ETSI TECHNICAL REPORT

ETR 332

November 1996

Source: ETSI TC-STAG

Reference: DTR/NA-002509

ICS: 33.020

Key words: Security

Security Techniques Advisory Group (STAG); Security requirements capture

ETSI

European Telecommunications Standards Institute

ETSI Secretariat

Postal address: F-06921 Sophia Antipolis CEDEX - FRANCE
Office address: 650 Route des Lucioles - Sophia Antipolis - Valbonne - FRANCE
X.400: c=fr, a=atlas, p=etsi, s=secretariat - **Internet:** secretariat@etsi.fr

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

Contents

Foreword 5

Introduction 5

1 Scope 7

2 References 7

3 Abbreviations 8

4 General Methodology 8
4.1 Working procedure within ETSI 9
4.2 Simplifications and models 10
4.3 Explanation of terminology 12
4.4 Methodology flow chart 12

5 Security objectives definition 13
5.1 Identification of the system's nature 14
5.2 Identification of individual security objectives 15

6 System review 15

7 Threat analysis 19
7.1 Identification of system-specific threats 22
7.2 Identification of threats based on external requirements 22
7.3 Guidelines to the identification of data protection threats 22
7.4 Guidelines to the identification of threats related to inter-network communication 23
7.5 Guidelines to the identification of threats to system integrity 24
7.6 Guidelines to the identification of threats due to security policies 24

8 Risk assessment 24
8.1 Evaluation of threats and definition of risks 25
8.2 Determine threshold for major threats respectively risks 27
8.3 Evaluation of the global risk, risk assessment report 27
8.4 TC/STC management decision 27
8.5 Setting up the final risk assessment report 27

9 Security requirements 28

Annex A: List of work items referred to in this ETR 30

History 31

Blank page

Foreword

This ETSI Technical Report (ETR) has been produced by the Security Techniques Advisory Group (STAG) Technical Committee of the European Telecommunications Standards Institute (ETSI).

Introduction

This ETR is one of a set of documents to support ETSI Technical Committees in analysing and defining their specific needs for security and in specifying the security measures that become necessary.

This ETR provides guidance and support for a comprehensive analysis of threats, vulnerabilities, risks and for the compilation of a specific set of security requirements.

Advice regarding working procedures and documentation is included.

Blank page

1 Scope

This ETSI Technical Report (ETR) provides guidance and support for a comprehensive analysis of threats, vulnerabilities, risks and for the compilation of a specific set of security requirements.

It is the intention to provide the user of this ETR with a comprehensive understanding and methodology regarding threats, vulnerabilities, risks and security requirements.

The security architecture of a particular system is always unique and the threats and security requirements are very specific to that system. The contents of this paper provide guidelines and checklists rather than specifying in too much detail in order to facilitate the application by the user.

This ETR should enable TCs to start their security work from scratch, to take advantage of the experience from other TCs Security Experts Groups (SEGs) or to adapt solutions that have already been devised.

STCs seeking advice on threat analysis and security requirements capture should ask STAG for support.

2 References

This ETR incorporates by dated and undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to this ETR only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies.

[1] ETR 236: "Security Techniques Advisory Group (STAG); A guide to the ETSI security standards policy".

[2] ETR 232: "Network Aspects (NA); Security Techniques Advisory Group (STAG); Glossary of security terminology".

[3] ETR 233: "Security Techniques Advisory Group (STAG); A directory of security features in ETSI standards".

[4] ETR 237: "Security Techniques Advisory Group (STAG); Baseline security standards; Features and mechanisms".

[5] ETR 340: "Security Technical Advisory Group (STAG); Guidelines for security management techniques".

[6] DTR/NA-002603: "Security Techniques Advisory Group (STAG); Guidelines for integrating security mechanisms into ETSI standards".

[7] ETR 234: "Security Techniques Advisory Group (STAG); A guide to specifying requirements for cryptographic algorithms".

[8] DTR/NA-002701: "Security Techniques Advisory Group (STAG); Guidelines on the relevance of security evaluation to ETSI standards".

[9] ETR 330: "Security Techniques Advisory Group (STAG); A guide to legislation, recommendations & guidelines governing the provision of security features".

[10] ETR 083: "Universal Personal Telecommunication (UPT); General UPT security architecture".

[11] ETR 086-3: "Trans European Trunked Radio (TETRA) systems; Technical requirements specification Part 3: Security aspects".

[12] COM(90) 314 SYN 287: "Draft EU directive on the protection of personal data".

[13] COM(90) 314 SYN 288: "Draft EU directive on the protection of personal data in digital telecommunication networks".

[14] CD-71-91-502-EN-C: "IT Security Evaluation Criteria (ITSEC)".

3 Abbreviations

For the purposes of this ETR, the following abbreviations apply:

ACT	Access Threats
DEF	system or service Deficiencies
DPT	Data Protection (Privacy) Threats
ECT	External (inter-) Communication Threats
EDI	Electronic Data Interchange
EU	European Union
ICT	Internal (Intra-) Communication Threats
ITSEC	Information Technology Security Evaluation Criteria
MNT	Management Threats
RPC	Remote Procedure Call
RT	Residual Threat
S	Security feature
SAGE	Security Algorithms Group of Experts
SAT	Threats generated by Safeguards
SEG	Security Experts Group
SIT	System Integrity Threats
SRCP	Security Requirements Capture Procedure
UPT	Universal Personal Telecommunication

4 General Methodology

The methodology defined here has 3 different aspects:

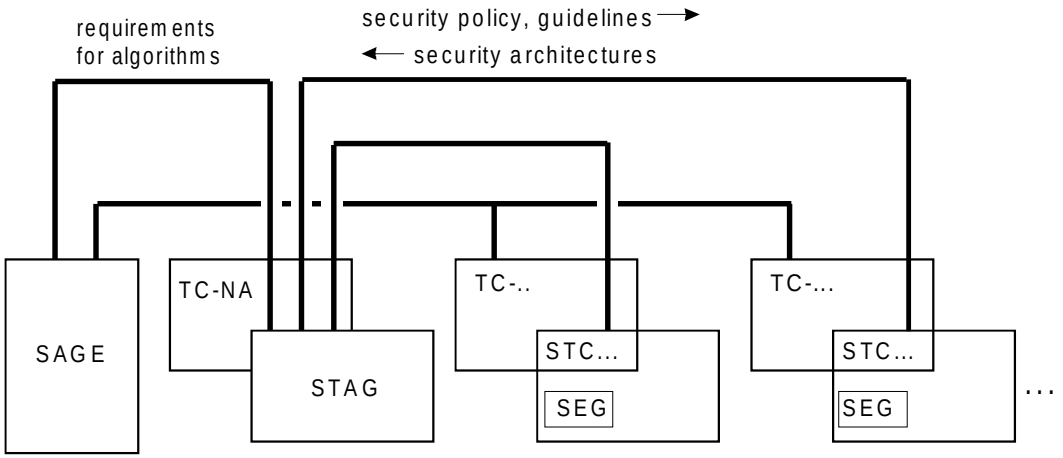
a) working procedure within ETSI;

b) simplifications and models;

c) methodology flow chart.

4.1 Working procedure within ETSI

As STAG is the responsible co-ordination group for security within ETSI, it provides a set of documents about general aspects of security. STAG provides a general security policy for ETSI and gives guidance to the TC/STCs so that the work on security in each TC/STC can be carried out efficiently. The relationship between the different security working groups within ETSI is illustrated in figure 1. For further information of relationships between these groups, see ETR 236 [1].



legend:
SEG = Security Experts Group
SAGE = Security Algorithms Group of Experts
(S)TC = (Sub-)Technical Committee

Figure 1: Relationship between security working groups within ETSI

Usually, when security work is started within an STC, a special SEG is set up for that purpose.

A SEG consists of both security experts and system service experts respectively. The flow of information between an individual SEG and STAG is shown in figure 2.

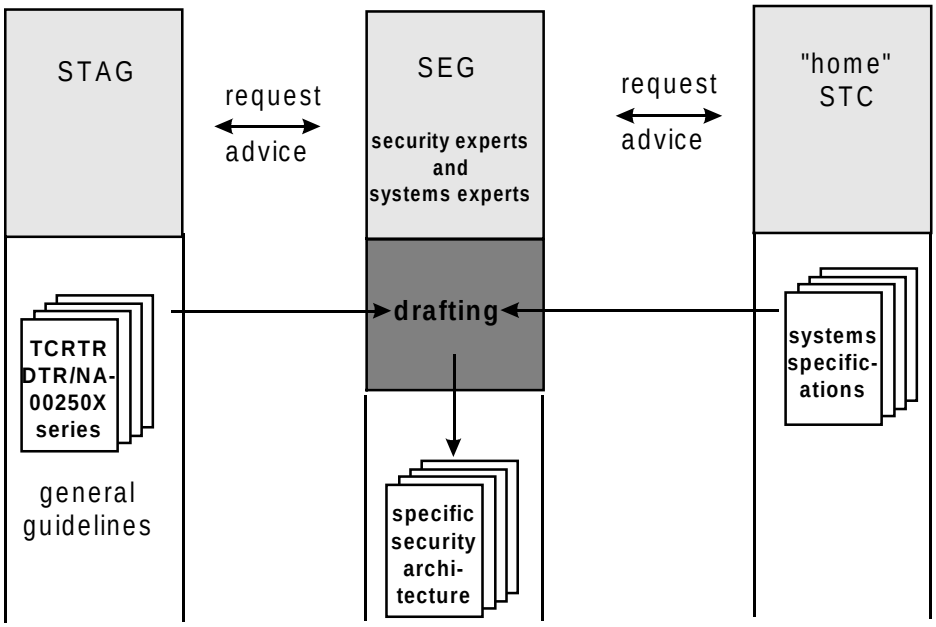


Figure 2: Information and documentation flow between STAG, SEG and STC

4.2 Simplifications and models

A large number of different methodologies can be defined for the security requirements capture. For example one possible approach is to use a special methodology for each system. This, however, would not be efficient in ETSI where many different systems have to be investigated and duplication of work has to be avoided.

The solution chosen here approaches the problem with a number of simplifications.

A first simplification is to discuss security on a more abstract level. Firstly security objectives have to be defined. Then as shown in figure 3 the unverified system is put under review by setting up an abstract model of the system to allow comparison to other system models that have already been investigated.

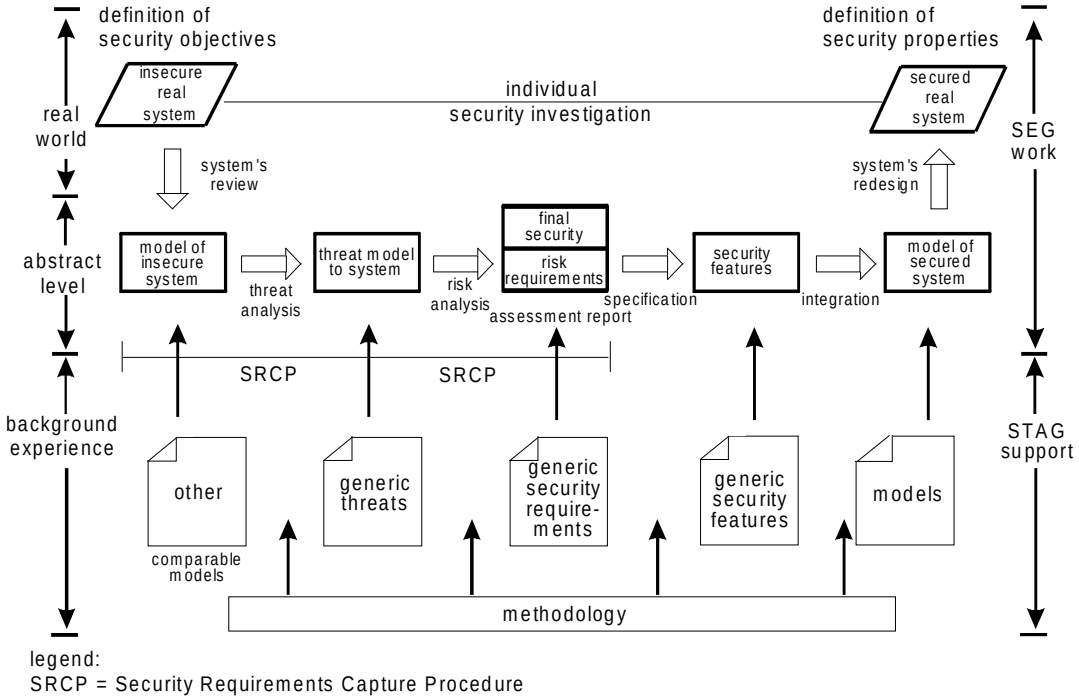
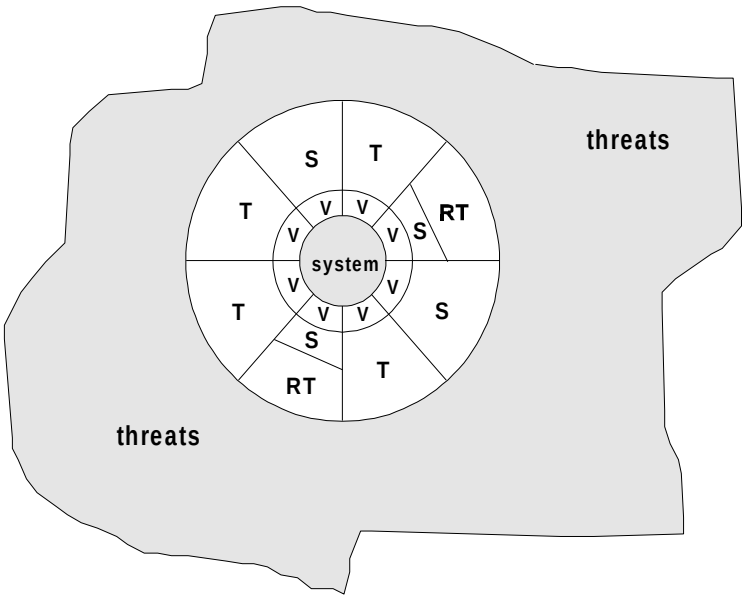


Figure 3: ETS Security Requirements Capture Procedure (SRCP)

At the abstract level threat analysis and all the security specification is done by taking advantage of existing STAG documentation about generic security aspects and methodology. Finally a model of the secured system is set up that will indicate where to redesign the system.

The second simplification is the definition of an abstract model for the security characteristics of a system. The dotted areas in figure 4 represent a real system with its associated threats. The abstraction of the real system is realized by its description in terms of security, i.e. the description of its technical vulnerabilities. From the opposite direction threats to those vulnerabilities are defined also at an abstract level.



Legend:

system:	real distributed system exposed to threats.	threats:	"cloud" of threats, constantly changing and only partially known.
S:	Security feature protecting an individual vulnerability.	V:	defined individual Vulnerability of the system.
T:	Threat.		
RT:	Residual Threat.		

Figure 4: Abstract model for the relationship between threats, risks, vulnerabilities, security features and residual risks

Following that procedure the security requirements will become apparent and security features can be defined. The model allows a one-to-one relationship of threats and security features so that the effectiveness and completeness of countermeasures can be controlled. Threats that will not, or that will only partially, be countered are identified as "residual threats" within the model.

Generally three reasons for vulnerability in a system can be identified:

- design vulnerabilities, caused by design weakness of the system which can be removed by a redesign of appropriate system functions;

- avoidable vulnerabilities, caused by a fundamental property of the system and can be fully protected by a certain security feature;

- unavoidable vulnerabilities, caused by a sensitive function of the system and for which a security feature cannot be found. In this case either the sensitive function shall be removed or the associated threats have to be accepted;

- forced vulnerabilities, causes by external restrictions or requirements, e.g. legal interception and data protection issues. Resulting features have to be implemented but should be clearly identified towards the users and operators of the system.

It becomes obvious that an SRCP can initiate a lot of different activities where the specification of technical countermeasures is only part of them. As a side effect the SRCP can increase the quality of a system's design significantly.

4.3 Explanation of terminology

One example for a security objective could be the confidentiality of information A.

A relevant threat could then be the disclosure of information A.

The needed security requirement could be the confidentiality of information A. Confidentiality could be provided by a security feature or a security service.

An appropriate security feature could then be realized with a security mechanism using, for example, the RSA algorithm.

Following this example, a threat could be everything that makes a security objective unsatisfied. The security requirement could be something that helps to satisfy security objectives in the presence of threats. Finally, security features should be understood as what needs to be provided in order to meet security requirements, e.g. security mechanisms, security management techniques, etc.

4.4 Methodology flow chart

Figure 5 briefly describes general steps of a SRCP.

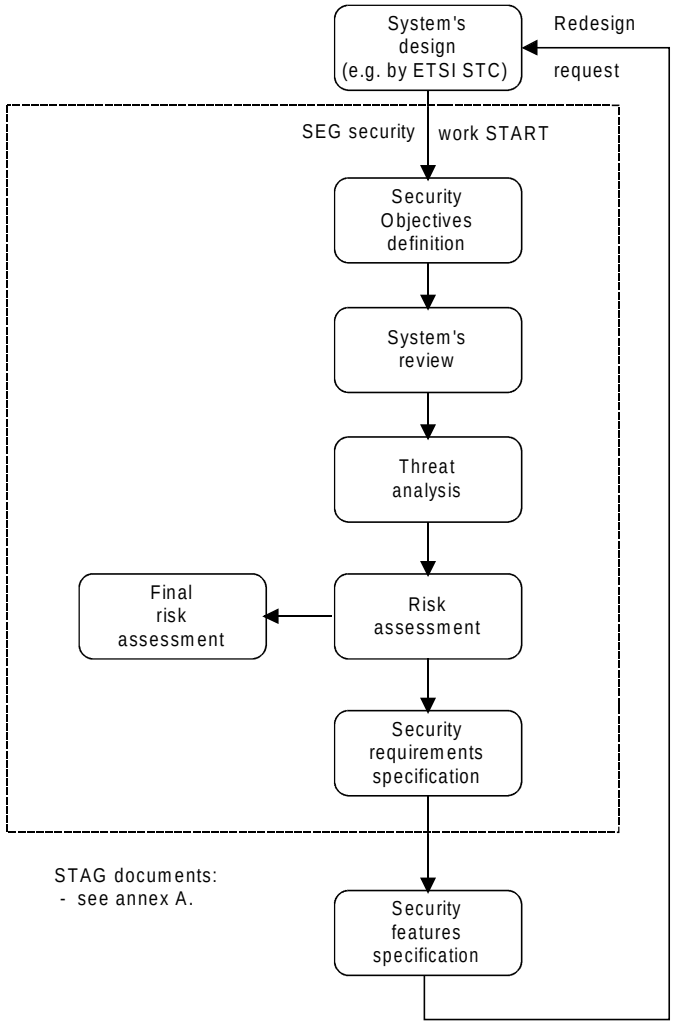


Figure 5: General methodology flow chart

Each distributed system has a specific profile of threats, vulnerabilities and security requirements. Depending on the internal structure and the intended tasks of the system a list of basic security objectives of a very general and generic nature should be defined before any detailed security investigation takes place. Knowing that an absolute secure system is illusory and prohibitively expensive the security objectives definition should give a clear orientation for the succeeding investigations.

Before a threat analysis can be started it is necessary to understand all the attributes of the system and to define the system's boundaries where further investigations should take place. Such a "system review" should also produce a complete understanding of the system's nature, its whole functionality and performance, in a way that potential vulnerabilities become transparent.

The succeeding "threat analysis" comes out with a list of system specific threats that have to be categorized to prepare the following "assessment of risks". System design deficiencies that have been recognized by SEG members, should lead to an early response to the system designers. This activity is also part of a threat analysis.

The intention of "risk assessment" firstly is to have some kind of a priority list, which threats are to be considered more severe, more important or more costly than others. Secondly, risk assessment should include a TC/STC's plenary decision considering what threats have to be countered and which not. The pros and cons have to be discussed by both security and system's experts.

The definition of "security requirements" prepares for the specification of the "security features" in the documents listed in annex A.

These documents will be applied again if the analysis of RTs and the assessment of residual risks become necessary.

Further details concerning methodology are given in clauses 7, 8, 9 and 10.

5 Security objectives definition

Security objectives represent a high level statement on the aims of the succeeding security investigations. They should give clear guidance and orientation so that the work on the time consuming efforts "system's review" and "threat analysis" can concentrate on the major issues. Further these security objectives should clearly state which Security Issues shall be resolved. The results of the security requirements capture process should also be in accordance with the security objectives defined.

To some extent the security objectives definition identifies the work programme for a SEG.

Often the definition of security objectives can be simplified when the system's nature is identified to be similar to another system for which such a definition already exists.

Security objectives should consider generic threats and security requirements and obey to internal/external security policies and their priorities, legal issues and data protection requirements. The general procedure is given in figure 6.

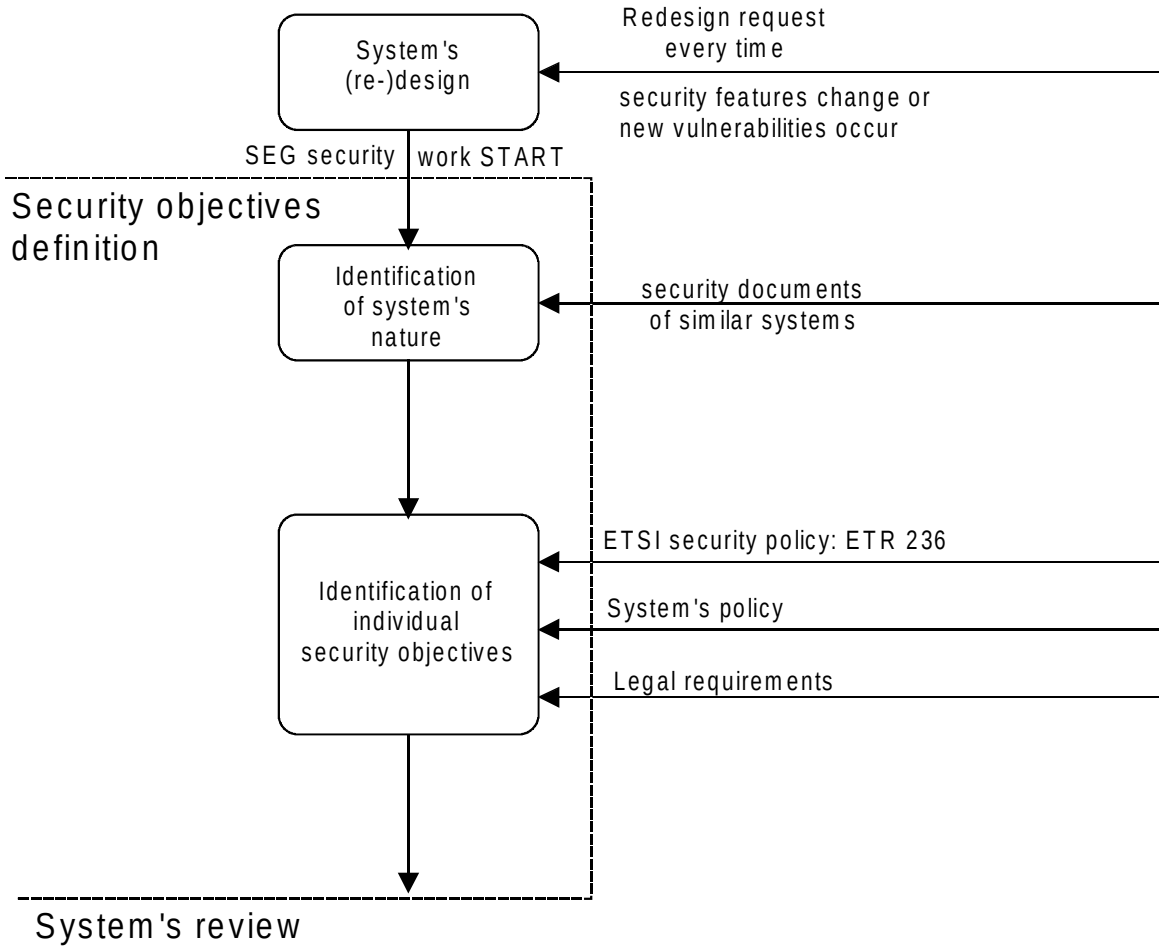


Figure 6: Methodology for the definition of security objectives

5.1 Identification of the system's nature

The identification of the system's nature helps to simplify the system's review and threat analysis because:

- security work on systems that have a similar nature may partly or fully be adopted;
- perhaps the system is composed of subsystems that have already been investigated and for which security objectives already exist.

In telecommunications, for example, the following "natures" of "systems" can be identified:

- TMNs;
- distributed databases;
- distributed processing (Remote Procedure Call (RPC));
- office-communication, e.g. providing e-mail services, Electronic Data Interchange (EDI), file transfer and messaging;
- information broadcasting; and
- real-time operating systems.

5.2 Identification of individual security objectives

Depending on the system's nature a typical profile of major threats and vulnerabilities can be obvious. In mobile systems, for example, always the radio path is of particularly concern to security.

Concerning the costs and performance restrictions to the whole system there could be the requirement of a reduced security level in a migration phase. Also there could be the requirement for compatibility to the security policy of some other system. This should be clearly stated as a security objective.

Usual security objectives are, for example:

- confidentiality, integrity, availability and authenticity of information;
- security control over the system's management;
- conformity to personal data protection directions; and
- conformity to national security requirements and export controls.

It is obvious that the security objectives have to be defined according to the security policy given by ETR 236 [1], legal obligations and any other directions coming from the general system's policy.

6 System review

The system review and the threat analysis are the most time consuming activities in the whole security requirements capture work.

Especially a comprehensive and complete understanding of the system, its properties, boundaries and relationships to the external world is a precondition to a successful work on the whole security issue.

Generally systems do not have a common infrastructure or common functional properties. At first glance this results in an individual model of each particular system.

Many systems, however, consist of components that each are comparable to similar ones within other systems. This fact can be used to simplify a system review significantly. Figure 7 gives an overview of possible system components.

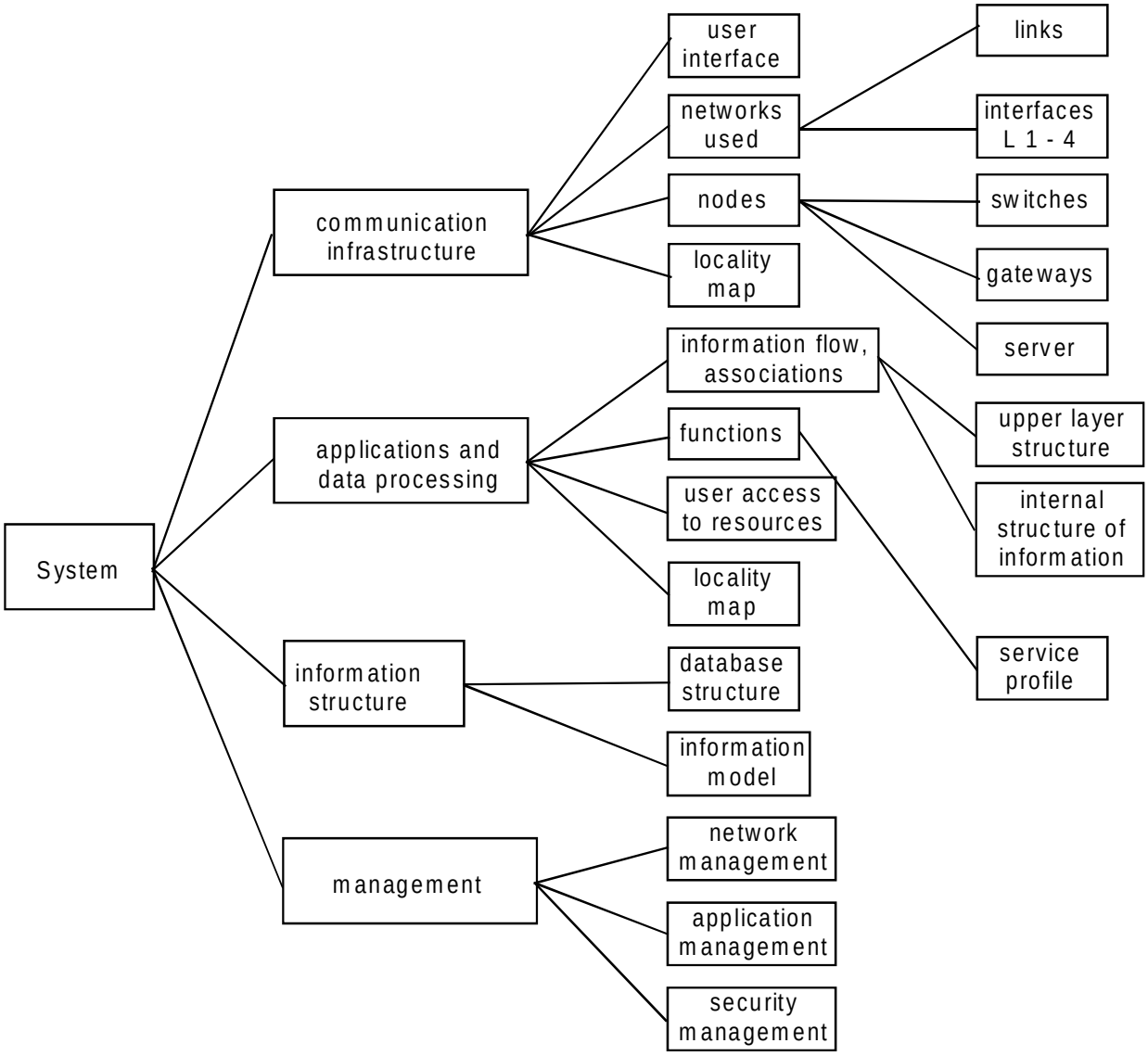


Figure 7: Overview of possible system's components

As security is mostly discussed in connection with a certain association between two communicating parties an abstraction of this configuration can be used as shown in figure 8. Subjects are defined to be communicating entities who are responsible for the communication. They can be humans or entities working on behalf, e.g. personalized smart cards. Objects represent a piece of information that has to be protected. These can, for example, be identities or signalling data.

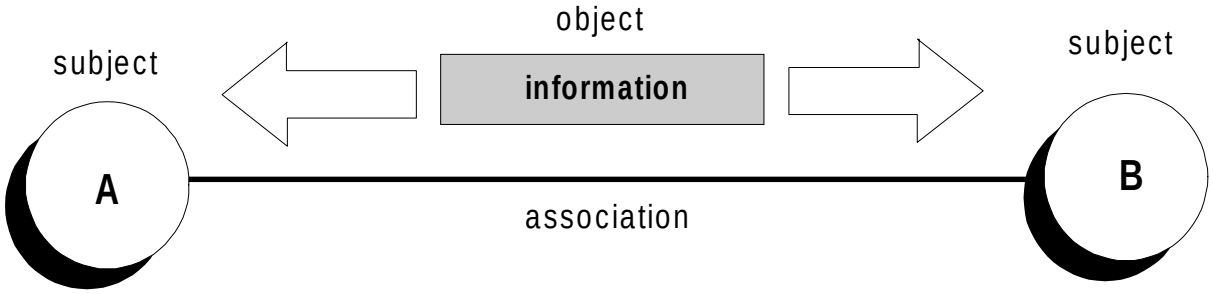


Figure 8: Abstraction of information flow for a simple association

Usually within ETSI a complete description of a "system" or service consists of the whole documentation output of an STC. It is rarely possible for an SEG to have all this material as their system review document.

Considering the work on Universal Personal Telecommunication (UPT) within NA 7 as an example, the following steps were taken to derive a system's review on the UPT system:

1) information flow analysis:

   - drawing an information flow map consisting of the communicating subjects and the associations between them;

2) identification of (personal data) to be stored and processed:

   - identify which (personal) data is collected, processed; and stored in the system;
   - identify the location of databases and processing functions. Identify the lifetime of data to be stored;

3) function and services analysis:

   - all functions and services are listed in connection with the individual association between the communicating entities;

4) define "vertical" boundaries:

   - separate functions and services that belong to an underlying infrastructure, e.g. IN, network services, etc. that have to be treated by other ETSI groups for consideration of their security aspects;

5) define "horizontal" boundaries:

   - identify procedural and physical interrelations to other systems. These systems might functionally either be different or similar or split into different administrational domains.

6) identify system's management functions:

   - identify the system's management functions, including network management and security management functions;

   - describe the information flows in the management network and the entities involved;

A subject is defined as a communicating party that can either be responsible or affected. Examples for subjects are given below:

- **subjects:**

  network provider;
  network operator (note 2);
  service provider;
  service operator (note 2);
  network user;
  network subscriber;
  service user;
  service subscriber;
  third party;
  intruder;
  prosecutor;
  procedure (note 1);

  NOTE 1: Working on behalf of a subject that is responsible for the procedure to be carried out correctly;

NOTE 2: In this case the operators are the people who actually operate the network components or the service.

Examples of endangered objects to be protected are:

- **objects:**

  transferred information;
  personal data;
  signalling data;
  database contents;
  network resources;
  application procedures.

The outcome of the preceding investigation should be a complete abstract model of the system which provides for a further analysis on any security aspect. It should rather be comprehensive than perfect in detail.

As far as the system review is concerned, the figure 5 flow chart can be refined according to figure 9.

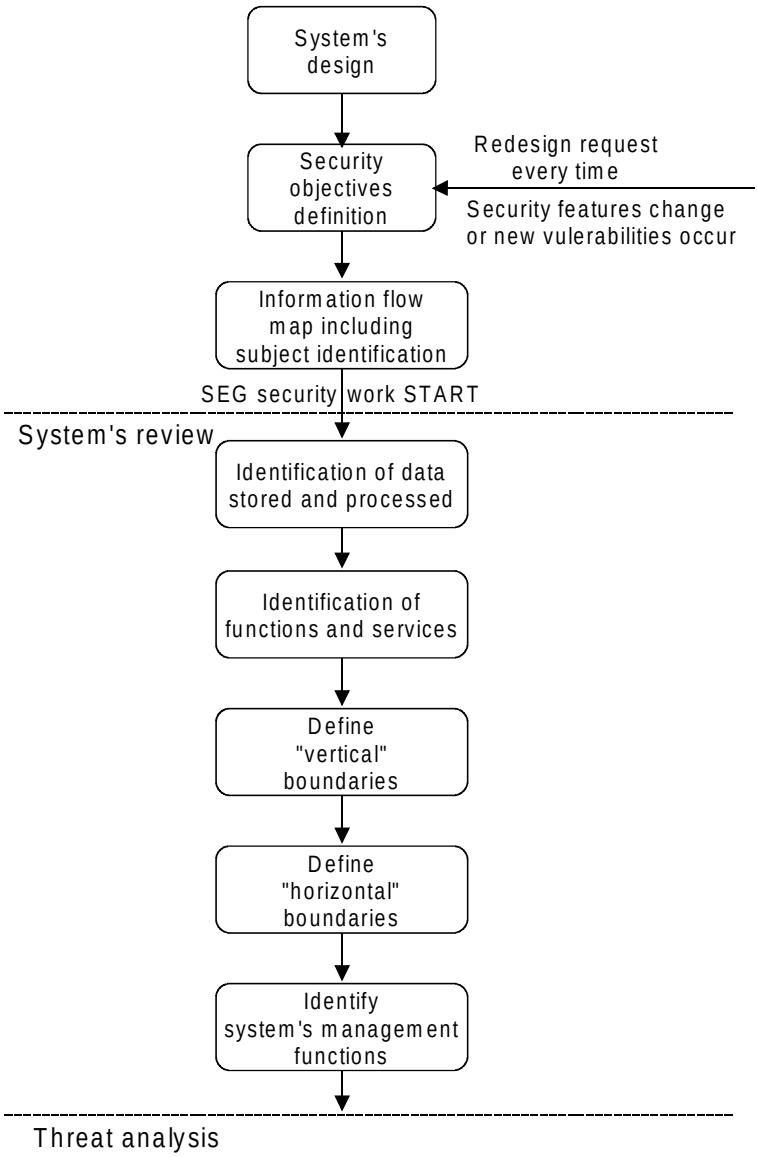


Figure 9: Methodology for a system's review

7 Threat analysis

The initial threat analysis follows the general concept illustrated in figure 10.

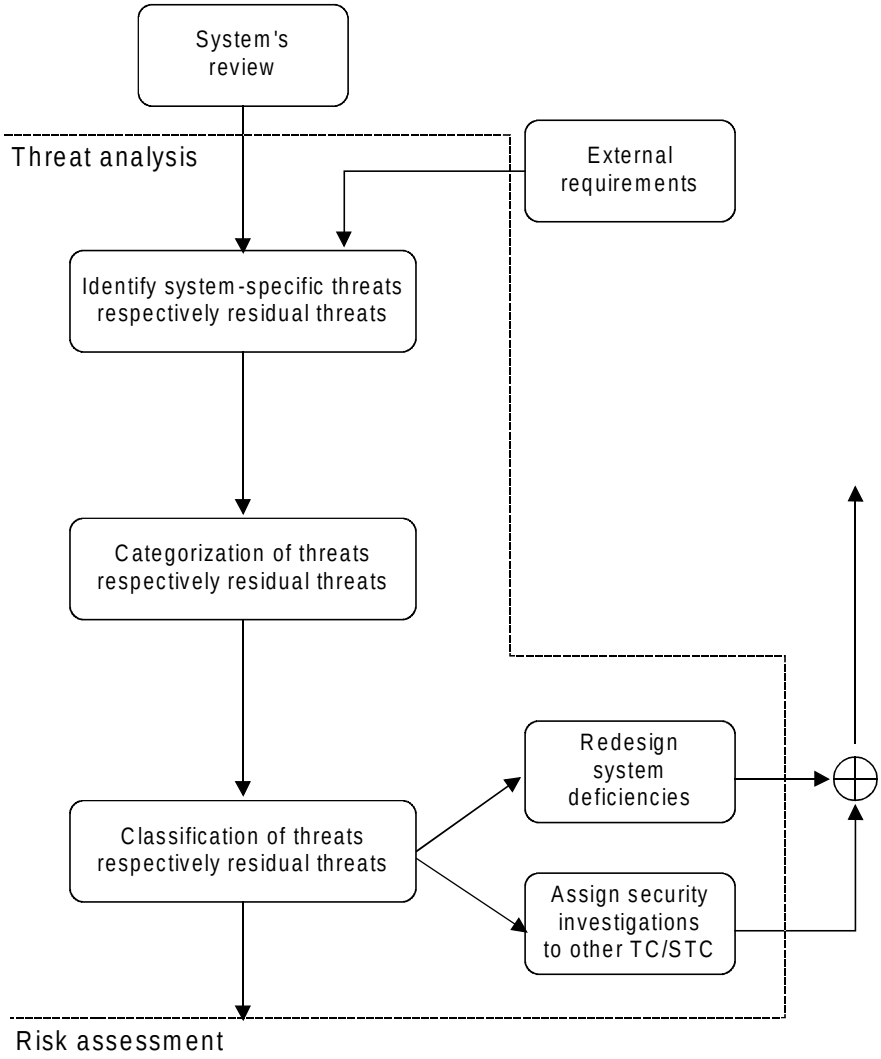


Figure 10: Methodology for a threat analysis

Threats can be described in a number of ways and their distinguishing features can be defined. Some examples of such "threat categories" are given in tables 1 and 2. Especially the telecommunication-specific threats categories shown in table 1 offer the opportunity to identify "standard" countermeasures against "standard"-threat-scenarios in different telecommunication environments.

Table 1: Examples for "general" categories of threats

"general" threat categories			
consequences	**motivation**	**technical**	
loss of accountability	accidental	active	physical
loss of transparency			
loss of availability			
loss of integrity	deliberate	passive	logical
loss of confidentiality			
loss of trustworthiness			
loss of validity			
loss of originality			
loss of privacy			
loss of prosecution			
loss of charges			
loss of image/clients			
fraud			

Table 2: Examples for "telecommunication-specific" categories of threats

telecommunication specific threat categories	
Abbreviation	**Category**
ACT	Access Threats
MNT	Management Threats
ECT	External (inter-) Communication Threats
ICT	Internal (intra-) Communication Threats
DPT	Data Protection (Privacy) Threats
SIT	System Integrity Threats
DEF	system or service Deficiencies
SAT	Threats generated by Safeguards

For telecommunication, a number of specific threats are shown in table 3.

Table 3: Threats common to telecommunication systems

Threat descriptor	typical application	category		
		telecommunication specific	technical	
			active	passive
impersonation	D	ACT, ECT, ICT	X	
masquerade of communicating parties and entities	D	ACT, ECT, ICT	X	
identity interception (note 3)	M, D	DPT, ECT		X
password interception (note 3)	D	ACT, ECT		X
data interception of signalling and user data (note 3)	M, D	ACT, DPT, ECT		X
replay of signalling and user data unauthorized copying (note 5)	M, D	ACT, ECT, ICT		X
modification and violation of data e.g. customers personal data (note 4)	M, D	ACT, ECT, ICT	X	
access right manipulation	M, D	ECT, ICT	X	
misuse of access rights	D	ACT, ECT, ICT	X	
denial of service	D	ACT, ECT, ICT	X	
denial of sending respectively authorship (repudiation)	M, D	ICT	X	
denial of receipt	M	ICT		X
access control	M	ICT		X
installation of intentional malfunction, sabotage	M, D	SIT	X	

NOTE 1: DEF threats can occur every time.
NOTE 2: D = Dialogue, including database access
M = Message, document or file transfer.
NOTE 3: Includes tapping.
NOTE 4: Includes deletion and addition.
NOTE 5: Means simple copying of information rather than the alteration of bits of it.

Threats may be caused by the subjects defined in clause 6, especially:

- inside (regular) users or operators;

- outside hackers or intruders.

A threat analysis may be comprehensive but will never be complete. A pragmatic approach, however, is to define threats with the help of general threat categories which are already known from other investigations and against those already well defined security features exist. For a complex and distributed system this approach has to be executed in several steps.

7.1 Identification of system-specific threats

A list should be generated from the information gathered during the system's review about all those functions and services of the system that can be accessed by any subjects, especially users and possible intruders.

All system functions should be defined to happen between particular subjects that communicate via certain associations. Each of these configurations of subjects and associations within the system is analysed for threats. After that the identified threats are categorized and described, according to the following scheme:

- guideline to identify, categorize and classify threats:

    1) select function;
    2) describe threats to this function;
    3) categorize each threat with a system and function-specific id;
    4) categorize each threat also with a general, telecommunication specific category according to tables 1 and 2;
    5) identify all associations and objects concerned and all threatening and threatened subjects;
    6) classify each threat according to whether:

        - it is inherent to the system or to mandatory system's function;
        - it is caused by design deficiencies;
        - it has to be investigated by another TC/STC because the threat comes from another domain, context or infrastructure;

    7) put all this information into a table.

7.2 Identification of threats based on external requirements

All system specific functions should additionally be investigated for threats resulting from external requirements like:

- system's design obligations;
- legal requirements on data protection;
- regulations for legal interception;
- national or international trade regulations;
- quality requirements;
- specific regulations for individual business branches.

External requirements of a very general nature might have been already defined in the security objectives phase, others might occur later during the threat analysis phase and still others might be caused by design directives to the system.

7.3 Guidelines to the identification of data protection threats

The general guidelines on the definition of threats to personal data integrity should be taken from European Union (EU) documents COM(90) 314 SYN 287 and 288.

It is useful to identify those human actors in the system whose personal data might be threatened, e.g.:

- users;
- subscribers;
- operators, service providers; and
- third parties.

Another issue is to identify the location of sensitive data within the system. Is it a distributed or a central database? Which are the data processing functions? Who has access rights on these functions? Is there any audit or control on personal data processing?

A general security objective of data protection is that:

> *"Only such personal data may be collected, processed and stored that are indispensable for the intended system or service features.*
>
> *Such data should only be stored at locations where necessary and should be deleted as soon as possible."*

Therefore requirements for the collection, location, processing and time of storage of personal data should be specified.

A common threat to personal data integrity is the possibility of collecting a profile of an individual personal behaviour concerning:

- the circumstances of his business;
- his personal time management; or
- his temporary location.

Eavesdropping of signalling or management data exchanged within or between networks could also present a threat to personal data integrity.

7.4 Guidelines to the identification of threats related to inter-network communication

For the exchange of data concerning operation, maintenance and charging between service providers and network operators, a number of procedures will usually have to be defined for the specific inter-network communication.

To define possible threats to the inter-network communication it is necessary to:

- identify the concerned functional entities in the network and communication links between them;
- identify the individual procedures for each communication link against which threats can occur.

Threats concerning the communication between subscribers, users and other parties to the network should also be addressed.

All inter-network procedures should be investigated for threats, for example:

- transfer of charging data;
- transfer of updates to databases (e.g. home and visited databases);
- call handling procedures.

Generic threats to inter-network communication are, for example:

- network connection to the wrong database;
- masquerading of network entities;
- modification, deletion and replay of signalling and management data; and
- eavesdropping of signalling data.

7.5 Guidelines to the identification of threats to system integrity

All systems applied or implemented by service providers face a number of threats resulting from any internal systems security violations, like:

- unintended or hidden functionality;
- insufficient reliability;

that are caused by means of:

- local implementation;
- local operation;
- the domain specific security policy.

Some support can also be taken from the EU documentation on Information Technology Security Evaluation Criteria (ITSEC).

7.6 Guidelines to the identification of threats due to security policies

Service providers and system operators are likely to have different security policies within their local domains. This may lead to different quality levels for features like the protection of personal data integrity as well as for the security mechanisms supporting authentication and access control.

A threatening situation may, for example, occur when the strong authentication and access procedures of system or an underlying network are weakened simply by the chaining of this system or this underlying network with another system or underlying network that applies less secure authentication and access control procedures.

Another example of threats resulting from different levels of security between different security domains is the threat to confidential user data that is to be transmitted via the chain of some mobile radio network and some conventional network.

If two entities implemented two different levels of security there would be the danger that one undermines the security of the other.

Security policy might also include individual national regulation on legal interception etc. that may lead to different levels of security.

8 Risk assessment

The main goals of risk assessment are:

- evaluation and comparison of threats;
- risk assignment to threats;
- identification of major risks; and
- preparation of management decisions (by setting up comprehensive risk assessment reports).

Risk assessment relies very much on an appropriate preceding categorization and classification of threats. The result of the risk assessment procedure should be presented to the system/service provider respectively to the responsible TC/STC plenary as the "risk assessment report" for decision. The presentation should be provided by the responsible SEG and the decision should be taken by the responsible TC/STC.

The methodology for a risk assessment procedure is shown in figure 11.

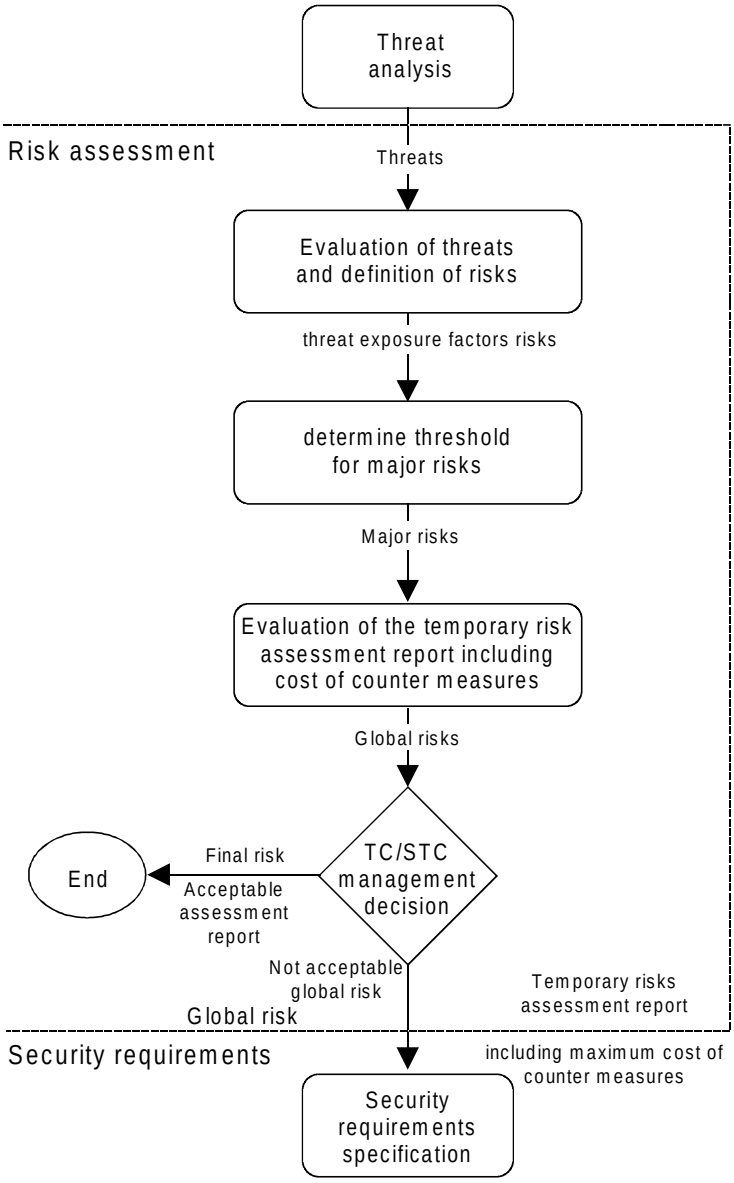


Figure 11: Methodology for risk assessment

TC/STCs plenaries may not be familiar with all aspects of security, however risks and the consequences for the system/service shall be brought to their full attention. Therefore the whole risk assessment procedure shall be documented in a comprehensible risk assessment report.

8.1 Evaluation of threats and definition of risks

In a first step all threats are evaluated according to the following scheme:

guideline to evaluate threats:

1) evaluate impact (= "I") on each threatened subject, e.g. using five different levels (1 through 5);

2) identify likelihood of occurrence (= "0") for each threat, using five different levels (1 through 5);

3) calculate an exposure factor (= "Ix0") for each threat;

4) identify the exposure ranking presenting a threat priority list;

5) put all this information into the threat evaluation table.

A threat evaluation table might look like table 4.

Table 4: Example of a threat evaluation table

Threat descriptor	Impact Value (I)	Likelihood of occurrence (0)	Exposure Factor (Ix0)	Exposure Ranking
Threat A	5	1	5	3
Threat B	3	3	9	1
Threat C	2	4	8	2

The exposure factor is a simple multiple of an assessment of the likelihood of a particular threat occurring, and the effect of that threat on the business/telecommunication service should it occur:

- the likelihood of occurrence should be graded on a simple scale (1 - 5 is a suitable resolution, with 1 being unlikely and 5 being highly likely);

- similarly the effect or impact of an occurrence should be graded on a simple scale (again, 1 - 5 provides sufficient resolution for evaluation purposes, 1 being low impact and 5 being high impact);

- the exposure factor is the multiple of the likelihood and the impact.

For example:

- threat A has a very low likelihood of occurrence (e.g. earthquake) but if it happens, would have a high impact so would have an impact grading of 5;

- threat B has a medium likelihood of occurrence (e.g. flood) and has a medium impact - 3;

- threat C has a fairly high likelihood of occurrence (e.g. incorrect data entry on a manual data entry system), but has relatively little impact so has an impact grading of 2.

These procedures make completely different threats comparable to one another with respect to the level of risk they mean to the system.

In a second step, a certain "risk" and its "risk evaluation value" is defined for each threat, as given in table 5.

The terms and values used in table 5 need to be such that they can be understood by non-security experts for evaluation and comparison. Terms that are usually used to define threats are mostly not very well understood by other people than the security experts themselves.

It should be noted the risk evaluation value sometimes has to be converted into monetary values. However, this conversion is outside the scope of this ETR. Therefore here we talk about "primary" evaluation values.

Table 5: Example for risk definition and the assignment of (primary) evaluation values

Risks		**Risk evaluation value**
loss of availability of resources or service		impact, percentage
loss of integrity or confidentiality		impact, frequency
loss of accountability (for actions or transactions)		impact, frequency
destruction of components		impact, number of identified components per period
loss of charges		impact, percentage
fraud	by subscriber	impact, percentage
	by intruder	
	by staff	
	by business partners	
loss of marketability		impact, percentage
penalty, e.g. for a breach of the law		impact, frequency
theft		impact, frequency
loss of trustworthiness	to subscriber	impact, frequency
	to third parties	
	to public	
	to authorities	

8.2 Determine threshold for major threats respectively risks

Risk assessment starts with the result of the evaluation of threats. A threshold has to be determined so that it can be decided which threats have to be treated further on in the risk assessment procedure and which not. For example, a threshold can be determined by setting a certain exposure factor.

8.3 Evaluation of the global risk, risk assessment report

The preceding analysis of individual risks comes out with a general evaluation of the risk situation for the system. This could be some kind of verbal interpretation of the evaluation tables set up previously.

All the tables, their interpretation for the global risk situation and recommendations on how to proceed are put down as a "temporary risk assessment report" appropriate for a management decision, e.g. in a TC/STC plenary meeting.

8.4 TC/STC management decision

In a TC/STC plenary the temporary risk assessment report is presented. It has to be discussed what expenditures in terms of time, money and effort could be afforded to meet the individual risks and what risks could be "accepted" and not further treated for countermeasures.

Therefore in case of each prioritized individual risk a decision has to be made. After that there is a mandate for the SEG against which risks countermeasures have to be worked out, beginning with the specification of security requirements. Also the SEG is given guidance what expenditures will be acceptable to the TC/STC for each individual countermeasures.

8.5 Setting up the final risk assessment report

After security requirements have been identified and countermeasures been investigated a review on threats and risks takes place.

In a final risk assessment report all non-avoidable residual risks are clearly identified also recalling the relevant (TC/STC) management decisions on that point.

As the final risk assessment report gives a good overview on the residual vulnerabilities of the secured system they should be kept as part of the system specification.

However, it could be reasonable to keep the final risk assessment report confidential.

9 Security requirements

For each threat associated with a prioritized risk identified in the risk assessment report a security requirement has to be postulated.

The number of different kinds of security requirements should be kept to a minimum.

However, they should be given attributes that allow a detailed specification. Security requirements should as much as possible be associated with the security features that have to be specified later on. This is to simplify the matching of countermeasures to the security requirements defined.

Figure 12 explains the methodology for the definition of security requirements.

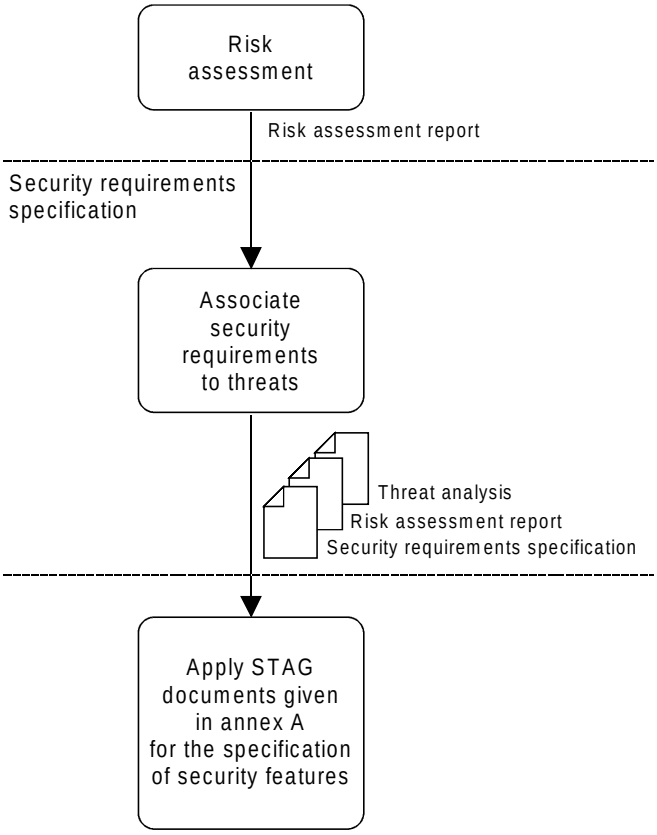


Figure 12: Methodology for a security requirements specification

A pre list of security requirements is presented in table 6. These will become more detailed following the assessment of more projects.

Table 6: Examples for common security requirements

Requirement	**Attributes (examples)**				
Authentication	Authenticated subject		Authenticated subject		
Mutual authentication	subject A	subject B	. . . .		
Integrity	File/message or dialogue		Voice	Data	. . . .
Non repudiation	. . . . .				
Receipt confirmation	. . . . .				
Protection against replay	. . . . .				
Protection against delay	. . . . .				
Protection against malicious traffic flow generation (note)	. . . . .				
Protection against misrouteing	Call/message				
Confidentiality	File/message or dialogue		Voice	Data	. . . .
Access control	. . . . .				
Activity monitoring	. . . . .				
Event control	. . . . .				
Security alerts	. . . . .				
Data protection	. . . . .				
Legal interception	. . . . .				
Evaluation according to ITSEC	. . . . .				
Charging control	. . . . .				
Access device identification	. . . . .				
Exclude service or function	. . . . .				
NOTE: e.g. Intended to increase a user's telephone bill.					

Sometimes it may be reasonable to present security requirements specifically with respect to either a service /system provider or to the user of the system, examples of which are given below:

- security requirements with respect to the service provider:

  - accountability;
  - correctness of user data transmitted;
  - controlled access to service network resources, e.g. via authentication of users;
  - confidentiality of signalling data;
  - availability of service;
  - integrity of signalling data;
  - non-repudiation of call charges;
  - auditing of service accesses;
  - prevention of misusing resources;
  - integrity of service and network management;
  - recognition of regulation. esp. data protection laws;

- security requirements with respect to the user:

  - availability;
  - reliability;
  - malicious call traceability;
  - privacy, anonymity, untraceability by another user or by an operator;
  - confidentiality of user data;
  - non-repudiation of data exchanged with other users;
  - authentication between users;
  - integrity of user data;

- security requirements with respect to external agencies:

  - provision for legal interception;
  - data protection restrictions;
  - evaluation requirements (e.g. ITSEC).

Annex A: List of work items referred to in this ETR

The following STAG work items are referred to in this ETR.

ETR 234:	"Security Techniques Advisory Group (STAG); A guide to specifying requirements for cryptographic algorithms".
ETR 330:	"Security Techniques Advisory Group (STAG); A guide to legislation, recommendations & guidelines governing the provision of security features".
ETR 237:	"Security Techniques Advisory Group (STAG); Baseline security standards; Features and mechanisms".
ETR 340:	"Security Technical Advisory Group (STAG); Guidelines for security management techniques".
DTR/NA-002603:	"Security Techniques Advisory Group (STAG); Guidelines for integrating security mechanisms into ETSI standards".
DTR/NA-002701:	"Security Techniques Advisory Group (STAG); Guidelines on the relevance of security evaluation to ETSI standards".

History

Document history	
November 1996	First edition

ISBN 2-7437-1144-2
Dépôt légal : Novembre 1996