MODSafe

European Commission
Seventh Framework Programme
MODSafe Modular Urban Transport Safety and Security Analysis

Acceptance, Approval, Certification

List of elementary activity modules

Deliverable No. D7.2

Contract No.	218606
Document type	DEL
Version	V1.0
Status	Final
Date	28-09-2011
WP	WP 7
Lead Author	Balázs Sághi BME
Contributors	TRIT, RATP, INRETS, LU
Description	Deliverable D7.2 Version 1.0
Document ID	DEL_D7.2_BME_WP7_280911_V1.0
Dissemination level	PU
Distribution	Consortium

Document History:

Version	Date	Author	Modification [*very short description]*
V0.1	21-01-2011	Balázs Sághi	New document: global structure
V0.2	21-04-2011	Balázs Sághi	First draft
V0.3	27-05-2011	Balázs Sághi	Reworked according to WP review
V0.4	19-07-2011	Balázs Sághi	Modified after WP review
V0.5	29-08-2011	Balázs Sághi	Modified according WP10 comments
V0.6	13-09-2011	Balázs Sághi	Modified according to TRIT comments
V0.7	24-09-2011	Balázs Sághi	Modified according to UITP comments
V1.0	28-09-2011	Balázs Sághi	WP10 consensus

Approval:

Authority	Name/Partner	Date
WP responsible	BME / WP7 Approval	26-09-2011
EB members	WP10 Approval	27-09-2011
Coordinator	TRIT	28-09-2011

SEVENTH FRAMEWORK PROGRAMME

Table of Content

List of Figures

1 Introduction

The Acceptance, Approval and Certification (AAC) procedures are characterised by high diversity in different European countries. Diverse actors are involved and different procedures and different roles are applied along the AAC course in the field of urban guided transport systems, which are non-interoperable with other rail systems and are rarely needed for interconnectivity with another rail system (e.g. tram-train). The diversity relates also to functional and safety requirements, safety models. The diversity also includes certain situations, in which there is no need for certification at all. However according to [MODURBAN D93] some synergies can be observed in this field.

The main objective of the work package 7 within this EU-founded MODSafe project is to make the diversity transparent for participants of these processes (suppliers, operators etc.) by developing and proposing a typical optimised framework for the AAC procedures, which is based on elementary activity modules and on an analysis of current AAC procedures over Europe.

This deliverable is dedicated to identify so-called elementary activity modules within the AAC procedures of different analysed practices.

1.1 References

Reference-ID	Document title, identifier and version
Case study UK	ModSafe WP6/7: Case Study UK (London Underground) Document ID: LU Case Study_WP67_V0_070709
Glossary.en	MODSafe Glossary - Deliverable No. D10.5
TS JV 2009:002	TS JV 2009:002 – Guide to the approval procedure (http://www.transportstyrelsen.se/Global/Jarnvag/English/Guideline/guide_to_the_approval_procedure.pdf)
JvSFS2006:1	JvSFS 2006:1 – "Järnvägsstyrelsens föreskrift om godkännande av delsystem m.m." (Regulation of the Swedish Transport Agency on the approval of subsystems in railways, etc. (incl. Metros and Trams).)
MODSafe D1.2	MODSafe Deliverable D1.2 State of the Art on Safety Responsibilities and Certification
MODSafe D6.1	MODSafe Deliverable D6.1 Survey of current lifecycle approaches
MODSafe D6.2	MODSafe Deliverable D6.2 Comparison of current safety lifecycle approaches
MODSafe D6.3	MODSafe Deliverable D6.3 Proposal of a common safety life cycle approach
MODSafe D7.1.	MODSafe Deliverable D1.2 Survey of Current AAC procedures
MODSafe DOW	MODSafe Annex 1 - Description of Work
MODURBAN D93	ModUrban Deliverable Report – WP23 – D93
ROGS	http://www.legislation.gov.uk/uksi/2006/599/pdfs/uksi_20060599_en.pdf
Transportstyrelsen	Transport Styrelsen /Railway - Homepage http://www.transportstyrelsen.se/en/Railway/Approval/

1.2 Terms and Abbreviations

The terms used in this project are explained in the document [GLOSSARY.en]. In addition, the following abbreviations are used in this document:

Abbreviation	Explanation
AAC	Acceptance, Approval, Certification
AOT	Autorité Organisatrice de Transport Transport Organising Authority (in France)
AP	Assurance Plan
BOStrab	Verordnung über den Bau und Betrieb der Straßenbahnen (BOStrab) German Federal Regulation on the Construction and Operation of Light Rail Transit Systems (including metros)
CAP	Change Assurance Plan
CNESTG	Commission Nationale d'Évaluation de la Sécurité des Transports Guidés National Committee for Evaluation of Guided Transport Safety
DART	Directors' Assurance Review Team
DDE	Direction Départementale de l'Equipement Departemental Directorate of Equipment
DDR	Detailed Design Reviews
DDS	Dossier de Définition de Sécurité (Safety Definition Case)
DPS	Dossier Préliminaire de Sécurité (Preliminary Safety Case)
DRACCT	Directors' Risk Assurance and Change Control Team
DRIEA	Direction Régionale et Interdépartementale de l'Equipement et de l'Aménagement d'Ile de France (Regional and Interdepartmental Directorate of Equipment and Development for Ile de France area)
DS	Dossier de Sécurité (Safety Case)
EAM	Elementary Activity Module
EOQA	Expert ou Organisme Qualifié Agréé Independent Safety Assessor (in France)
ESAC	Engineering Safety & Assurance Case
ESC	Engineering Safety Case
ESHL	Engineering Safety Hazard Log
FR	Functional Requirement
HMRI	Her Majesty's Railway Inspectorate
ICP	Independent Competent Person
ISA	Independent Safety Assessor
LU	London Underground
ORR	Office of the Rail Regulator (Safety)
PAP	Project Assurance Plan
PCHC	Project Completion & Handover Certificate
PEP	Project Execution Plan
PHA	Preliminary Hazard Analysis
PMF	Project Management Framework
PPP	Public Private Partnership
RAMS	Reliability, Availability, Maintainability and Safety
ROGS	Railways and Other Guided Transport Systems Regulations 2006
SAR	Safety Assessment Report
SMS	Safety Management System

Abbreviation	Explanation
SR	Safety Requirement
SRS	System Requirements Specification
SSC	System Safety Case
STRMTG	Service Ttechnique des Remontées Mécaniques et des Transports Guidés French Technical Agency for Ropeways and Guided Transports Safety
SVS	Safety Verification Scheme
TAB	Technische Aufsichtsbehörde (Technical Supervisory Authority)
TL	Tube Lines
TO	Transport Operator
TR SIG ZA	Technische Regeln Zulassung und Abnahme von Signal- und Zugsicherungsanlagen gemäß BOStrab
TRS	Technical Requirements Specification
TSI	Technical Specification for Interoperability
UGT	Urban Guided Transport
UML	Unified Modelling Language
VAP	Verification Activity Plan
VVR	Verification and Validation Report

The definition of terms Acceptance, Approval and Certification was done in [MODSAFE D7.1] as follows:

Acceptance: the status given to a product by a final user. In case of urban guided transport (UGT-) system the final user is the operator, so the acceptance shows the operator's positive opinion about a specified technical system. (This does not necessarily mean a final permission for putting the system into service, as in many cases further permissions are also required, like e.g. independent safety assessment or certification.).

Approval: the final (formal) decision to permit to use a system, regardless of which body, authority or institution makes this final decision. (In some cases the final decision is made by the operator – in these cases acceptance and approval may cover the same activity.)

Certification: a procedure of examination or investigation, fulfilled by an independent body (i.e. independent from the developer, the supplier and the operator of the system), in order to state, whether the examined product or system fulfils some functional and/or safety requirements. (The independent body can be in some cases an authority or another designated, competent person or body.)

2 Method of the work package

This chapter briefly introduces the method of work package 7.

As mentioned in the introduction, the Acceptance, Approval and Certification (AAC) procedures are characterised by high diversity in different European countries. The main objective of this work package is to develop a typical optimised framework for the AAC procedure based on elementary activity modules and on an analysis of current AAC procedures over Europe.

Such typical optimised framework could offer relevant authorities a common reference over Europe and therefore facilitate the creation of new UGT-systems.

A typical optimised framework AAC procedure can only be proposed based on an adequate analysis and synthesis process (Figure 1). The analysis phase of this WP consists of two steps: first the current AAC procedures in different countries and cities of Europe were reviewed in [MODSafe D7.1]. Secondly, in this survey the elementary activity steps were identified. As a result a list of elementary activity modules is provided in this deliverable. In the synthesis phase first a typical model of an AAC procedure are drafted based on the elementary activity modules. In a second step, based on the typical model, a typical optimised framework AAC procedure is proposed.

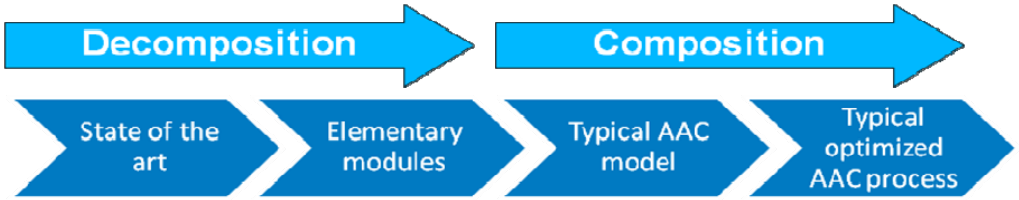


Figure 1 – Work process of WP7

The work process is organised into different tasks:

Task 7.1: Survey of current AAC procedures
Any future proposal can reach its aim only if the current situation is clear, functions and motivations in the current processes are understood. Thus, in this task a compilation of current AAC procedures in different European countries is carried out.

Task 7.2: Identifying elementary activity modules (current task)
A convergence of the different national and regional framework AAC procedures may only be successful, if a generic AAC model consists of *elementary activity modules*. Though carried out by different authorised bodies or at different phases of the safety life cycle the formal activities carried out in the different AAC procedures are to a wide extent similar. A main task is to identify the major *activity modules* on which the AAC processes are in principle based.

Task 7.3: Typical AAC model
Under this task a typical AAC procedure, based on the elementary activity modules is modelled and proposed.

Task 7.4: Proposal for a typical optimised AAC process
Based on the survey and based on the generic description of an AAC process a typical (i.e. clear, logical and both in time and cost minimal resources) process framework is developed and proposed.

As described in the [MODSafe DOW], results of [MODSafe D1.2] have been used as input for the survey [MODSafe D7.1], mainly taking credit of the case studies. For this delivery [MODSafe D7.2] - identifying the elementary activity module - synergy effects have been used, sharing the results with WP6 [MODSafe D6.1], [MODSafe D6.2] and [MODSafe D6.3] due to the fact that Work Packages 6 and 7 have a common base and interdependencies.

3 Methodological background of D7.2

In order to achieve the goal of this task, it is necessary to lay down its methodological basis. The elementary activity modules (EAM) are activities, that are identical in their generic principle as part of approval, acceptance and certification processes of different countries, but they may be carried out by different parties with different level of independency, furthermore partly at different stage of the system life cycle.

To identify these elementary activity modules, they have to be found in different processes. These can be effectively achieved, if different procedures of different countries or cities can be compared. The comparison will deliver adequate results, if the different processes are described in the same way, i.e. using the description method. The applied description method is described in sub-clause 3.1.

After finishing Task 7.1 (Survey of current AAC-procedures [MODSafe D7.1]) it became obvious that the identification of EAM's is most effective with an appropriate selection of countries, which represent different practices in Europe. The processes of these countries are analysed in more detail. This selection method is described in sub-clause 3.2.

3.1 Means of description

To be able to compare the different processes of different countries or cities a common description method has to be found. A compilation of possible description means was done in deliverable 7.1. There the following methods were introduced as possible means:

- Simple block diagram,
- Flowchart,
- Cross functional flowchart,
- UML activity diagram.

The simple block diagram is very intuitive from the application point of view, but it has the disadvantage that this method does not represent well the timing aspects and subsequent activities. On the other hand the relations between organisations are represented clearly.

Flowcharts represent the successiveness of processes well, but the different actors are not easy to distinguish.

The so-called cross functional flowchart has all of the advantages of flowcharts, plus the activities can be clearly distributed between the actors or organisation units.

UML activity diagrams are well formalised method to describe processes; the information content is similar to cross functional flowcharts, however there are more restrictions because of higher level of formalisation.

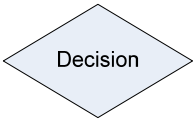
After the evaluation of strengths and weaknesses of different methods, the cross functional flowcharts were selected.

A flowchart generally is a type of diagram that represents an algorithm or process, showing the steps as boxes of various kinds, and their order by connecting these with arrows. This diagrammatic representation can give a step-by-step solution to a given problem. Process operations are represented in these boxes, and arrows connecting them represent flow of control. Data flows are not typically represented in a flowchart, in contrast with data flow diagrams; rather, they are implied by the sequencing of operations. Flowcharts are used in analysing, designing, documenting or managing a process or program in various fields.

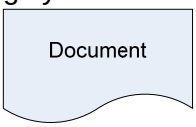
Flowcharts are used in designing and documenting complex processes. Like other types of diagram, they help visualise what is going on and thereby help the viewer to understand a process, and perhaps also find flaws, bottlenecks, and other less-obvious features within it. There are many different types of flowcharts, and each type has its own repertoire of boxes and notational conventions. The two most common types of boxes in a flowchart are:

- a processing step, usually called activity, and denoted as a rectangular box

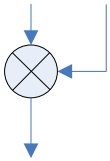
- a decision, usually denoted as a diamond.



Furthermore in the description of acceptance, approval and certification processes the following symbol is used to represent a result of a process, in form of a documentation:



To represent the merging of two processes the following symbol is used:



A flowchart is described as **cross-functional** when the page is divided into different swimlanes describing the control of different organisational units. A symbol appearing in a particular "lane" is within the control of that organisational unit. This technique allows the author to locate the responsibility for performing an action or making a decision correctly, showing the responsibility of each organisational unit for different parts of a single process.

The applied template for the description of AAC procedures therefore include the participants (each represented as column or swimlane), and the three types of boxes, as depicted in Figure 2. The number of the columns can be of course adjusted to the requirements: if a process has more participants, there can be more columns used.

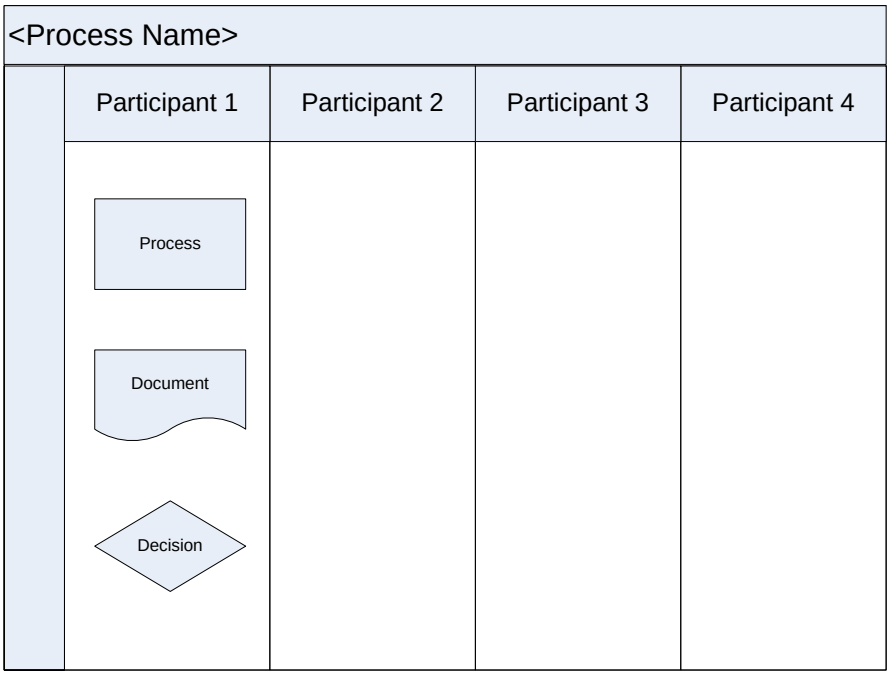


Figure 2 – Template for the description of AAC procedures

The formal representation of the processes can be depicted on cross functional flowcharts, but there is obviously a strong need for textual descriptions, which can add more information, to understand the processes more easily.

3.2 Selection of case studies for detailed process

As mentioned earlier, it became obvious that the identification of EAM's is most effective with an appropriate selection of countries, which represent different practices in Europe. The processes of these countries are analysed in more detail.

During the analysis those countries which have not got relevant UGT-systems, and countries from which a reliable source of information was not available, were not considered. These considerations are based on the experiences which were gained in course of tasks 6.1, 6.2 and 7.1 which aimed to collect information about the current status of AAC procedures.

On the other hand such a selection (based upon information from [MODSafe D7.1]) was required which can reflect different approaches, juridical and cultural differences of European countries.

After considering all of these issues, the following cases were selected, for which a detailed description of approval, acceptance and certification procedure was elaborated:

- France,
- Germany,
- Hungary,
- United Kingdom (London Underground),
- Sweden.

In the following chapter these case studies are described.

4 Description of AAC procedures for case studies

This chapter contains the description of AAC procedures for selected countries (see 3.2). For the formal description cross functional flowchart was selected (see 3.1).

4.1 Case “France”

For the AAC process in France firstly the key participants of the process are listed, then the main documents are presented, and in the end the process description can be found.

4.1.1 Key players in the process

AOT:
In France the public authorities are responsible for organising passenger transport (e.g.: Government itself, regions, departments, cities or groups of cities). The **Transport Organising Authority** (AOT) is appointed to qualify these levels of responsibility. It takes the main decisions in terms of defining services, pricing and finance. To operate a transport network, AOT may choose between direct use (régie in French) and public service delegation. In the latter case, operator is chosen by AOT by using open tender.

CNESTG:
This safety assessment commission was set-up in June 2003 as a national commission. Its role is to give accreditation to the **EOQA** (Independent Safety Assessor) in accordance to **STRMTG** rules. This commission can also advise the Prefect on special dispensation or exemption from the regulations (in case of technologic innovation for example).

STRMTG:
In France, STRMTG the French Technical Agency for Cableways and Guided Transports safety and its departmental or regional agencies are intended to assess all safety analysis in order to give expert opinion to the Prefect for approval or rejection of new applications. The regional agencies are joined to **STRMTG** since the beginning of 2011. These regional agencies provide advice to the **DDE** (**DREIA** for Ile de France) to give an opinion about safety cases.

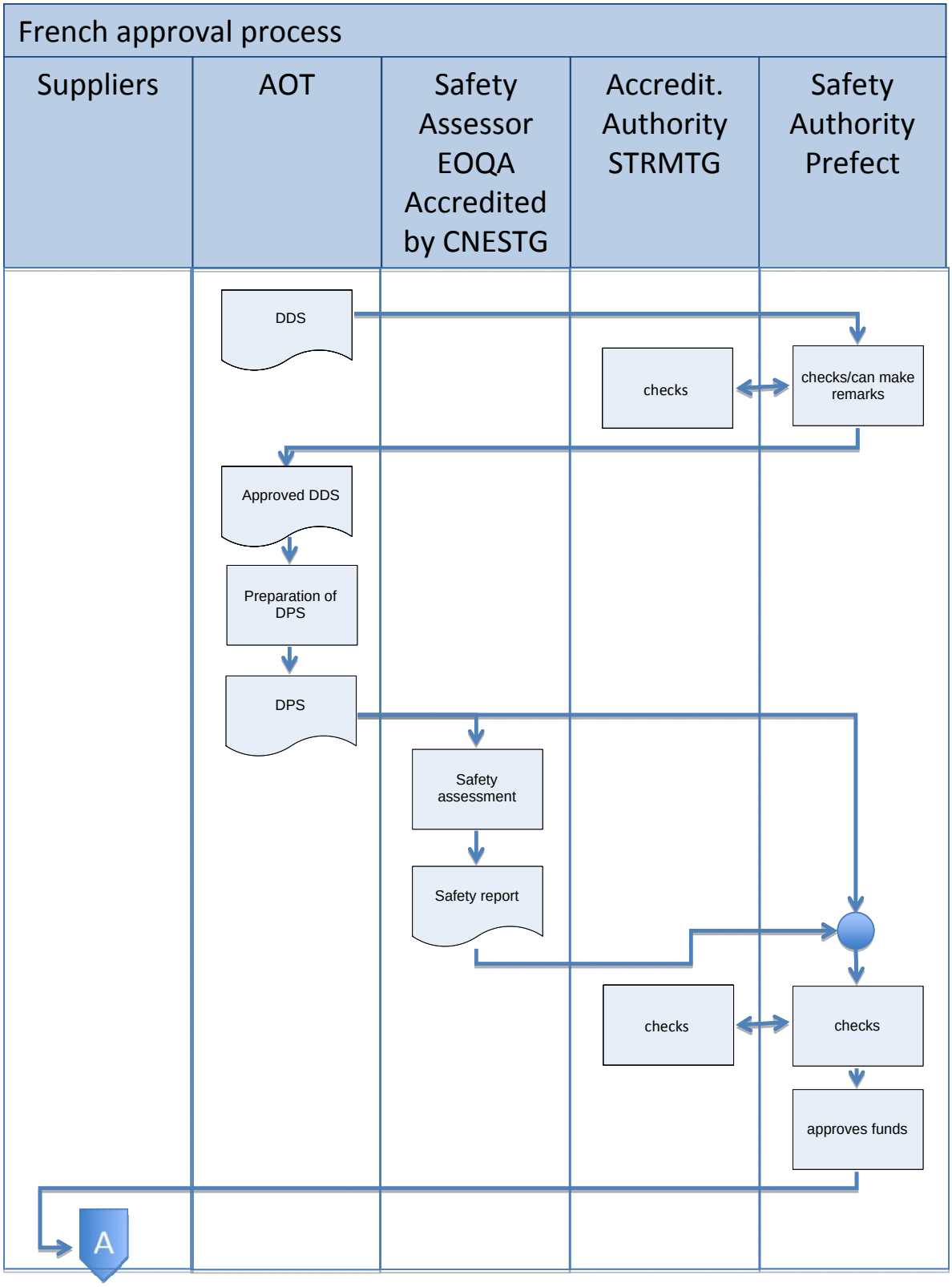
4.1.2 Documents

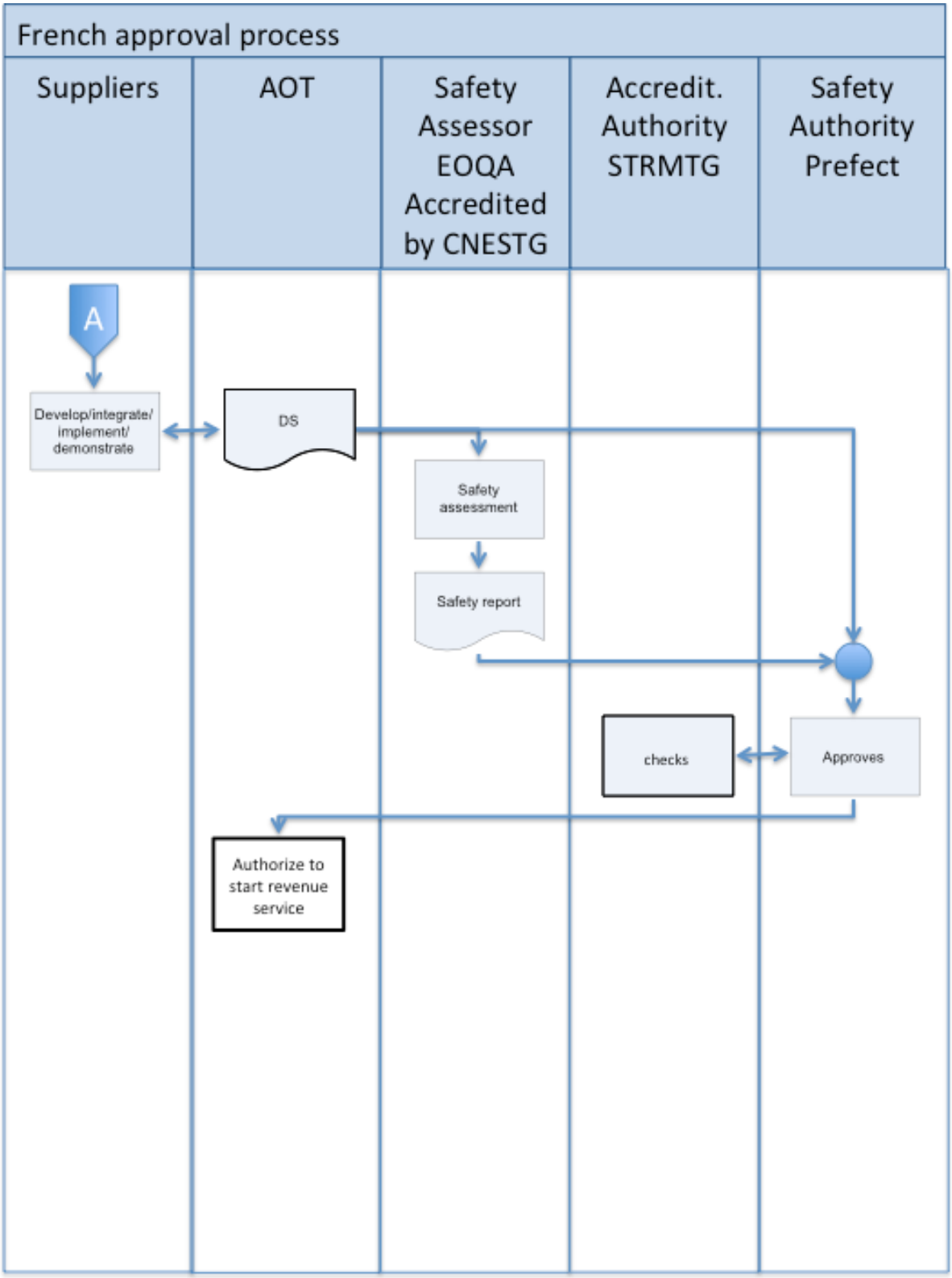
DDS:
The Safety Definition Case is the first step to initialise a dialog between the Transport Organising Authority (**AOT**) and the relevant representatives of the national Safety Authority (**Prefect**, **DRIEA**/**DDE**, **and STRMTG**). It applies the legal framework by establishing the Preliminary Safety and Quality Plans and the main characteristics (functional, technical, the general safety targets). It also includes an important point namely the reference system: set of regulations, standards, and instructions applicable to the system. It may be considered as a concept submission to the safety authority that accepts it or not. The assessment of the **DDS** by an independent Safety Assessor is not mandatory.

DPS:
The Preliminary Safety Case specifies in detail the safety targets, the requirements, the methods and the principles used to reach them. The **DPS** also includes an update of all chapters of the **DDS**, in particular for the most important chapters regarding safety aspects. An independent safety assessor report delivered by an **EOQA** is added to the file. In some cases several **EOQA** can be involved for a same project for different subsystems or at different levels. The national Safety Authority approves the **DPS**; the starting point of works is given by supplying the funds.

DS:
The safety case is the final and most important document. It includes the **DDS** and the **DPS** updated, and has to demonstrate that the requirements described in the **DPS** are fulfilled. It classically includes a hazard log, to keep track of the coverage of all Hazards identified in the PHA, including the reference of the justification documents (detailed safety analyses, calculation notes, test reports, operating and maintenance requirements, etc.). A second independent safety assessor report delivered by the same independent Assessor body (**EOQA)** is added in this file. To summarise, it can be stated that the **DS** file gives the assurance that the system reached the safety targets. It is constantly updated and managed by the operator during the whole life cycle of the concerned system(s).

4.1.3 Process description




French approval process
Suppliers
AOT
Safety Assessor EOQA Accredited by CNESTG
Accredit. Authority STRMTG
Safety Authority Prefect
A
Develop/integrate/ implement/ demonstrate
DS
Safety assessment
Safety report
checks
Approves
Authorize to start revenue service

4.2 Case “Germany”

4.2.1 Legal Bases

The process for approval and acceptance to be followed for Tram-, Light Rail- and Metro applications is based on the "German Federal Regulation on the Construction and Operation of Light Rail Transit Systems" (BOStrab) as required there in §60, §61 and §62.

It is the legal fact that the transport company, which is obliged by state-licence to carry out operations, is the entity which is responsible for all safety aspects of operations. It is responsible that premises and installations used for operations are designed in an appropriate way and are maintained in a state which allows safe operations. This applies even, if design of network or subsystems as well as manufacturing of subsystems and their maintenance are carried out by external companies (e.g. railway supplier industry).

To ensure that all laid down legal requirements are observed by the transport company, all activities are subject to be supervised by a safety regulatory authority. Although BOStrab is a federal regulation, each Federal State of Germany has its own safety regulatory authority, which is appointed by the Ministry of Transport of the respective Federal State, for the field of Trams, Metros and Light Rail called "Technical Supervisory Authority (TAB)".

For Signalling and Train Control and Protection Systems, the process for approval and acceptance is laid down in the Technical Rule (TR SIG ZA, eng. TR SIG AA), issued by the VDV. Such Technical Rules following the provisions of BOStrab are issued with agreements of the Federal Ministry of Transport and the Technical Supervisory Authorities of the Federal States. There is no direct mandatory obligation to use these Technical Rules, but it is usually accepted and more and more required. Because of its generic content covering the required process, the spirit of TR SIG ZA might be used also for all types of subsystems including rolling stock. TR SIG ZA uses the CENELEC standards EN 50126/128/129 as a base or, if applicable, DIN EN 61508.

Currently for vehicles there is not such a technical rule for the process. Instead, there are technical rules (guidelines) for several aspects, e.g. brakes, fire protection, electrical equipment, which contain technical requirements.

Similarly, there are technical rules (guidelines) for the tracks, e.g. route planning (“Trassierungsrichtlinie”) or the interaction between wheels and rails (“Spurführungsrichtlinie”).

Independent from sub-systems there are technical rules for driverless operation of UGT systems. VDV_399 raises requirements on the equipment of stations in order to guarantee the safety of passengers. It supports the Preliminary Guidelines for the Driverless Operation according to the BOStrab (“FoF”). ”FoF“ contains technical requirements for operation, track, stations, and vehicles for driverless operation, mirroring and refining applicable requirements of the BOStrab.

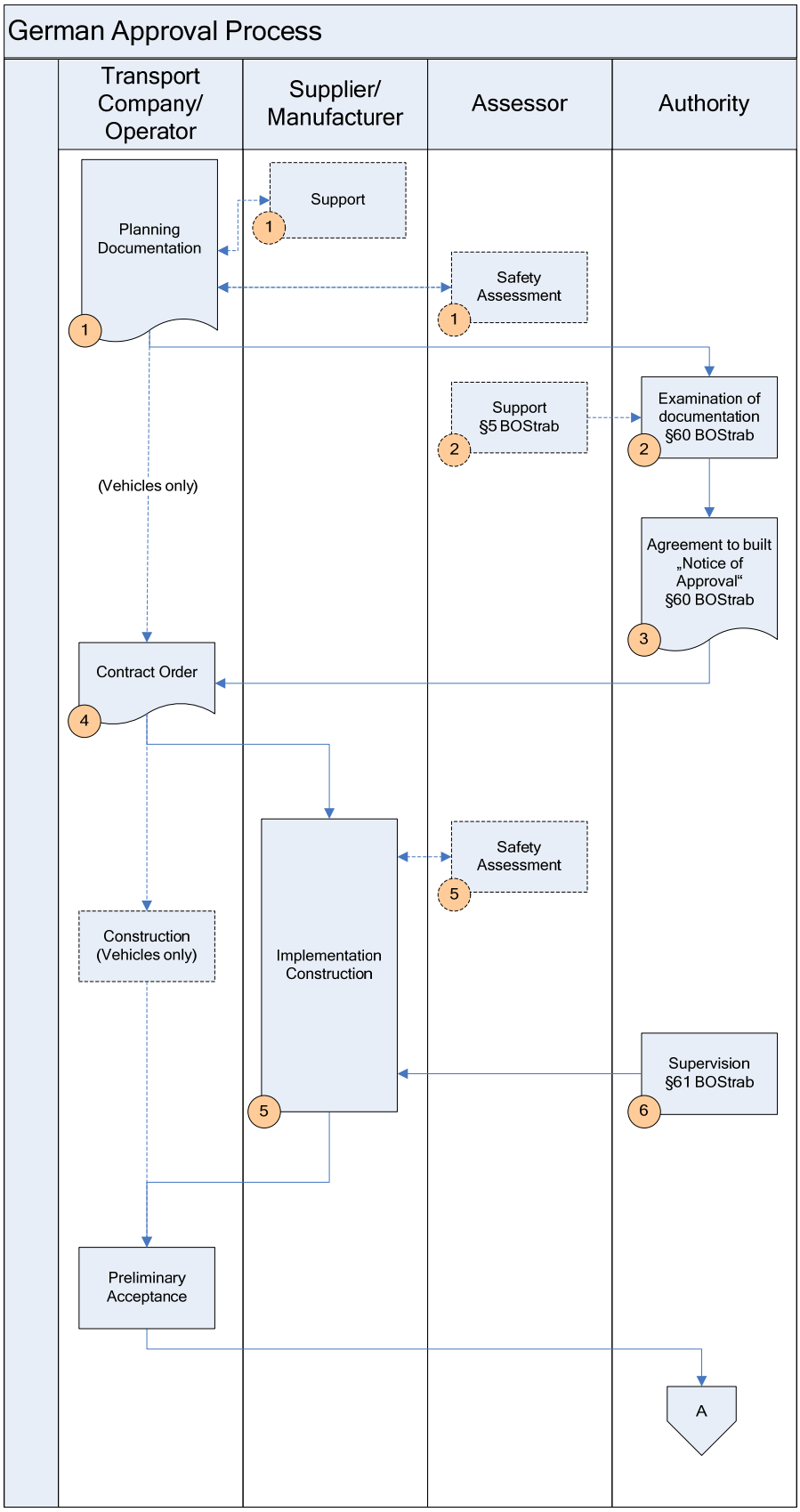
The Technical Supervisory Authority (TAB) issues, as the final act of an approval process, a so-called ”Abnahmebescheid”, which is to be understood as an Authority Approval and legal permit to put the system into commercial operation.

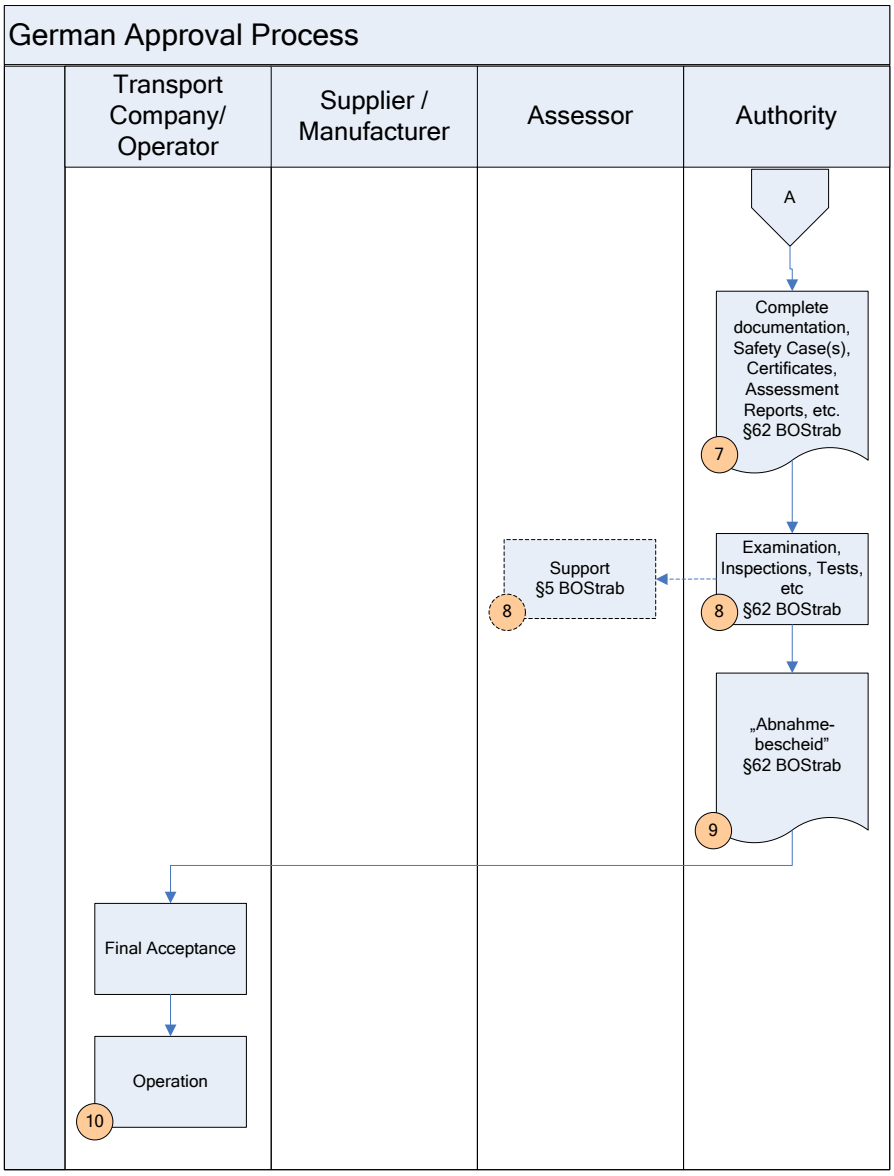
4.2.2 General Process and Responsibilities

The interaction between roles in an approval process has in principal already been introduced in [MODSafe_D1.2], sub-clause 8.1.4 and [MODSafe_D6.1], sub-clause 3.5.

This case focuses on the safety of “pure” Tram-, Light Rail- and Metro systems according to BOStrab only. Mixed systems, where Light Rail etc. vehicles and Heavy Rail vehicles share the same tracks or cross borders of Federal States, and thus require the involvement of more than one safety regulatory authority, is not discussed. Not safety related issues are also outside the scope.

The process and the roles are depicted in the following figure. It has to be noted that the mentioned Independent Safety Assessors may be different from each other.


German Approval Process
Transport Company/ Operator
Supplier/ Manufacturer
Assessor
Authority
Planning Documentation
1
Support
1
Safety Assessment
1
Support §5 BOStrab
2
Examination of documentation §60 BOStrab
2
(Vehicles only)
Agreement to built „Notice of Approval“ §60 BOStrab
3
Contract Order
4
Safety Assessment
5
Construction (Vehicles only)
Implementation Construction
5
Supervision §61 BOStrab
6
Preliminary Acceptance
A



Typically the process starts with the planning of a project by the transport company (1). Dependent of the type and the complexity of the project the transport company may already be supported by a supplier and / or an Independent Safety Assessor. If it is an infrastructure project (e.g. track and signalling system), after completion of the planning the transport company applies for the "Notice of approval" by the TAB (2). This step is not required for vehicles. With this the company provides the necessary documentation to the TAB. This step is laid down in §60 of the BOStrab. The TAB examines the documentation for compliance with the applicable legal and technical requirements.

After successful examination of the documentation the TAB issues the "Notice of approval", which is the agreement to build (3). With this agreement the company may order (4) the manufacturer / contractor to begin the implementation (5).
According to §61 of the BOStrab the TAB supervises the construction of installations (6). They may limit their activity to spot checks.

After finishing of the implementation and the preliminary acceptance, the company applies

for the “Acceptance” by the TAB according to §62 of the BOStrab (7). This step is also required for vehicles. This application is accompanied by the complete documentation of the implemented / erected system.

The documentation is typically a Safety Case and may include assessment reports and type / product certificates issued by (an) Independent Safety Assessor(s) and / or already existing type approvals. The TAB examines the documentation, inspects the system and may carry out tests (8). Again, according to §5 of the BOStrab, the TAB may use other competent persons and organisations, e.g. an Independent Safety Assessor.

After successful examination of the documentation, inspection, and practical demonstrations (tests) the TAB issues a so-called (“Abnahmebescheid”) (9). With this legal permit the transport company is allowed to start operation (10).

4.3 Case “Hungary”

The main steps and the participants of the approval, acceptance and certification procedure are demonstrated on a flowchart diagram (see next pages). In the following the main steps are discussed in more detail. The numbers refer to the process numbers on the flowchart.

1. The operator of the system (e.g. the railway company) formulates its functional and safety requirements in a document *Requirement Specification*.
2. This document has to be checked by the *National Transportation Authority*. The Safety Authority can accept the document or may suggest modifications.
3. The developer designs the product according to the requirements of the SRS.

   As a result of the development not only the *system* is produced, but also the *documentation* and the respective *safety case*.
4. The development may be followed by an independent safety assessor, according to the CENELEC standards (if it is required). The safety assessor investigates, whether the system development accords to the relevant standards. The result of the assessment is summarised in a *Safety Assessment Report* (SAR).
5. On the basis of the system documentation, the safety case and the SAR, the independent “certifier” certificates the system. During the certification it is examined, whether the developed system fulfils the requirements, formulated in *Requirement Specification*.

   With the certifier body is the situation in Hungary something special: the role of the independent certifiers is being played by authorised universities, in particular by two university departments, who have the required knowledge and independency.

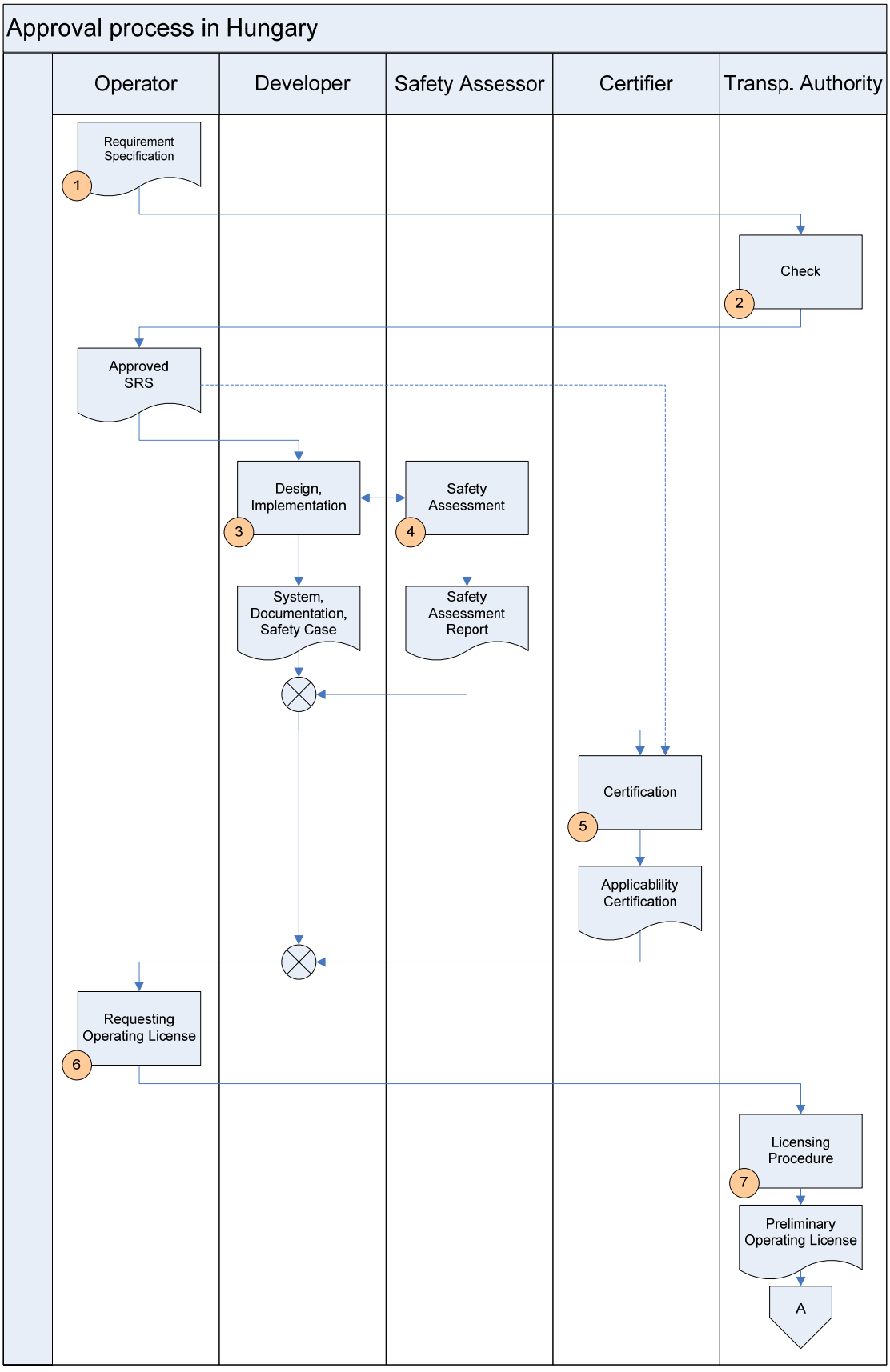
   As a result of the certification process, the certifier issues a document, called *Applicability Certification*, which contains all conditions, under which the system can be applied.

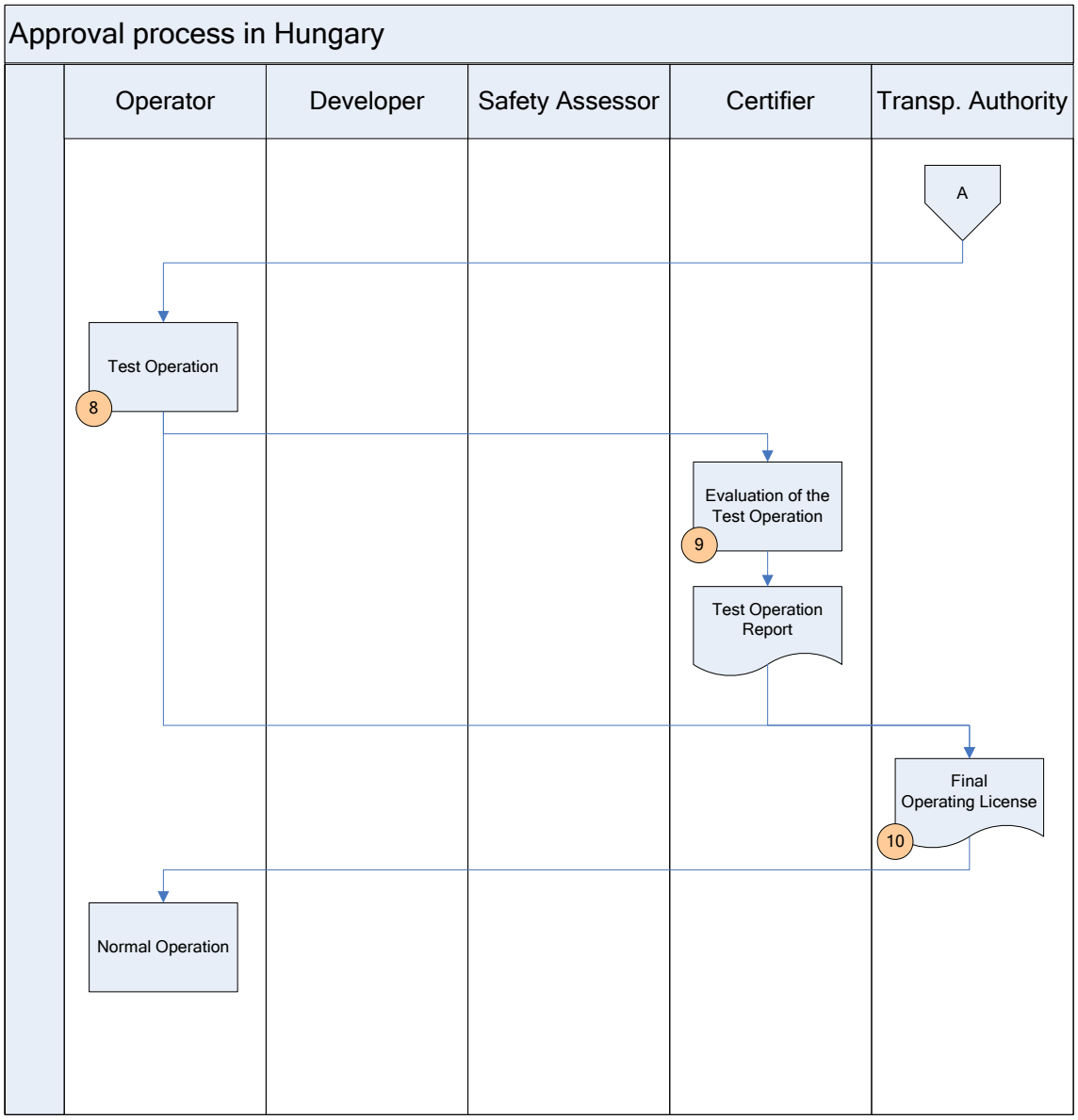
   The certification is ordered by the developer, so the Applicability Certification is handed over to the developer.

   This certification process is often divided into more phases (this is not depicted on the picture):

   - At first, only a *Preliminary Applicability Certification* is issued, which states, that the system can be so developed or modified, that it will probably fulfil the requirements of the operator.
   - Then, before starting the test operation (see later), a *Consent* is issued (of course after adequate investigations), by which the certifier consents to the starting of the test operation.
   - Finally, after a successful test operation a *Final Applicability Certification* will be issued.
6. The developer (contractor) gives over the necessary documentation, safety case and the Applicability Certification to the operator. With all of this, the operator can request the operating license from the transportation authority.

7. Based on the handed over documentation the safety authority performs a *Licensing procedure* and as a result, gives out a Preliminary Operating License. During this investigation the authority is mainly supported by the Applicability Certification, prepared by the independent certifier.
8. After receiving the Preliminary Operating License, the Operator may put the system into service (test operation).
9. The results of the test operation are evaluated by the certifier in a Test Operation Report.
10. After a successful *test operation*, and based on the positive Test Operation Report of the Certifier, the Operator receives the final Operating License from the Safety Authority.


Approval process in Hungary
Operator
Developer
Safety Assessor
Certifier
Transp. Authority
Requirement Specification
1
Check
2
Approved SRS
Design, Implementation
3
Safety Assessment
4
System, Documentation, Safety Case
Safety Assessment Report
Certification
5
Applicablility Certification
Requesting Operating License
6
Licensing Procedure
7
Preliminary Operating License
A


Approval process in Hungary
Operator
Developer
Safety Assessor
Certifier
Transp. Authority
A
Test Operation
8
Evaluation of the Test Operation
9
Test Operation Report
Final Operating License
10
Normal Operation

4.4 Case “United Kingdom - London Underground”

In the following sub-clauses the acceptance, approval and certification procedures of London Underground is presented, as an example from the UK. Note, that other operators in the UK may follow different procedures.

4.4.1 Legislation and process description

In the United Kingdom, the process to be followed for the introduction of new or altered vehicles or infrastructure is currently mandated by the Railways and Other Guided Transport Systems (Safety) Regulations 2006 (ROGS). ROGS were introduced to demonstrate how UK puts the requirements of the European Railway Safety Directive 2004 into practice. ROGS replaced 3 key regulations – The Railways (Safety Case) Regulations 2000, The Railways (Safety Critical Work) Regulations 1994 and The Railways and Other Transport Systems (Approval of Works, Plant and Equipment) Regulations 1994. When ROGS came into force it allowed the government safety regulator, Her Majesty’s Railway Inspectorate (HMRI), to withdraw from direct approval of changes to railway infrastructure and transferred that role and accountability to the Transport Operator. HMRI’s prime role is now to assess the Safety Management Systems of Transport Operating companies, such as London Underground, and grant them a Safety Certificate once they have approved their Safety Management System.

Under ROGS, no-one is allowed to run vehicles or manage infrastructure unless the Office of the Rail Regulator (ORR) has awarded them with a Safety Certificate (for transport undertakings) or authorisation (infrastructure managers). (This replaces the requirement to hold a Safety Case under the Railways (Safety Case) Regulations 2000.)

4.4.1.1 Safety Certificate

A Safety Certificate is held by a Transport Operator. It is a document issued by ORR, valid for up to 5 years, that permits the Transport Operator to carry out a specified operation or operations. The certificate describes the type and/or extent of the operation and references the evidence on the basis of which it is issued. It certifies ORR’s acceptance that the holder has produced:

- sufficient written evidence that their SMS satisfies the requirements of the Regulations and,
- sufficient written evidence of the provisions adopted to meet the requirements necessary to ensure safe operation (documented within the Safety Management System).

4.4.1.2 The Safety Management System (SMS)

The Safety Management System is required to have, among other things, clearly defined procedures in place to introduce new or altered vehicles or infrastructure safely. Two key elements of these procedures for assessment and approval of changes are a “Written Safety Verification Scheme” and the use of Independent Competent Persons to perform a safety

and conformity assessment of the project as part of the verification process. It is important to note that safety verification is only needed if the risk arising from the project is new (or new to the transport system) and there will be a significant safety risk or significant increase in safety risk from the introduction of new or altered vehicles or infrastructure on the railway in question. Introduction of new or altered vehicles or infrastructure which is seen as a "substantial change" also requires the Transport Operator to apply for an amended safety certificate or authorisation.

4.4.1.3 SMS - London Underground Standards and Project Management Processes

This section gives a brief description of the primary standards within the Safety Management System of London Underground and its contractor (Tube Lines) that define the verification activities and assurance documentation which are required to comply with the requirements of the ROGS Regulations. The Safety Management System is embedded within the London Underground Company Management System. London Underground has also developed the Project Management Framework (PMF) suite of procedures and guidance which are part of the Company Management System and they are also mandatory for any party managing and delivering programmes or projects. The PMF details how London Underground projects should be managed, the project delivery lifecycle, key deliverables and roles and accountabilities for all parties involved. As Tube Lines are a separate company they are not required to follow PMF, although they are required to comply with London Underground standards such as 1-538 Assurance. The diagram below shows the linkage between the PMF lifecycle and 1-538 Assurance activities.

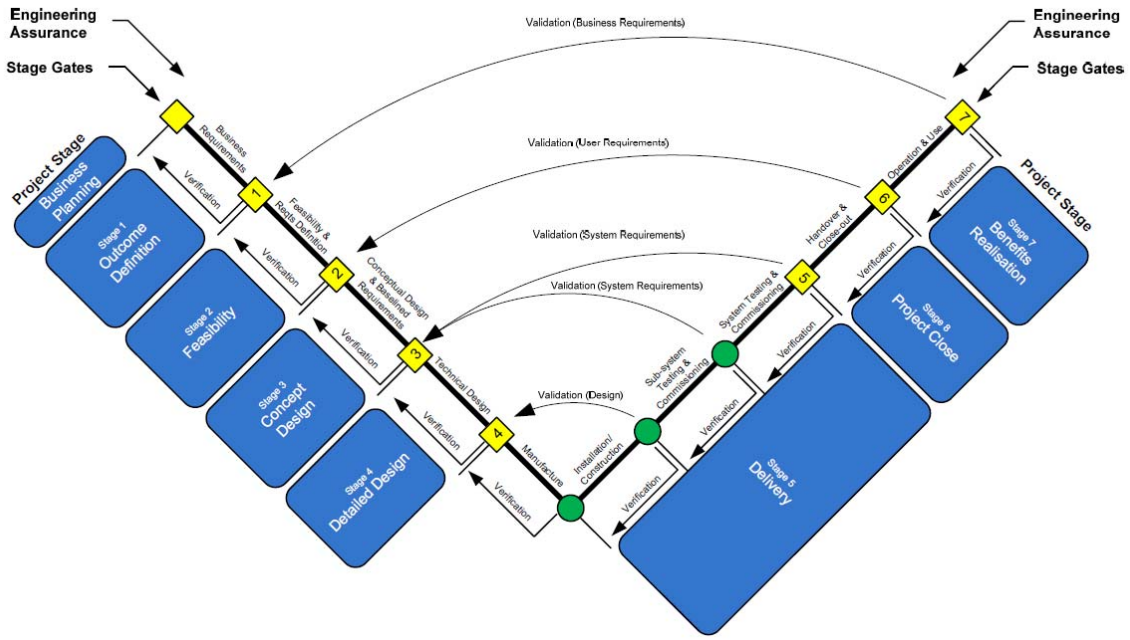


Figure 3 – Linkage between the PMF lifecycle and 1-538 Assurance activities

LU Standard 1-538 Assurance

The purpose of this standard is to define the requirements for the management and delivery of assurance by both providers and receivers of assurance. The definition of assurance is the extent that defined requirements have been complied with and that controlled processes have been followed in achieving the deliverables.

The following are key requirements from standard 1-538:

1. LU and its suppliers shall establish documented and controlled processes and procedures for both receiving and providing risk based assurance in respect of initiation, development, design, construction, delivery, testing, commissioning and handover of new, refurbished or altered systems or assets (infrastructure or vehicles);

2. No change, project or contract for service shall be commenced until:
   - An Assurance Plan / Project Execution Plan (PEP) / Change Assurance Plan (CAP) is approved by LU,
   - all pre-implementation risk control measures have been established and pre-implementation actions and conditions complied with, in accordance with the relevant Assurance Plan / PEP / CAP or management system arrangements.

   Note: the CAP and PEP are documents produced by internally-led Projects, Assurance Plans are produced by projects initiated by Third Parties or Suppliers (e.g. Tube Lines). To aid understanding the universal term Assurance Plan is used in the rest of this section.

   An Assurance Plan is a document which outlines the supplier's assurance milestones; and defines the supplier's proposals for providing evidence of assurance to LU at each assurance milestone, by way of tests, demonstrations or otherwise and it is one of the key documents that is assessed as part of the Verification activities of LU.

3. During the project lifecycle, LU have defined 3 assurance "gateways" at which assurance evidence is required to be provided (in formal documents) by the supplier and assessed by LU. The gateways and documents are as follows:
   - Concept Design (documents – Conceptual Design Statement & Concept Report)
   - Detailed Design (documents – Design Check Certificates and Compliance Report / Declaration)
   - Delivery (documents - Consent to Test / Trial Report, Staged Completion Report, Completion & Consent to Operate Reports / Engineering Compliance Declaration, Project Completion & Handover Certificate / Delivery into Service)

   As each stage (or Gate) is passed an Acceptance Certificate is issued which allows the project to move forward to the next stage. There are a predefined set of deliverables (documents) which must be produced and approved by all relevant stakeholders and this is monitored via Stage Gate review meetings. The diagram below maps key assurance deliverables to the PMF lifecycle.

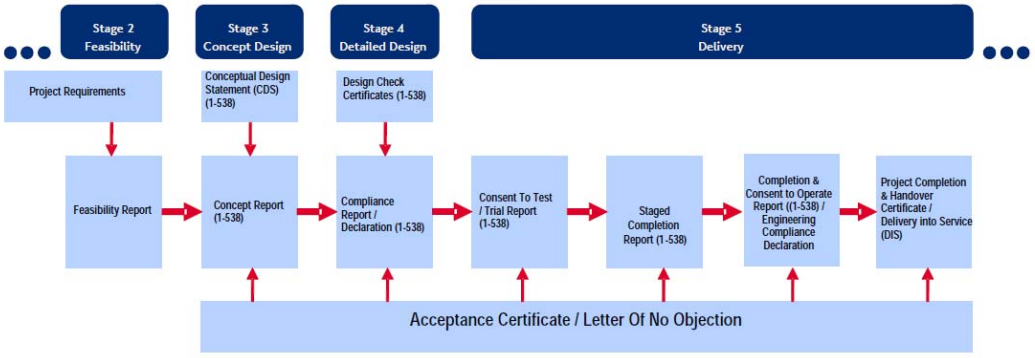


Figure 4 – Key assurance deliverables

Note: the design will typically be based on an option identified and selected in the Feasibility Report which is the output of Stage 2 (Feasibility).

4. Accreditation to provide Assurance
   Another important element of LU's Safety Management System is that Suppliers must be accredited to provide Assurance by the receivers of that assurance evidence. Accreditation means that the Supplier has been assessed by LU and deemed fit to provide assurance. The assessment includes a review of the Suppliers Safety Management System Procedures and the competence of key Engineers whose role is to assess the technical safety of new or altered infrastructure or vehicles. The accreditation of individuals to provide assurance is routinely reviewed by LU to ensure they remain fit to deliver that assurance.

5. LU Verification Activity
   In addition to the Accreditation activity detailed above, in accordance with the ROGS regulations, LU shall determine and document the verification activities to be undertaken by LU to verify the assurance evidence provided by Suppliers. In this regard LU acts as the Independent Competent Person as described in ROGS. The level of verification will be dependent upon what is stated within the Assurance Plan.
   The details of the verification to be undertaken will be documented within a risk-based Verification Activity Plan (VAP) which includes :

   - the activities to be undertaken throughout the lifecycle of the proposed change or contract for service.
   - any evidence detailed in the Suppliers or third party's Assurance plan which will be required to be submitted to LU to assist in verification activity, including any evidence required to support the safety verification activities of LU's Independent Competent Person.
   - any evidence required for LU to grant approval for the Supplier or third party to progress between the project stages.

   An approved VAP shall be in place prior to any design activity.

6. DRACCT
   All projects to which Schedule 4 of ROGS "Written Safety Verification Requirements" applies shall be reviewed by the LU Directors' Risk Assurance and Change Control Team (DRACCT). Assurance Plans, supplier assurance evidence and VAPs for changes, projects or contracts for service that are complex, or pose significant risk shall be referred to LU DRACCT for acceptance. This may include those where the most likely outcome if controls fail is:
   a) One or more fatalities;
   b) Prosecution for failure to comply with legislation;
   c) Significant non-compliance with requirements having either an adverse health and safety or operational impact;
   d) Significant environmental damage, likely to result in enforcement action;
   e) Significant loss of customer benefit;
   f) Significant risk to LU reputation.

Tube Lines Procedure P308 – Assurance of New and Altered Assets

In order to demonstrate how they meet the requirements of LU standard 1-538 and ROGS Regulations, Tube Lines (TL) have produced a procedure which describes how they plan and provide assurance to LU. The evidence which demonstrates how TL achieves the responsibilities of the LU standards and legislation is documented within an Assurance Plan for each Project they deliver. The Assurance Plan (AP) will identify the structure and programme of all assurance submissions needed and how these are approved within Tube Lines (in cases of high risk these are reviewed by TL's Safety Review Group) and those needing LU approval (and therefore submission to the LU DRACCT).

For new or altered assets, Tube Lines has obligations under the Public Private Partnership (PPP) Contract and LU Category 1 Standards to make submissions and to provide evidence of compliance and the necessary controls to LU at defined times. The V-cycle based upon EN 50126 will be used within Tube Lines with regards to asset assurance. Each project will select one or more as appropriate (in consultation with the Asset Engineers (AEs) and LU) and declare the agreed submissions in the AP. In terms of plan delivery the AP needs to cover the key requirements set out in Tube Lines Assurance Regime (a document which is an important part of Tube Lines Safety Management System demonstrating how Tube Lines deliver assurance for all of their activities). In summary the plan must cover:

- How people of the required competence will be deployed internally and in the supply chain, with assessment as necessary if not established by other procedures.
- The defined processes by which the work is enacted.
- How the product is approved, particularly where new or novel equipment is inducted
- How the product is handed over into maintenance
- How the above is verified on a risk basis.

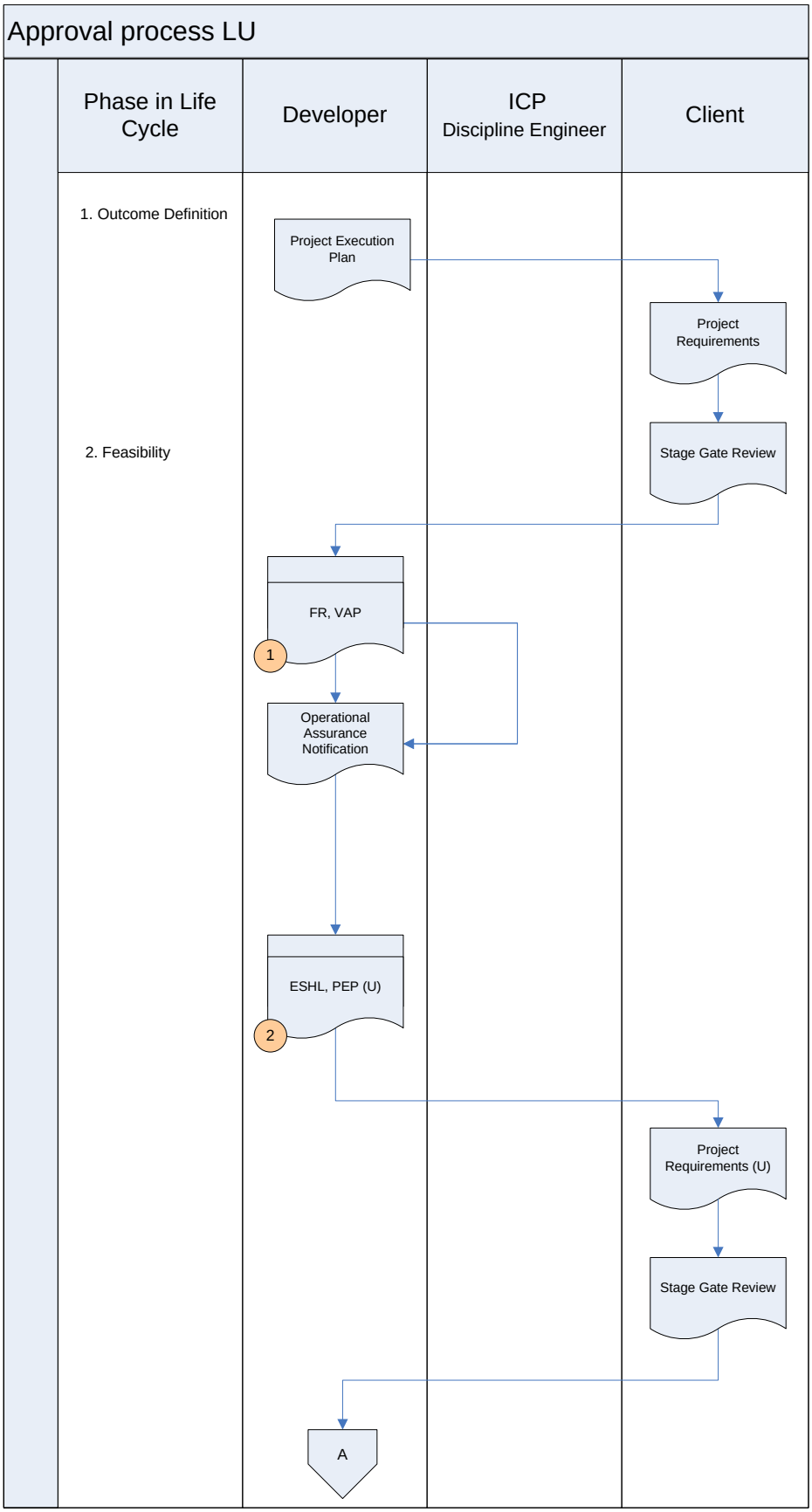
The AP must normally be completed before detailed design commences. It must also be reviewed at defined points (corresponding to key stages, eg, completion of design, prior to testing) to ensure the project controls continue to manage all the risks.

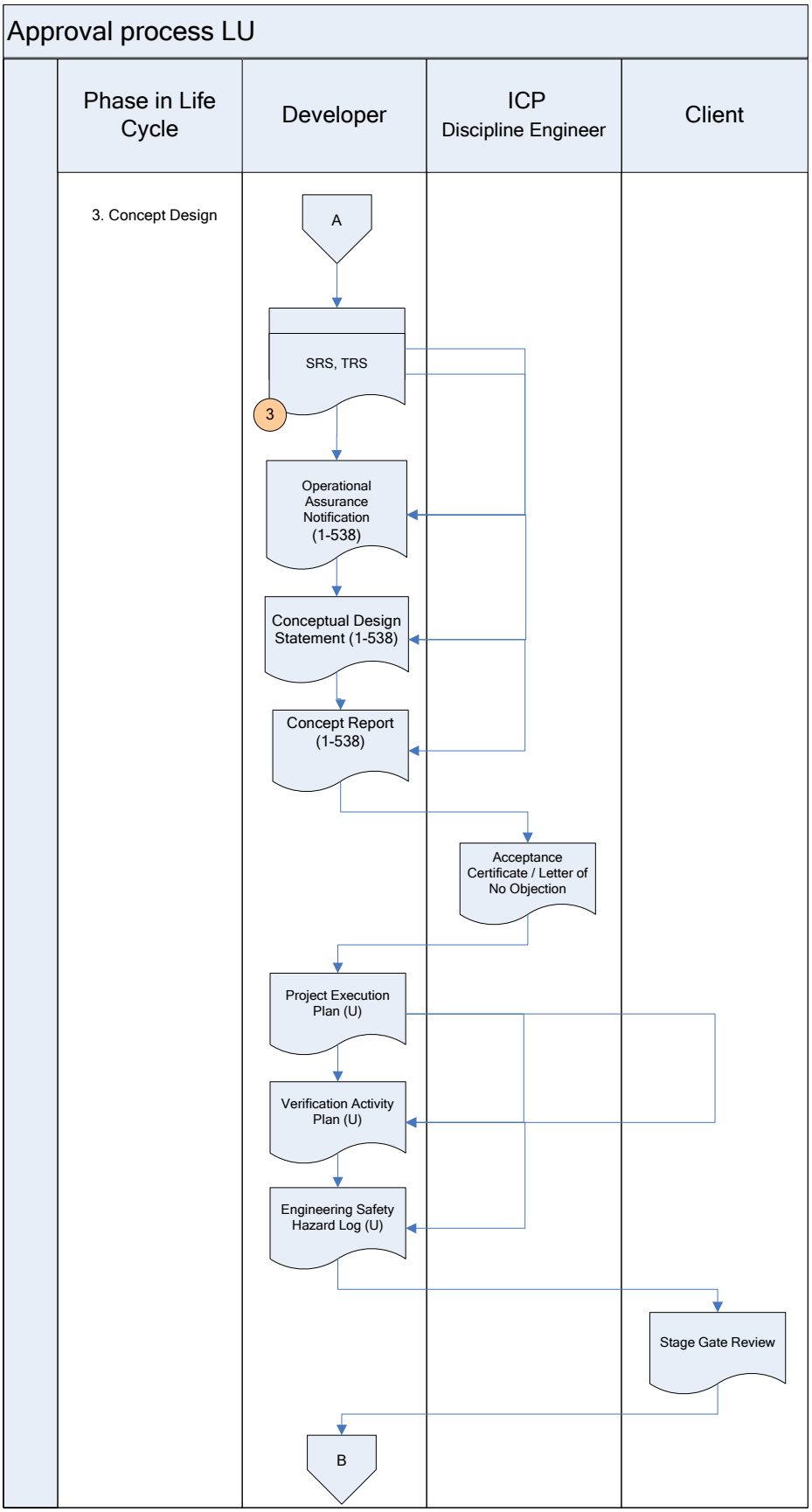
4.4.1.4 Safety Verification Scheme

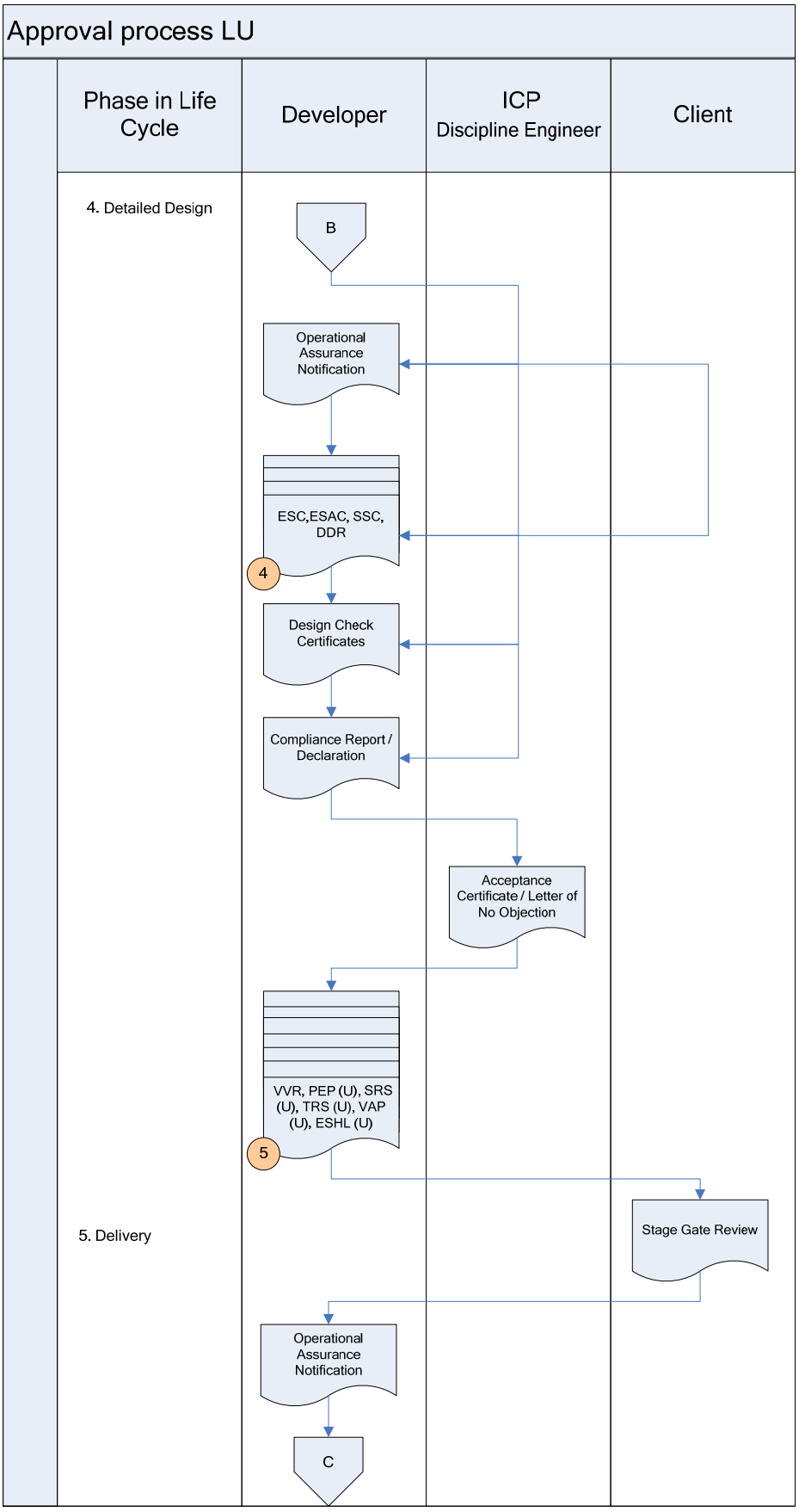
The foundation of the Safety Verification Scheme is the appointment of an Independent Competent Person (ICP). The Transport Operator should devise the scheme taking into consideration the advice of the ICP. The ICP should be involved in the establishment of the verification criteria. Within the PMF process, the ICP role is fulfilled by the Discipline Engineer.
The actual standards and criteria utilised in the verification process should be agreed and recorded to give transparency to the process and provide an audit trail. The governance arrangements for making changes to the verification scheme should be recorded and where any changes are made they too should be recorded. The retention of a written record of the verification undertaken is an essential part of the process. The records should be retained for the life of the subject of the verification scheme. To ensure effective governance of the safety verification process the key information should be communicated to the appropriate management level. An appropriate level is that with sufficient authority to ensure that any action required in relation to the safety verification is taken.

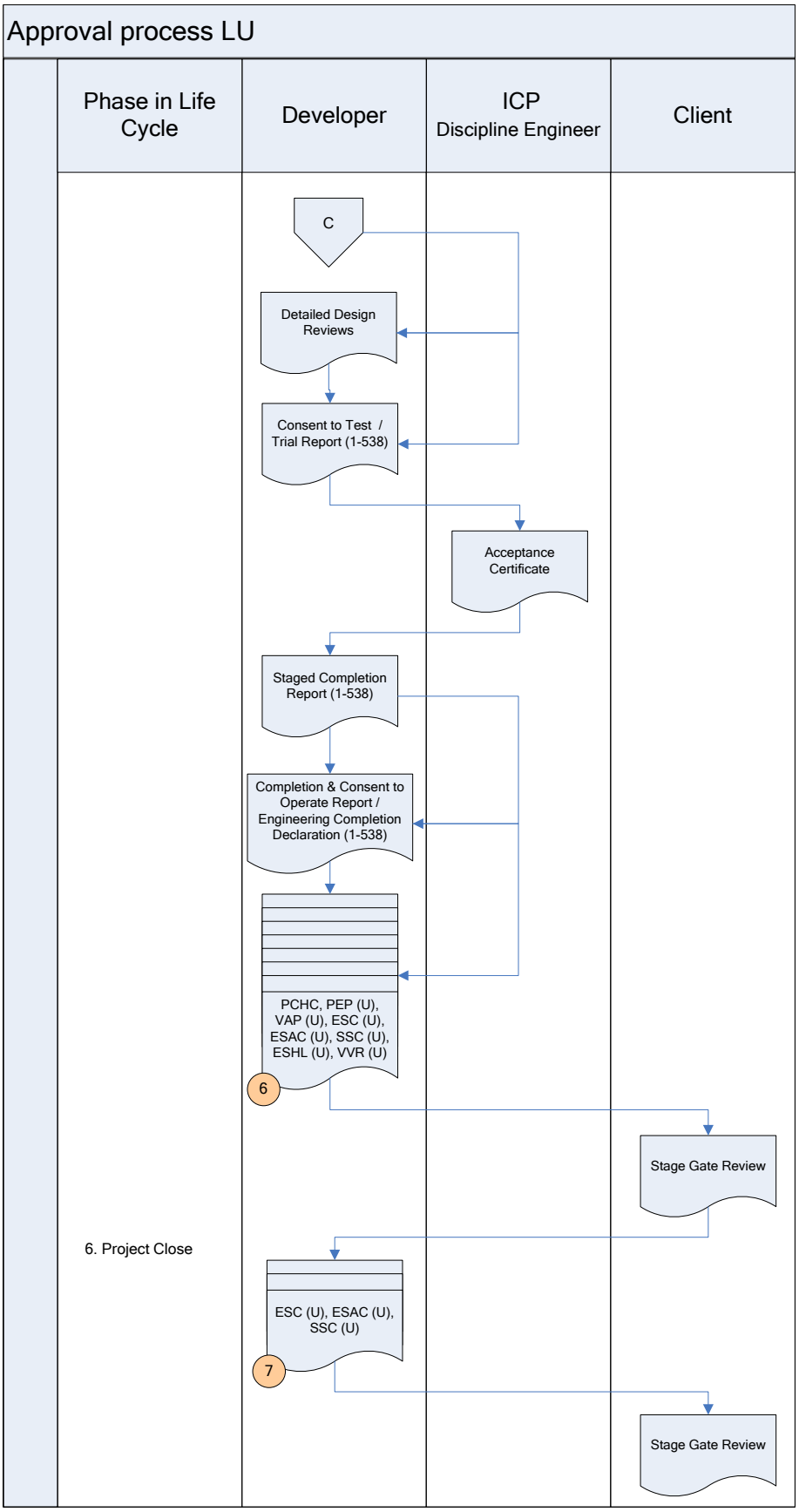
4.4.2 Approval Process London Underground

The process is based upon UK legislation and corporate procedures. The main steps and the participants of the approval, acceptance and certification procedure are demonstrated on a flowchart diagram (see next pages). Updated products are marked with (U).


Approval process LU
Phase in Life Cycle
Developer
ICP
Discipline Engineer
Client
1. Outcome Definition
2. Feasibility
Project Execution Plan
Project Requirements
Stage Gate Review
FR, VAP
1
Operational Assurance Notification
ESHL, PEP (U)
2
Project Requirements (U)
Stage Gate Review
A


Approval process LU
Phase in Life Cycle
Developer
ICP
Discipline Engineer
Client
3. Concept Design
A
SRS, TRS
3
Operational Assurance Notification (1-538)
Conceptual Design Statement (1-538)
Concept Report (1-538)
Acceptance Certificate / Letter of No Objection
Project Execution Plan (U)
Verification Activity Plan (U)
Engineering Safety Hazard Log (U)
Stage Gate Review
B


Approval process LU
Phase in Life Cycle
Developer
ICP
Discipline Engineer
Client
4. Detailed Design
B
Operational Assurance Notification
ESC,ESAC, SSC, DDR
4
Design Check Certificates
Compliance Report / Declaration
Acceptance Certificate / Letter of No Objection
VVR, PEP (U), SRS (U), TRS (U), VAP (U), ESHL (U)
5
5. Delivery
Stage Gate Review
Operational Assurance Notification
C


Approval process LU
Phase in Life Cycle
Developer
ICP
Discipline Engineer
Client
C
Detailed Design Reviews
Consent to Test / Trial Report (1-538)
Acceptance Certificate
Staged Completion Report (1-538)
Completion & Consent to Operate Report / Engineering Completion Declaration (1-538)
PCHC, PEP (U), VAP (U), ESC (U), ESAC (U), SSC (U), ESHL (U), VVR (U)
6
Stage Gate Review
6. Project Close
ESC (U), ESAC (U), SSC (U)
7
Stage Gate Review

Acronyms regarding Approval Process LU flowchart:

1. Feasibility Report and Verification Activity Plan
2. Engineering Safety Hazard Log, Project Execution Plan
3. System Requirements Specification, Technical Requirements Specification
4. Engineering Safety Case, Engineering Safety & Assurance Case, System Safety Case, Detailed Design Reviews
5. Verification and Validation Report, Project Execution Plan (U), System Requirements Specification (U), Technical Requirements Specification (U), Verification Activity Plan (U), Engineering Safety Hazard Log (U)
6. Project Completion & Handover Certificate / Delivery into Service, Project Execution Plan (U), Verification Activity Plan (U), Engineering Safety Case (U), Engineering Safety & Assurance Case (U), System Safety Case (U), Engineering Safety Hazard Log (U), Verification and Validation Report (U), Engineering Safety Case (U), Engineering Safety & Assurance Case (U), System Safety Case (U)

4.5 Case “Sweden”

A vehicle for rail traffic must be approved by the Swedish Transport Agency before it is allowed to be used in Sweden. This applies to new, imported and significantly modified vehicles. Likewise, a new or significantly remodelled track installation or technical system must be approved before it can be taken into service. This is laid down in the Railway Act 2004:519. Station names and training plans also require approval (refer to [Transportstyrelsen]).

Note, that in Sweden the rail approval process is covering all rail systems, including urban ones.

JvSFS 2006:1 governs what information forms the basis for approval by the Swedish Transport Agency and when this information must be submitted to the Technical Unit of the Swedish Transport Agency, Department of Railway (refer to [Transportstyrelsen] and [JvSFS2006:1]).

This guide is intended to assist applicants when reading the regulation JvSFS 2006:1 “Järnvägsstyrelsens föreskrift om godkännande av delsystem m.m.” (The regulations of the Swedish Rail Agency on the approval of subsystems in railways, etc.). The term “subsystem” refers to distinct parts of the railway system, such as vehicle, technical system and railway infrastructure (refer to [Transportstyrelsen]).

4.5.1 General Information

The approval of the Swedish Transport Agency is required before infrastructure, vehicles or technical systems can be put into service. This also applies to upgrading or renewal of an already approved subsystem, where safety is affected. Station names and education plans also require an approval before they are used (refer to [Transportstyrelsen]).

Projects not covered by TSIs are based entirely on national rules. No notified body is involved in the approval process; instead, the Swedish Rail Agency’s operatives have the equivalent role of monitoring safety control from the start of the project until commissioning (refer to [TS JV 2009:002], sub-clause 5.1).

4.5.2 Approval Process

1) Contacting the Swedish Rail Agency

Contacting the Swedish Rail Agency at an early stage enables the Agency to provide information about current legislation, regulations and official requirements, even in adjacent areas such as the environment, health and safety and electrical safety. If the application relates to the approval of a vehicle, the applicant should also contact the infrastructure manager. The Swedish Rail Agency and the applicant should conduct a running dialogue during the course of the project (refer to [TS JV 2009:002], sub-clause 1.5.1).

2) The Operator applies for Certification at the Swedish Rail Agency

If several parties are involved, the applicant assumes a coordinating role with respect to the Swedish Rail Agency. Before applying for approval, the applying parties should agree who will stand as the applicant (refer to [TS JV 2009:002], sub-clause 5.6.1)

The applicant may submit an application with the aid of this guide and using the forms in the appendices. The submitted documentation may be more or less detailed, depending on the complexity of the system. In certain cases, the content of the document required by the Swedish Rail Agency can be considerably simplified (refer to [TS JV 2009:002], sub-clause 1.5).

Applicants may be the inventor or purchasers of a vehicle, infrastructure or technical system, for instance a railway undertaking, a manufacturer or an infrastructure manager (refer to [TS JV 2009:002], sub-clause 1.3).

In the case of upgrading and renewal, an application must be submitted in the same way as for new constructions if the nature of the activity is such that approval is required (i.e. if the change affects safety). As far as possible, the information on which the Swedish Rail Agency bases its approval must be limited to the actual change, but the change must be described in relation to the whole, so that the context can be understood (refer to [TS JV 2009:002], sub-clause 1.7).

Depending on the system, the times for handing in the requested application documents varies along the approval process. First documents are expected with the start of the design, the last documents are necessary for permanent approval.

3) Involvement of an Independent Safety Assessor (refer to [TS JV 2009:002], sub-clause 5.5).

For projects with a major safety impact, the Swedish Rail Agency requires applicants to engage an assessor. The assessor must be a third party, independent of the group developing and reviewing the system. It is assumed that the assessor has far-reaching expertise in the field of safety-critical designs. The role of the assessor is, among other things, to review the development of the system and the work that is done by different key individuals (who have had responsibility for safety-related tasks).

One of the most important tools for the assessor is the “safety case” according to SS-EN 50129:2003. The documentation of a project and a system (the safety case) must be complete. It must not be necessary to have been involved in a project to know why something is the way it is.

The assessor should preferably be engaged early in the process. The assessor and the applicant may work together interactively, so that the assessor can give feedback on the prepared documentation. In this way, the assessor can point out any shortcomings at an early stage, without actually suggesting solutions (refer to [TS JV 2009:002], sub-clause 5.5).

4) The Swedish Rail Agency checks that the safety requirements laid down in Sections 1-5 of the Railway Act (2004:519) are met

The Swedish Rail Agency has different grounds for assessment depending on the technical and safety-related scope of the system. This has an indirect effect on the requirements imposed by the Swedish Rail Agency as regards documentation of the safety of the system. For this reason, the Swedish Rail Agency has divided the required information into two sections: *information that is always required* and *information that is required where the system has a major effect on safety* (refer to [TS JV 2009:002], sub-clause 5.2)

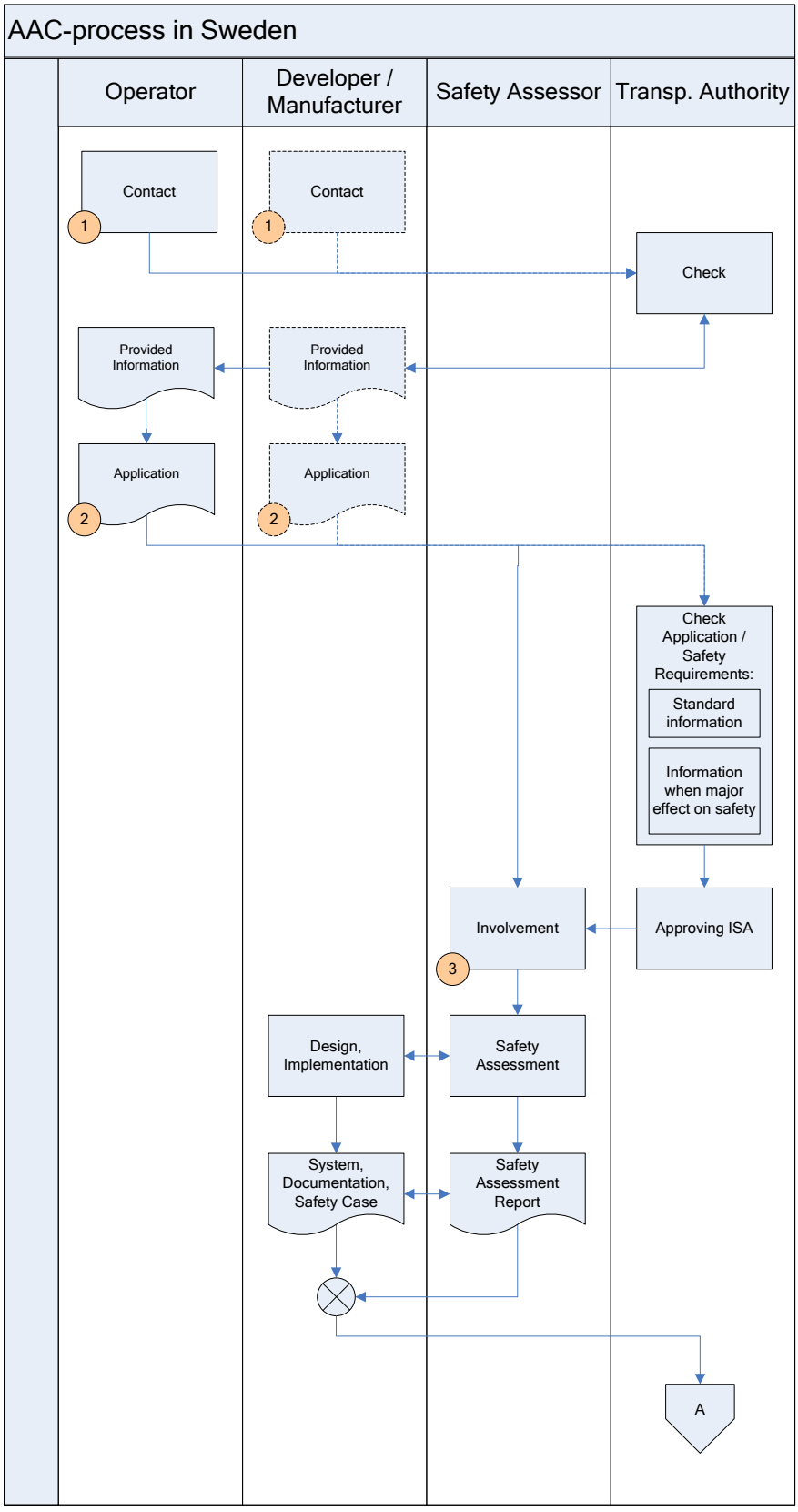
The fundamental safety requirements according to the Railway Act state that it is the **railway undertaking who is responsible** for ensuring that the standard of traffic safety of every subsystem is sufficiently high (refer to [TS JV 2009:002], sub-clause 5.1).

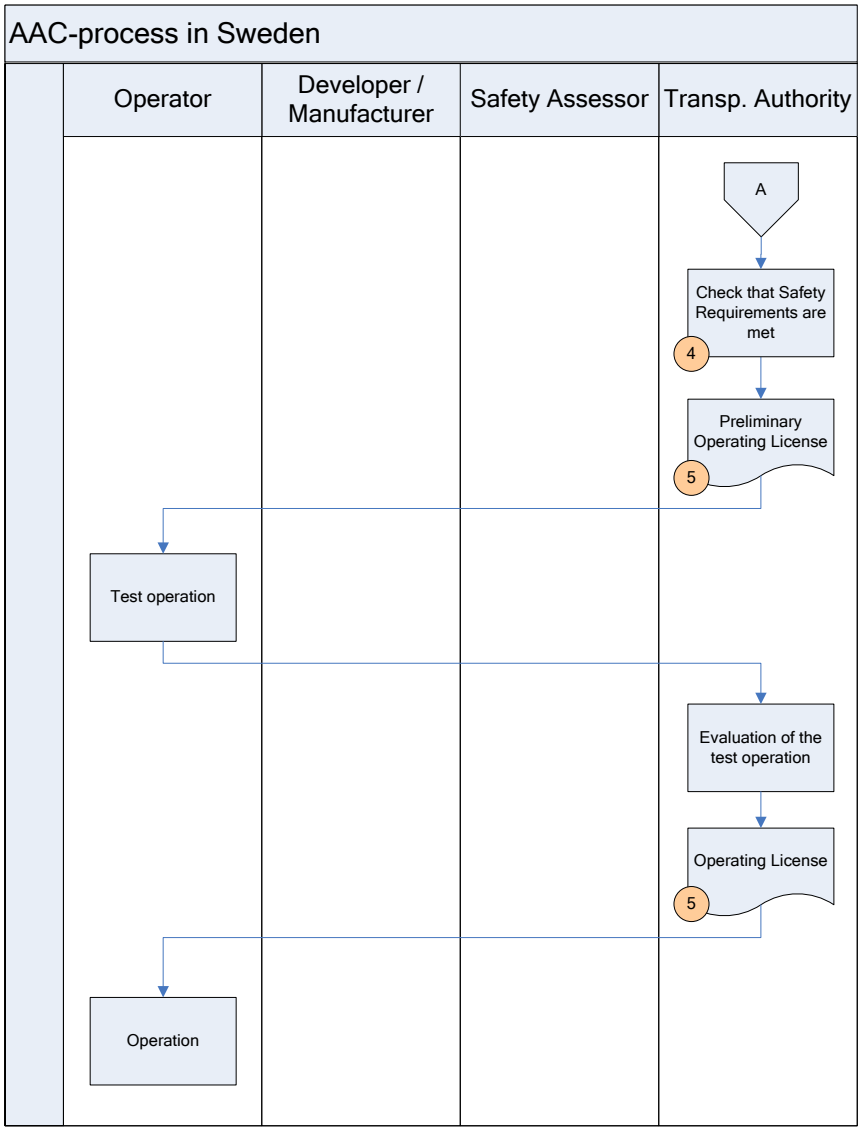
5) Time-limited and permanent approval

The Swedish Rail Agency often grants approval in two stages, first a time-limited approval in order to conduct trial operation or to gain experience with operation of the vehicle, and then permanent approval. Time-limited approval may also include restrictions and conditions on use (refer to [TS JV 2009:002], sub-clause 1.9).

When trial operation or operation to gain experience has been conducted and the result is approved and documented, the Swedish Rail Agency can give permanent approval (refer to [TS JV 2009:002], sub-clause 5.6.4).

4.5.3 Description of procedure




AAC-process in Sweden
Operator
Developer / Manufacturer
Safety Assessor
Transp. Authority
A
Check that Safety Requirements are met
4
Preliminary Operating License
5
Test operation
Evaluation of the test operation
Operating License
5
Operation

5 Identification of Elementary Activity Modules

After the analysis and comparison of the processes, described in detail in the case studies similar activities can be found. These are the activities that are defined as Elementary Activity Modules. These are elementary parts of the processes.

In this chapter the common activities of these processes are identified. These activities can be organised according to different views:

- hierarchy of the system, i.e. system level, level of functionality and safety;
- timeline of the life cycle.

According to the timeline similar activities can be identified:

- definition of requirements,
- check of requirements,
- demonstration of fulfilment of requirements and
- check of fulfilment of requirements.

This sequence of activities can be found at system level, functional level and safety level, with slight differences:

- The act of approval is an important elementary activity module, and it can be interpreted mainly at system level. Therefore it is discussed in sub-clause 5.1.
- The activity of safety assessment is a parallel activity, which is linked mainly to the safety level, therefore it is discussed in sub-clause 5.3.

Note that the wording used to define these activities is consciously different from the wording of CENELEC standards. This is to help to keep independency from the wording of description of existing AAC procedures.

In the following sub-clauses the elementary activity modules is discussed according to different system hierarchy levels. Following this, the link between MODSafe life cycle phases (as described in [MODSafe D6.3]) and the identified EAMs are described.

5.1 System level

The following activities can be defined with respect to system functionality:

- Definition of system requirements
- Check of system requirements
- Demonstration of fulfilment of system requirements, test operation
- Check of fulfilment of system requirements
- Approval

These activities are described in the following sub-clauses. For each activity the most relevant inputs and outputs are also demonstrated.

5.1.1 Definition of system requirements

The definition of system requirements does not belong strictly to the acceptance, approval and certification but clearly these are the basis for these activities, as they all include some examination of fulfilment of some requirements. The main input for the definition of system requirements is the system concept and the output is the system requirements specification.

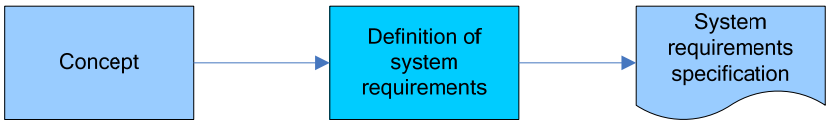


Figure 5 – Definition of system requirements

5.1.2 Check of system requirements

System requirements are checked at least by the operator, but independent organisations, or even the authority may check the system requirements.

The input for this EAM is the system requirement specification, the output is some type of consent, but in some cases remarks and suggestions may be done also.

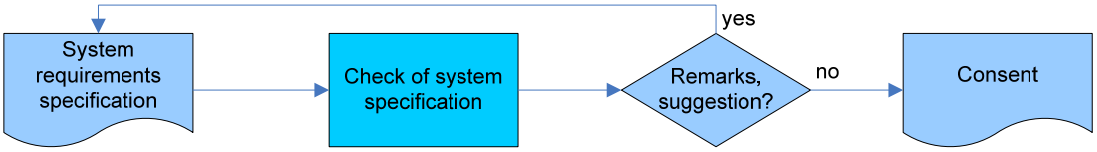


Figure 6 – Check of system requirements

5.1.3 Demonstration of fulfilment of system requirements, test operation

The developer or supplier of a system has the task to demonstrate, that the system fulfils its requirements. From the other hand, the operator has also sometimes the task to demonstrate the fulfilment of system requirements e.g. to obtain approval from an authority. The input for this activity is the system specification and the design or the implementation of the system, tests results etc. For test purposes the normal operation of a rail system is often preceded by a test operation. The test operation can be various with respect to functionality, place, period etc. The inputs for the test operation are the system itself with the implementation plans. The test operation results in the evaluation of test operation. The test operation can be identified as an EAM too.

The test evaluation report can be used as an input for the demonstration of the fulfilment of system requirements.

The output can be various, can be e.g. a part of the safety case, but other types of documentation are also possible.

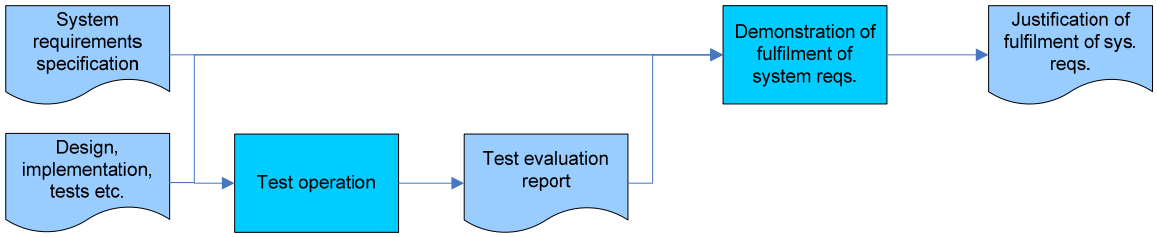


Figure 7 – Demonstration of fulfilment of system requirements

5.1.4 Check of fulfilment of system requirements

The developer's or supplier's demonstration is generally followed by a check of fulfilment of system requirements by another party or other parties. Clearly, the operator, the user of the system checks the fulfilment of system requirements, but often the authority also checks it, and in some cases the assessor also can have such a task.

For this EAM the functional requirements and the developer's justification is a clear input, but additional tests, analyses and examinations can also be carried out. The output can be various, according to the person or organisation, who carries out this check.

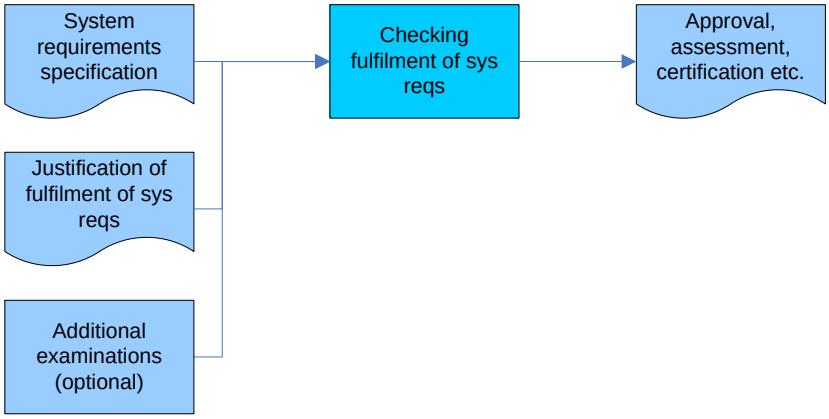


Figure 8 – Checking of fulfilment of system requirements

The fulfilment of system requirements is clearly a pre-requisite for the final consent to putting a system into operation. So the output of this EAM can be in some cases the Approval.

5.1.5 Approval

All of the processes are closed by a final act, a final decision or permission to put the system into service. According to the definitions of D7.1, this act is called approval.

Figure 9 – Approval

5.2 Activities at functional level

The following activities can be defined with respect to system functionality:

- Definition of functional requirements
- Check of functional requirements
- Demonstration of fulfilment of functional requirements
- Check of fulfilment of functional requirements

These activities are described in the following sub-clauses. For each activity the most relevant inputs and outputs are also demonstrated.

5.2.1 Definition of functional requirements

The definition of functional requirements does not belong strictly to the acceptance, approval and certification but clearly these are the basis for these activities, as they all include some examination of fulfilment of some requirements. The main input for the definition of functional requirements is the system requirements and the output is the specification of functional requirements.

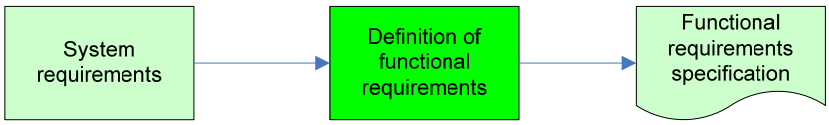


Figure 10 – Definition of functional requirements

5.2.2 Check of functional requirements

Functional requirements are often checked in UGT-systems by an independent organisation, such as an authority (see e.g. Hungary), however this is not always the case. The aim of checking of the functional requirements is to maintain the functional safety of the UGT system.

The input for this EAM is the functional requirement specification, the output is some type of consent, but in some cases remarks and suggestions may be done also.

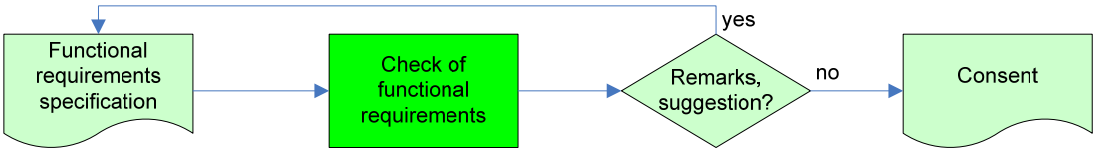


Figure 11 – Check of functional requirements

5.2.3 Demonstration of fulfilment of functional requirements

Almost without exception, the developer or supplier of a system has the task to demonstrate, that the system fulfils the functional requirements. The input for this activity is the functional requirement specification and the design or the implementation of the system, tests results etc. The output can be various, can be e.g. a part of the safety case, but other types of documentation is also possible.

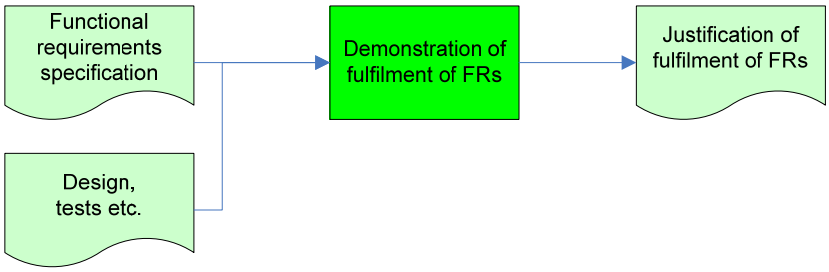


Figure 12 – Demonstration of fulfilment of functional requirements

5.2.4 Check of fulfilment of functional requirements

The developer's or supplier's demonstration is generally followed by a check of fulfilment of functional requirements by another party or parties. Clearly, the Operator (user of the system) checks the fulfilment of functional requirements, but often the authority also checks it, and in some cases the assessor also can have such a task. For this EAM the functional requirements and the developer's justification are clear inputs, but additional tests analyses and examinations can also be carried out. The output can be various, according to the person or organisation, who carries out this check.

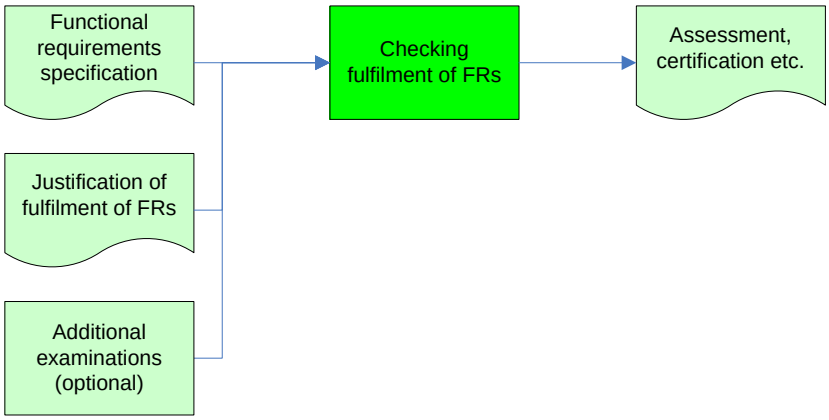


Figure 13 – Checking of fulfilment of functional requirements

5.3 Activities at safety level

The following activities can be defined with respect to system safety:

- Definition of safety requirements
- Check of safety requirements
- Demonstration of fulfilment of safety requirements
- Check of fulfilment of safety requirements
- Independent safety assessment

Under safety requirements two kinds of requirements can be understood. On one hand safety requirements include those functional requirements, which functions are safety relevant (e.g. occupancy detection). On the other hand the safety requirements include non-functional requirements, such as safety integrity requirements. Clearly, safety integrity requirements are closely linked to safety functions, as safety integrity requirements are

defined as a result of risk analysis of safety functions.

The safety level activities are described in the following sub-clauses. For each activity the most relevant inputs and outputs are also demonstrated.

5.3.1 Definition of safety requirements

The definition of the safety requirements is based on the functional requirements and on a hazard and risk analysis. The result of the activity is the safety requirement specification.

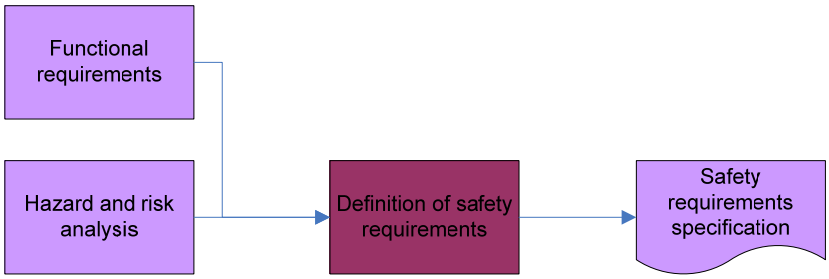


Figure 14 – Definition of safety requirements

5.3.2 Check of safety requirements

Similarly to functional requirements, the safety requirements are also checked in some cases by third parties (i.e. independently from the supplier and the operator).

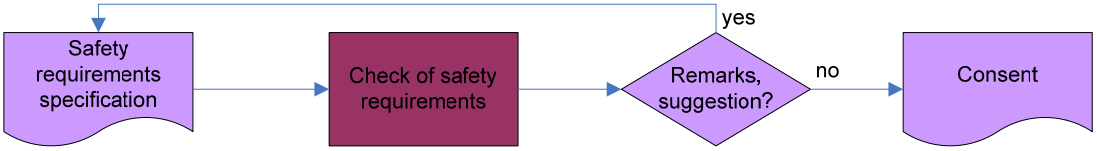


Figure 15 – Check of safety requirements

5.3.3 Demonstration of fulfilment of safety requirements

The supplier of the system has to demonstrate that the safety requirements of the supplied system are met. The input for this activity is the safety requirement specification and of course the system itself, with designs, analysis etc. The demonstration typically results in a safety case or similar document.

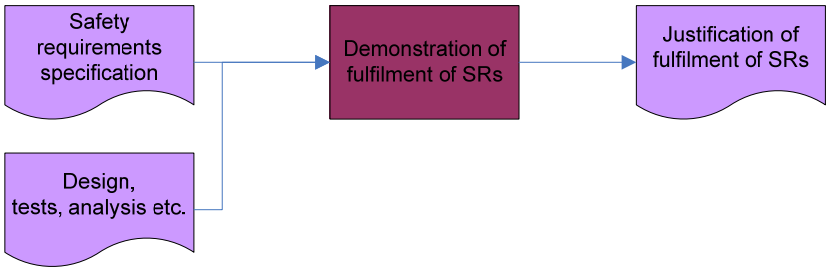


Figure 16 – Demonstration of fulfilment of safety requirements

5.3.4 Check of fulfilment of safety requirements

The independent check of fulfilment of safety requirements is more characteristic than that of functional requirements, but various organisations can provide this EAM. The result of this activity can be typically an assessment or certification.

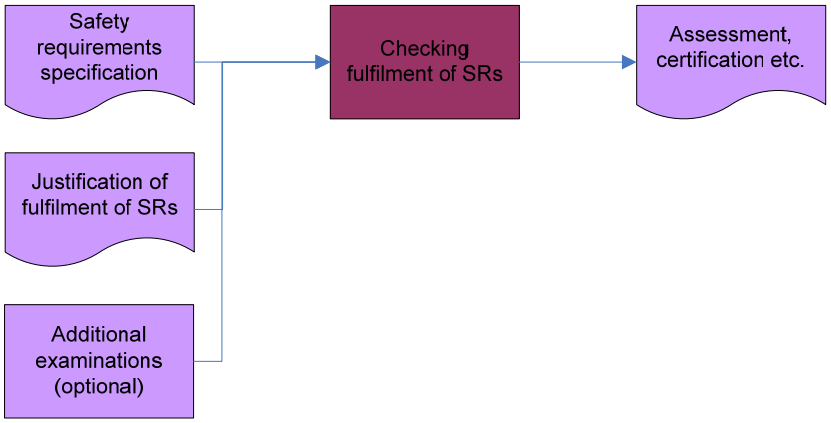


Figure 17 – Check of demonstration of safety requirements

5.3.5 Independent Safety Assessment

Independent Safety Assessment can provide various activities in the approval, acceptance and certification processes. In some cases the assessment includes only safety aspects in other cases both functional and safety aspects. The examinations can be a part of the functional examination of the system or the part of the safety examination of the system. However the independency of assessment plays here an important role, therefore safety assessment was defined as an EAM. The inputs and outputs can be various, according to the contents of the assessment.

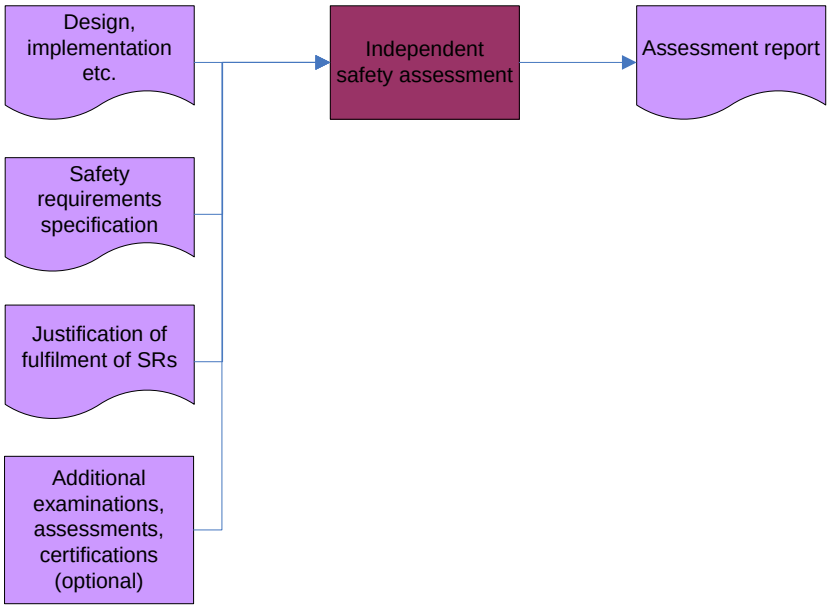


Figure 18 – Safety assessment

A more detailed view on safety assessment activities is done in later phases of this work package.

5.4 Link of EAMs to MODSafe life cycle phases

In [MODSafe D6.3] the following life cycle was proposed. In this sub-clause the link between the Elementary Activity Modules and specific life cycle phases are described.

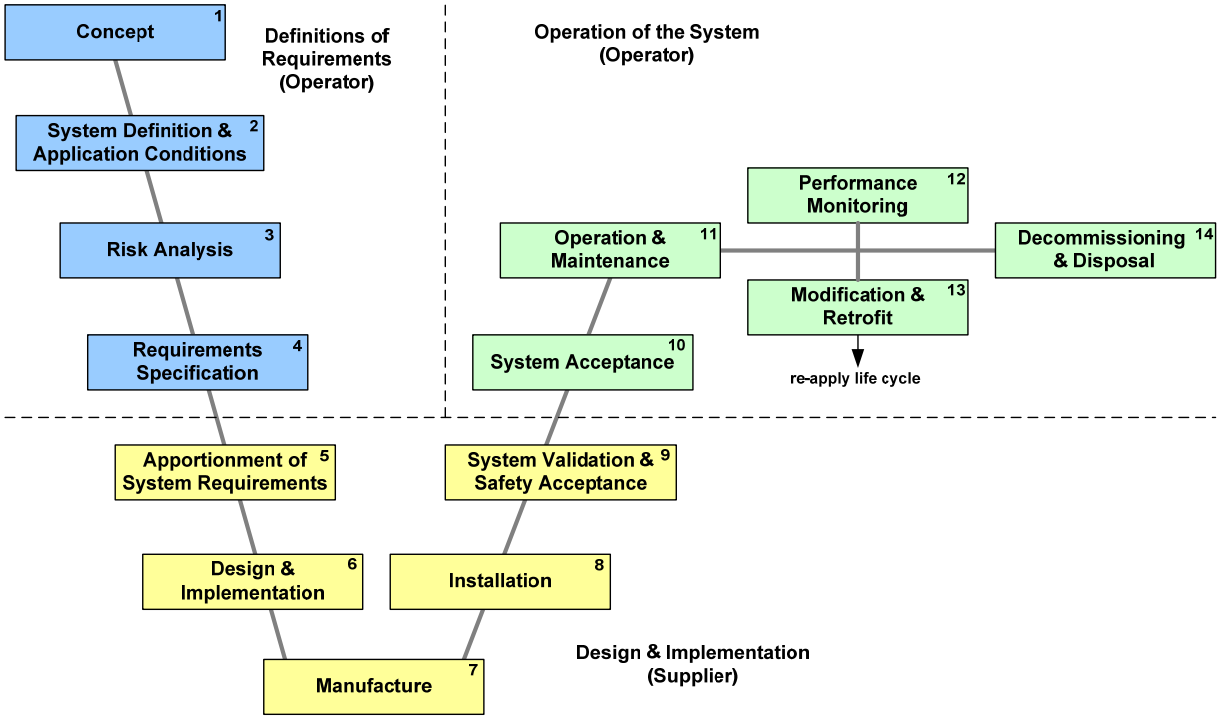


Figure 19 – Common Life Cycle Approach Proposal [MODSafe D6.3]

In the previous sub-clauses the following EAMs were identified:

- System level
  - Definition of system requirements
  - Check of system requirements
  - Demonstration of fulfilment of system requirements, test operation
  - Check of fulfilment of system requirements
  - Approval
- Functional level
  - Definition of functional requirements
  - Check of functional requirements
  - Demonstration of fulfilment of functional requirements
  - Check of fulfilment of functional requirements
- Safety level
  - Definition of safety requirements
  - Check of safety requirements
  - Demonstration of fulfilment of safety requirements
  - Check of fulfilment of safety requirements
  - Independent safety assessment

The following table lists the life cycle phases proposed in [MODSafe D6.3] and adds the elementary activity modules that are performed at that stage. The CENELEC life cycle as the source of the MODSafe life cycle does not specify acceptance, approval and certification activities. Therefore not all life cycle phases can be linked with an EAM, and conversely more than one EAM can be performed during a phase.

No. of Life Cycle phase	Name of Life Cycle phase	Performed EAMs
1	Concept	
2	System Definition & Application Conditions	Definition of system requirements Check of system requirements (this EAM can be interpreted as the verification of this life cycle phase)
3	Risk Analysis	
4	Requirements specification	Definition of functional requirements Check of FR Definition of safety requirements Check of SR
5	Apportionment of System Requirements	
6	Design & Implementation	
7	Manufacture	Demonstration of fulfilment of SR Demonstration of fulfilment of FR
8	Installation	Demo. of fulfilment of sys reqs/ test operation (at the end of the life cycle phase)

No. of Life Cycle phase	Name of Life Cycle phase	Performed EAMs
9	System Validation & Safety Acceptance	Check of fulfilment of SR Check of fulfilment of FR Check of fulfilment system req.
10	System Acceptance	Approval (at the end of the life cycle phase)
11	Operation & Maintenance	
12	Performance Monitoring	
13	Modification & Retrofit	
14	Decommissioning & Disposal	

Figure 20 – List of EAMs to life cycle phases

The EAM “Safety assessment” is a parallel activity, which is performed from phase 3 up to phase 11, as described in [MODSafe D6.3, sub-clause 5.10.2].

5.5 List of elementary activity modules

In the previous sub-clauses the elementary activity modules were identified for different levels of hierarchy. In the following figure the horizontal and vertical organisation of the EAMs is demonstrated, according to the two main parameters: hierarchy and life cycle timeline.

This depiction allows to demonstrate the horizontal connection of the EAMs: the functional requirements are derived from system requirements, while safety requirements are derived from functional requirements. Similarly, the demonstration of fulfilment of system requirements encapsulate the demonstration of fulfilment of functional requirements and safety requirements.

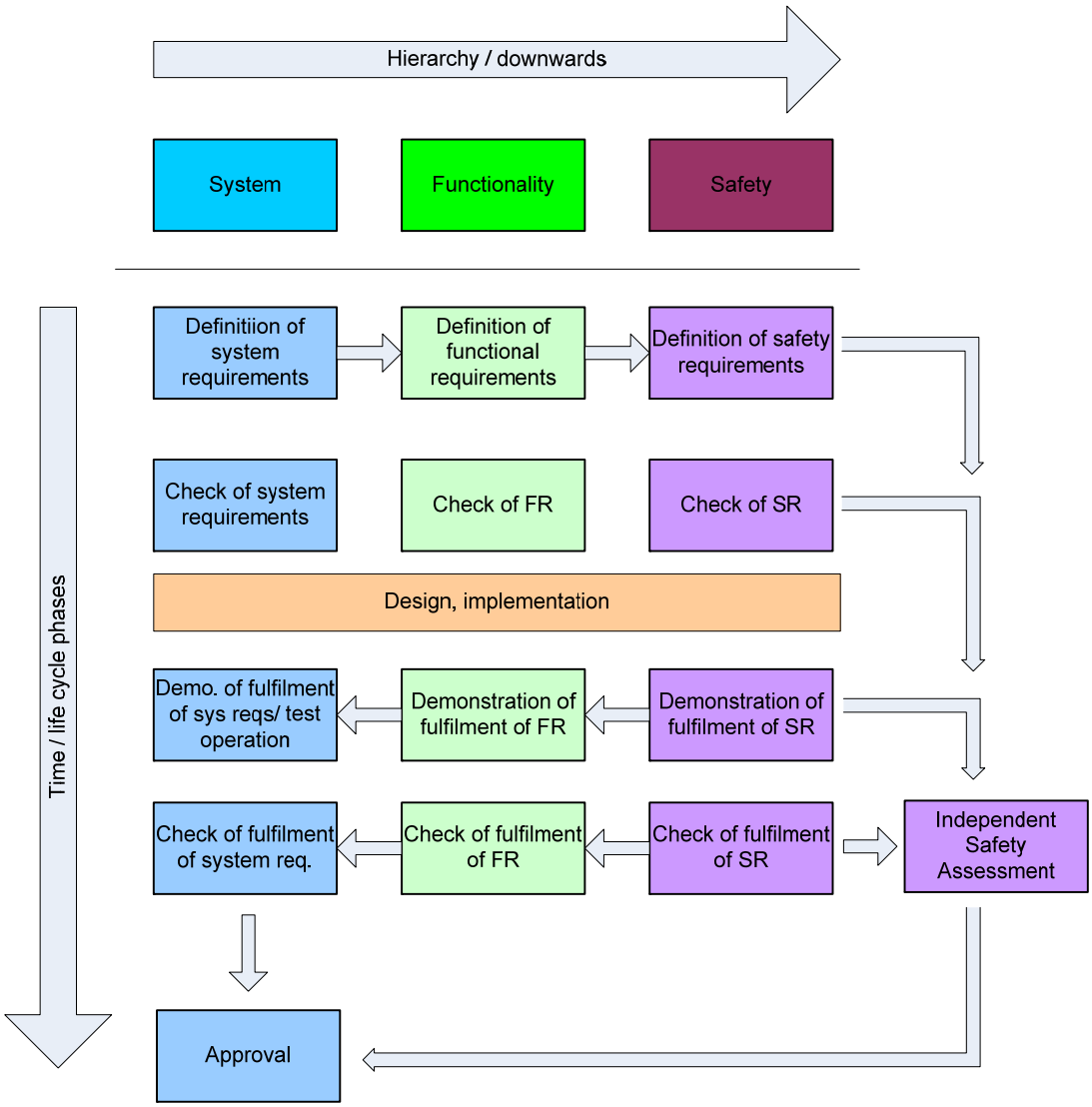


Figure 21 – System of EAMs

6 Conclusion and further work

In this deliverable the so-called elementary activity modules were identified, based on the analyses of detailed case studies. The elementary activity modules are listed and summarised in sub-clause 5.5.

In later phases of this work package these elementary parts of the process are used to describe the task of different parties involved in the acceptance, approval and certification processes, furthermore to establish a generic, optimised process.

In MODSafe deliverable D7.3 a generic model of acceptance, approval and certification processes is presented from different views, like process at different levels of system hierarchy, roles and responsibilities of parties, typical, generic processes of different participants, with the help of EAMs.

MODSafe deliverable D7.4 focuses on optimisation issues, possible reduces of efforts in acceptance, approval and certification procedures.