assets to the system and may create new vulnerabilities, indicating that the TVRA will need to be undertaken again, and the method should be repeated until all the risks have been reduced to an acceptable level. Furthermore, by allowing the analysis to be rerun when attack likelihood changes, the risk to the system may be re-evaluated as knowledge of new or revised attacks becomes available.

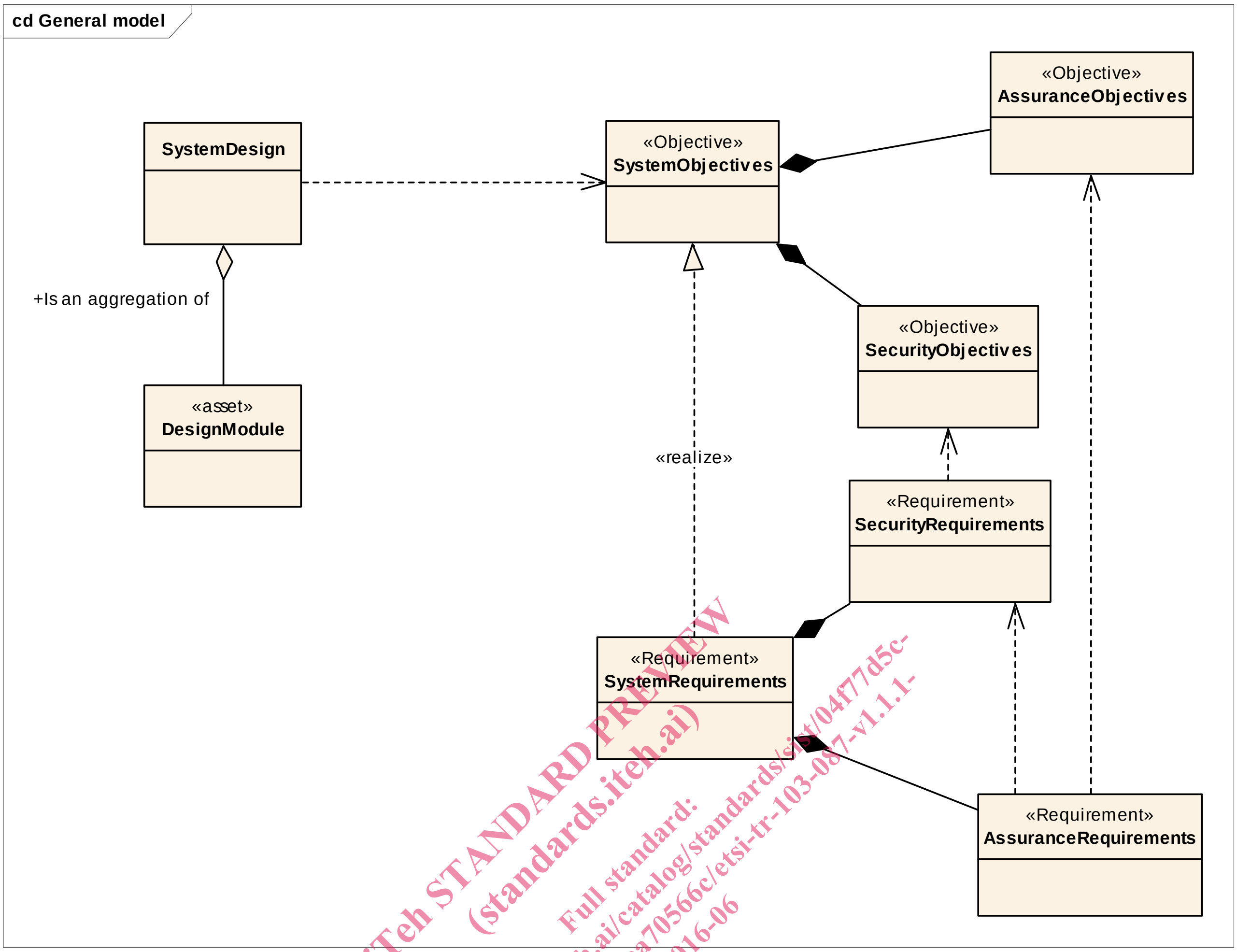

Figure 2: Relationship between system design, objectives and requirements

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.

A TVRA requires that both the system being examined (with its catalogued objectives and requirements) and the assets of the system and how it fits to its environment are clearly identified. 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 3.