SEVENTH FRAMEWORK PROGRAMME

MODSafe

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

Acceptance, Approval, Certification

Typical AAC model

Deliverable No.D7.3

Contract No.	218606
Document type	DEL
Version	V1.0
Status	Final
Date	23-04-2012
WP	WP 7
Lead Author	Balázs Sághi BME
Contributors	TRIT, RATP, INRETS, LU, R&B, UITP, UTC
Description	Deliverable D7.3 Version 1.0
Document ID	DEL_D7.3_BME_WP7_230412_V1.0
Dissemination level	PU
Distribution	Consortium

Document History:

Version	Date	Author	Modification [*very short description]*
V0.1	28-01-2011	Balázs Sághi	New document: global structure
V0.2	03-05-2011	Balázs Sághi	Reworked after WP10 comments
V0.3	15-08-2011	Balázs Sághi	First draft with contents
V0.4	28-11-2011	Balázs Sághi	Reworked after WP7 comments
V0.5	18-01-2012	Balázs Sághi	Modified according to review comments and WP meeting
V0.6	08-02-2012	Balázs Sághi	Modified according to review comments
V0.7	02-03-2012	Balázs Sághi	Modified after WP7 meeting for WP10 review
V0.8	29-03-2012	Balázs Sághi	Modified according to WP10 review
V1.0	23-04-2012	Balázs Sághi	Final version for submission

Approval:

Authority	Name/Partner	Date
WP responsible	BME / WP7 Approval	02-03-2012
EB members	WP 10 Approval	09-04-2012
Coordinator	TRIT	23-04-2012

SEVENTH FRAMEWORK PROGRAMME

Table of Contents

List of Figures

List of Tables

1 Introduction

In Europe, Light Rail, Metros and Trams are characterized by a diversified landscape of safety requirements, safety models, roles and responsibilities, schemes for safety acceptance and approval; however, there are convergences between some architectures and systems, [MODUrban D93].

There are currently no standardised procedures at the European level for bringing Urban Guided Transport into service. There are no common standard procedures in Europe for safety evaluation (each country applies its own safety conformity assessment). Recent applications have been increasingly assessed by taking into account the European standards EN 50126/50128/50129, [CENELEC].

Most Urban Guided Transport stakeholders believe that the development of European (and even worldwide) standards should be encouraged, in order to facilitate the voluntary reference to such standards by relevant national authorities and the various stakeholders, [MODUrban D93].

The European Commission is favouring this approach, notably through its support of major European research projects such as the MODSafe project.

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 national or local obligation for certification at all. However according to [MODURBAN D93] some synergies can be observed in this field.

This work package focuses on one hand on Metros, Light Rail Systems, and Trams, covering the whole transportation system including all sub-systems, e.g. signalling system or rolling stock. Heavy rail and urban commuter trains like “S-Bahn” in Germany or SNCF “RER” in France are not within the focus.

The work package 7 focuses on the other hand on acceptance, approval and certification, i.e. it deals with activities, the sequence of which is closed by putting into service. Regulatory and supervisory activities *after* putting into service are not in the scope of this work package. These activities are however are important to ensure safe operation and are discussed within work package 6. Under authority in this deliverable always a *safety* authority is meant, the function of which is to certify that a safety-related system is fit for service and complies with relevant statutory and regulatory safety requirements, according to EN 50129 [CENELEC]. The term *supervisory* authority refers to a body entrusted with the tasks regarding supervision of the operation and maintenance of urban guided transport systems (i.e. with tasks *after* putting into service). The supervisory authority and the safety authority is often the same organisation, but e.g. in the UK, at London Underground these are separated: the Safety Authority is within the organisation of London Underground, and a supervisory authority (called Rail Regulator) is an independent organisation

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 (operators, suppliers 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 model a typical AAC procedure. During the modelling, the so-called elementary activity modules are used, which were identified and listed in [MODSafe D7.2].

1.1 References

Reference-ID	Document title, identifier and version
[CENELEC]]	EN 50126:2000 "Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)" EN 50128:2011 “Railway applications - Communications, signalling and processing systems - Software for railway control and protection systems" EN 50129:2003 “Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling”
[MODSafe D6.3]	MODSafe Deliverable D6.3 v1.0 Proposal of a common safety life cycle approach
[MODSafe D7.1]	MODSafe Deliverable D7.1 v1.0 Survey of Current AAC procedures
[MODSafe D7.2]	MODSafe Deliverable D7.2 v1.0 List of elementary activity modules
[MODUrban D93]	MODUrban Deliverable Report – D93 Revision 2 Conformity Assessment, Guidelines for Functional and Technical Specifications
[Glossary.en]	MODSafe Glossary - Deliverable No. D10.5
[EN ISO/IEC 17020]	EN ISO/IEC 17020:2004 General criteria for the operation of various types of bodies performing inspection
[EN 45011]	EN 45011:2008 General requirements for bodies operating product certification systems
[IRSE-Rep.6]	Proposed Cross Acceptance Processes for Railway Signalling Systems and Equipment. Institution of Railway Signal Engineers. International Technical Committee. 6th report.
[TR 50506-1]	CLC/TR 50506-1:2007 “Railway applications - Communication, signalling and processing systems” - Application guide for EN 50129 – Part 1: Cross-acceptance
[TR 50506-2]	CLC/TR 50506-2 Railway applications – Communication, signalling and processing systems – Application guide for EN 50129 – Part 2: safety assurance

1.2 Terms and Definitions

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

Term	Description
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.)

The following terms and definitions are further used throughout this document.

Term	Description
Independent Safety Assessor	"Independent Safety Assessor" (ISA) is an independent third party to assess safety in the field of urban guided transport applications.
Light Rail	Light Rail Transit (LRT) is an electric rail-borne form of transport which can be developed in stages from a tram to a metro-like system operated partially on its own right-of-way. The general term 'light transit' covers those systems whose role and performance lie between a conventional bus service running on the highway at one extreme and an urban heavy rail or underground metropolitan railway at the other. Light rail systems are thus flexible and expandable. Source: http://www.uitp.org/public-transport/light-rail/index.cfm

Term	Description
Metros	Metropolitan railways are urban, electric transport systems with high capacity and a high frequency of service. Metros are totally independent from other traffic, road or pedestrians. They are consequently designed for operations in tunnel, viaducts or on surface level but with physical separation. Metropolitan railways are the optimal public transport mode for a high capacity line or network service. Some systems run on rubber-tyres but are based on the same control-command principles as steel-wheel systems. In different parts of the world metro systems are also known as the underground, subway or tube. Source: http://www.uitp.org/Public-Transport/metro/index.cfm
Operator	"Operator" means a public or private undertaking, the activity of which is to provide the transport of passengers by urban guided transport (UGT) systems.
Safety Authority*	"Safety Authority" refers to the body responsible for certifying that a safety-related system is fit for service and complies with relevant statutory and regulatory safety requirements, ref. EN 50129, [CENELEC].
Safety Case	The documented demonstration that the product complies with the specific safety requirements.
Supplier	"Supplier" is defined as a contractor who provides the urban guided transport system or one of its sub-systems. Generally, a supplier is a manufacturer of a sub-system such as Rolling Stock or Infrastructure. In addition, a supplier may also be appointed as a company supplying the whole urban guided transport system by means of sub-contractors.
Tram	A tram is an urban electric rail-borne system sharing the track right-of-way with the general road traffic. It is a special kind of "Light Rail".

Refer also to [GLOSSARY.en]

1.3 Abbreviations

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)
BOStrab	Verordnung über den Bau und Betrieb der Straßenbahnen (German Federal Regulations on the construction and operation of light rail transit systems)
CCOR	Completion & Consent to Operate Report
CDS	Conceptual Design Statement
CNESTG	Commission Nationale d'Évaluation de la Sécurité des Transports Guidés National Committee for Evaluation of Guided Transport Safety
CR	Concept Report
CTR	Consent to Test / Trial Report
DAkkS	Deutsche Akkreditierungsstelle National accreditation body for the Federal Republic of Germany
DCC	Design Check Certificates
DDR	Detailed Design Reviews
DDS	Dossier de Définition de Sécurité (Safety Definition Case)
DPS	Dossier Préliminaire de Sécurité (Preliminary Safety Case)
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 Requirements
GOA	Grade of Automation
ICP	Independent Competent Person
ISA	Independent Safety Assessor
LRT	Light Rail Transit
LU	London Underground
MODSafe	Modular Urban Transport Safety and Security Analysis
MODUrban	Modular Urban Guided Rail System project
PCHC	Project Completion & Handover Certificate

Abbreviation	Explanation
PEP	Project Execution Plan
PMF	Project Management Framework
RAMS	Reliability, Availability, Maintainability and Safety
SNCF	Société nationale des chemins de fer français
SR	Safety Requirements
SRS	System Requirements Specification
SSC	System Safety Case
STRMTG	Service Technique des Remontées Mécaniques et des Transports Guidés French Technical Agency for Ropeways and Guided Transports Safety
TRS	Technical Requirements Specification
UGT	Urban Guided Transport (System)
UK	United Kingdom
UKAS	United Kingdom Accreditation Service
VAP	Verification Activity Plan
VVR	Verification and Validation Report
WP	Work Package

2 Methodological background

2.1 Method of work package 7

This sub-clause briefly introduces the method how this work package 7 can reach its desired aim.

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 throughout Europe.

Such typical optimised framework could offer relevant authorities a common reference throughout Europe and therefore facilitate the creation of new urban guided transport 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 [MODSafe D7.1]. Secondly, in this survey the elementary activity steps were identified [MODSafe D7.2]. As a result a list of elementary activity modules was provided. In the synthesis phase first a typical model of an AAC procedure is drafted, based on the elementary activity modules. This is done in this deliverable in a second step, based on the typical model, a typical optimised framework AAC procedure is proposed.

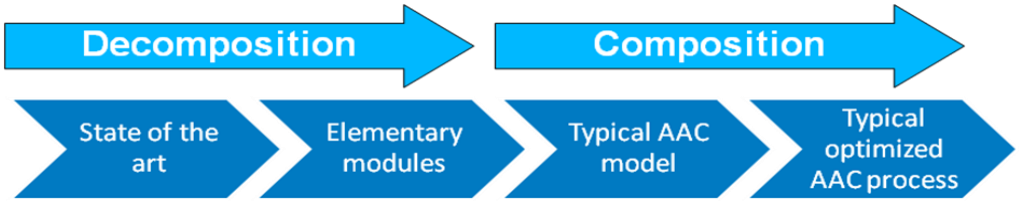


Figure 1 – Work process of WP7

The work process is organized 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
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 (current task)
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.

2.2 Summary of the results of preceding tasks

In task 7.1 a survey was carried out in order to collect data about the current acceptance, approval and certification processes used in different countries of Europe in the field of urban guided transport systems. For this a questionnaire was used, which was elaborated in work package 6, task 6.1. From this questionnaire the relevant questions and answers were selected and analysed. As an outcome of the analysis the following results were gained:

- Definition of the terms acceptance, approval and certification
- Identification of the main participants of the approval, acceptance and certification processes.

In task 7.2 the work was continued in order to identify the so-called elementary activity modules (EAM). The elementary activity modules (EAM) are activities that are identical in approval, acceptance and certification processes of different countries, but they may be carried out by different parties with different levels of independence, and possibly at different stages of the system life cycle.

To identify these elementary activity modules, they have to be found in different processes. This can be 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. As a result of comparison of different description methods, cross functional flowcharts were selected as a common description.

After finishing the task 7.1 it became clear, that a whole and complete European survey with such details that enable the identification of EAMs was not possible within this work package. Therefore it was decided to select a possible representative sample of countries, which can be analysed in more details. Using the cross functional flowcharts, the following case studies were elaborated in more details:

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

After the analysis and comparison of the processes, described in detail in the case studies, similar activities were found. These are the activities that were defined as Elementary Activity Modules. These are elementary parts of the processes. In [MODSafe D7.2] the following EAMs were identified (grouped according to system hierarchy level):

- 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 EAMs were organised in a system, according to life cycle phases and the system hierarchy level. The result of this is shown in Figure 2.

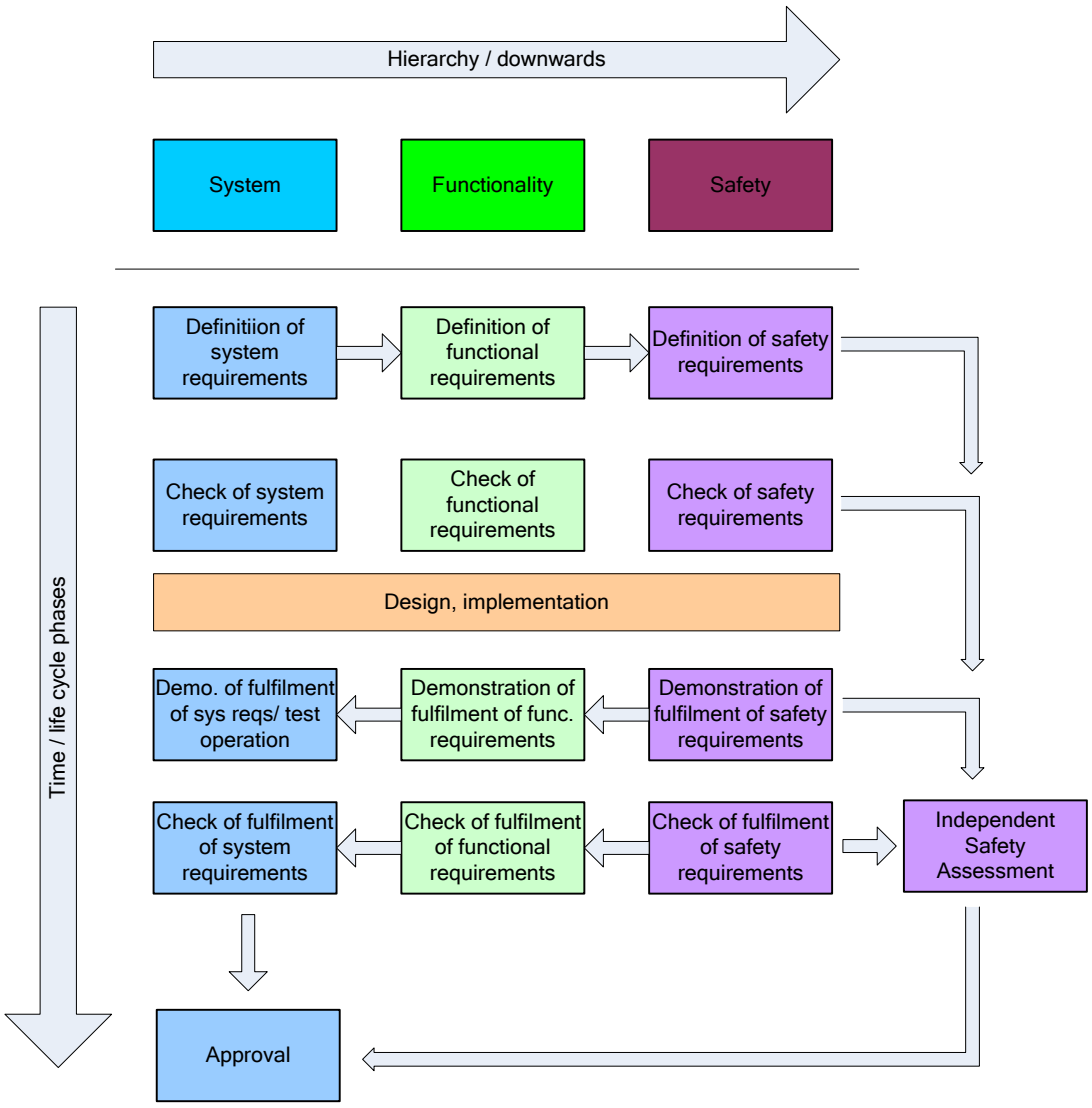


Figure 2 – System of EAMs [MODSafe D7.2]

Furthermore, the EAMs were linked to specific phases of the life cycle, proposed in [MODSafe D6.3]

2.3 Method of D7.3

In this task the following objectives are met:

In [MODSafe D7.2] the elementary activity modules were identified and systematised. For validation purposes it must be investigated whether these EAMs can be used to describe real AAC processes. This validation is done in chapter 3, where case studies, elaborated in [MODSafe D7.2] are shown, covered by EAMs.

Chapter 4 is dedicated to the description of generic AAC procedures. In frame of this, the generic AAC procedures are described in sub-clause 4.1 according to different system hierarchy levels (system, functionality and safety).

Following this an allocation is presented in sub-clause 4.2, where EAMs are linked to the main participants of AAC process. Based on this allocation the typical participant actions are described in sub-clause 4.3.

In sub-clause 4.4 the role of certification and the necessary qualification of independent bodies is discussed.

3 Description of AAC procedures with help of EAMs

The main goal of this chapter is to show that the elementary activity modules (EAMs), identified in [MODSafe D7.2] can be used in the description of existing, practised AAC procedures. For this purpose the same flowcharts are used and the coverage of the activities by EAMs is shown in the figures.

Following the flowchart for each case study the allocation of EAMs to generic participants is presented using a table. The generic potential participants were identified in [MODSafe D7.1] as follows:

- the operator
- the supplier,
- the authority,
- an Independent Safety Assessor,
- an independent (certification) body.

For the allocation of the EAMs the following concepts are used, also showing their abbreviation:

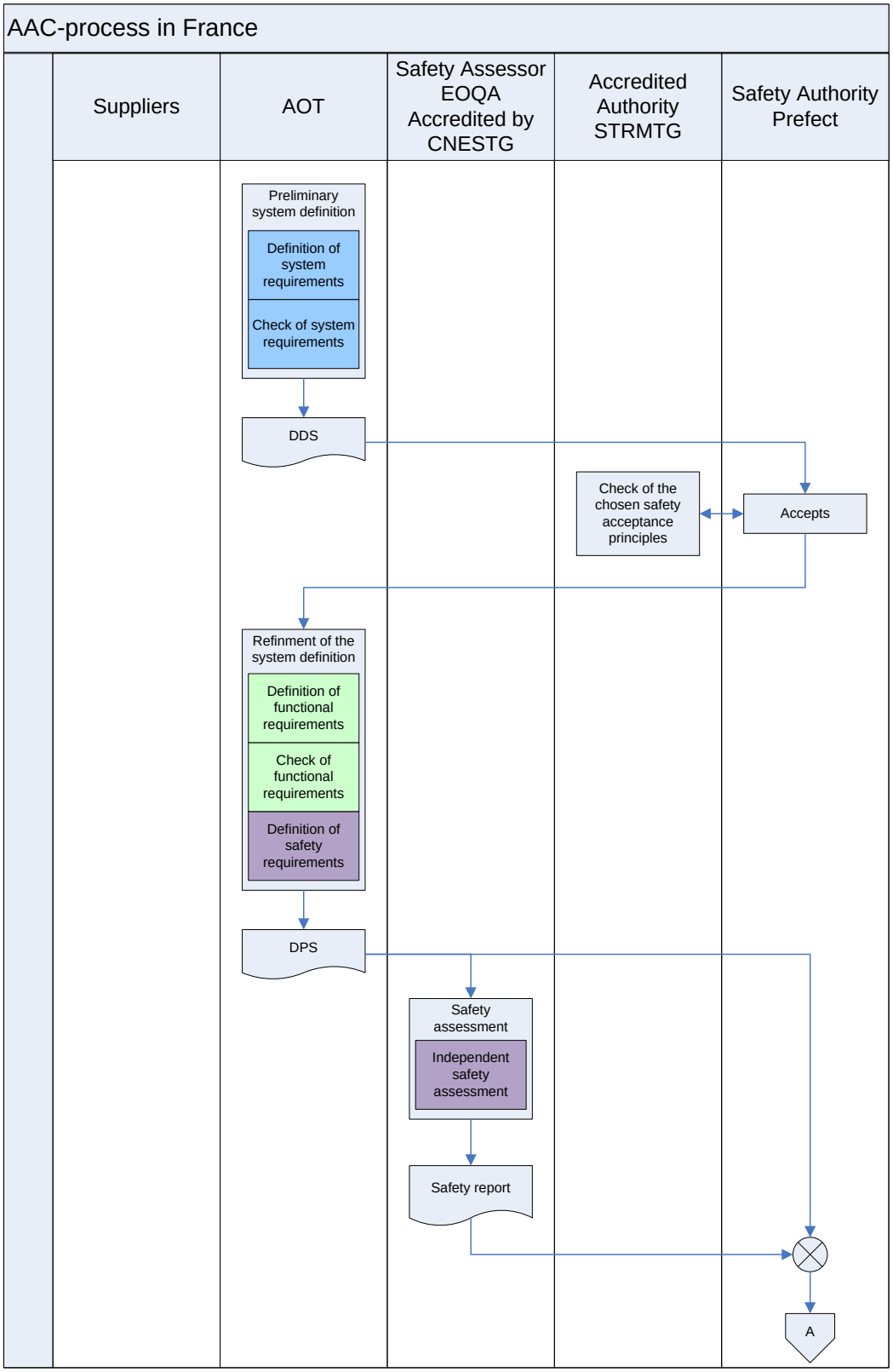
- Responsible: R (the organisation which is responsible for the execution of the activity)
- Perform: P (the organisation which performs/executes the activity)
- Consulted: C (an organisation which is consulted during the execution of the activity)
- Informed: I (an organisation which is informed during the execution of the activity)

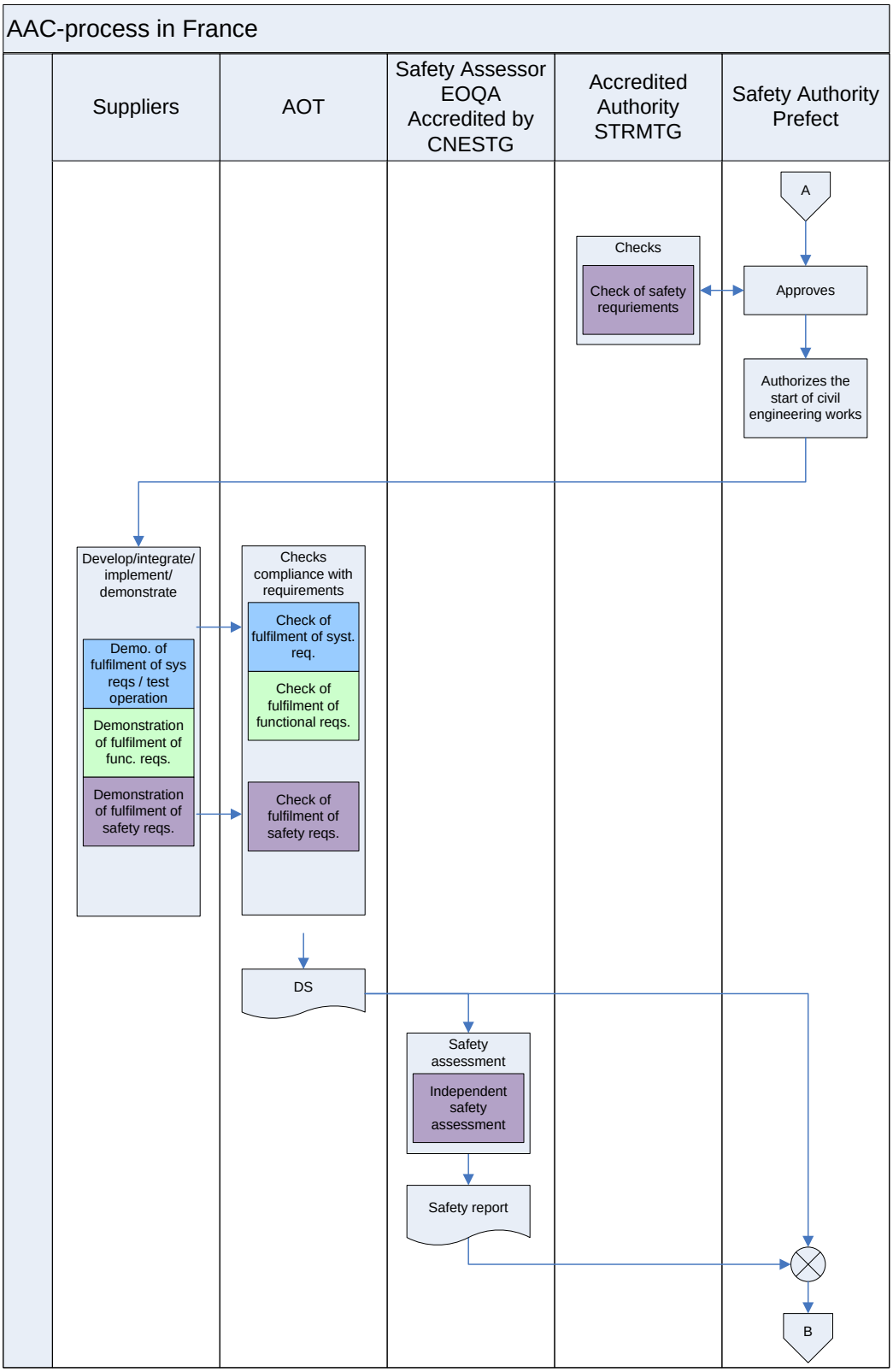
In certain cases there are alternative possibilities to perform an activity. In these cases the alternative possibilities are marked by '/a'.

Note that in most of the cases the organisation which is responsible for the execution of the given activity is the same which performs the activity. In these cases the responsibility and the performance is not indicated separately.

3.1 Case study France

3.1.1 Process description with EAMs France




AAC-process in France
Suppliers
AOT
Safety Assessor EOQA Accredited by CNESTG
Accredited Authority STRMTG
Safety Authority Prefect
A
Checks
Check of safety requriements
Approves
Authorizes the start of civil engineering works
Develop/integrate/ implement/ demonstrate
Demo. of fulfilment of sys reqs / test operation
Demonstration of fulfilment of func. reqs.
Demonstration of fulfilment of safety reqs.
Checks compliance with requirements
Check of fulfilment of syst. req.
Check of fulfilment of functional reqs.
Check of fulfilment of safety reqs.
DS
Safety assessment
Independent safety assessment
Safety report
B

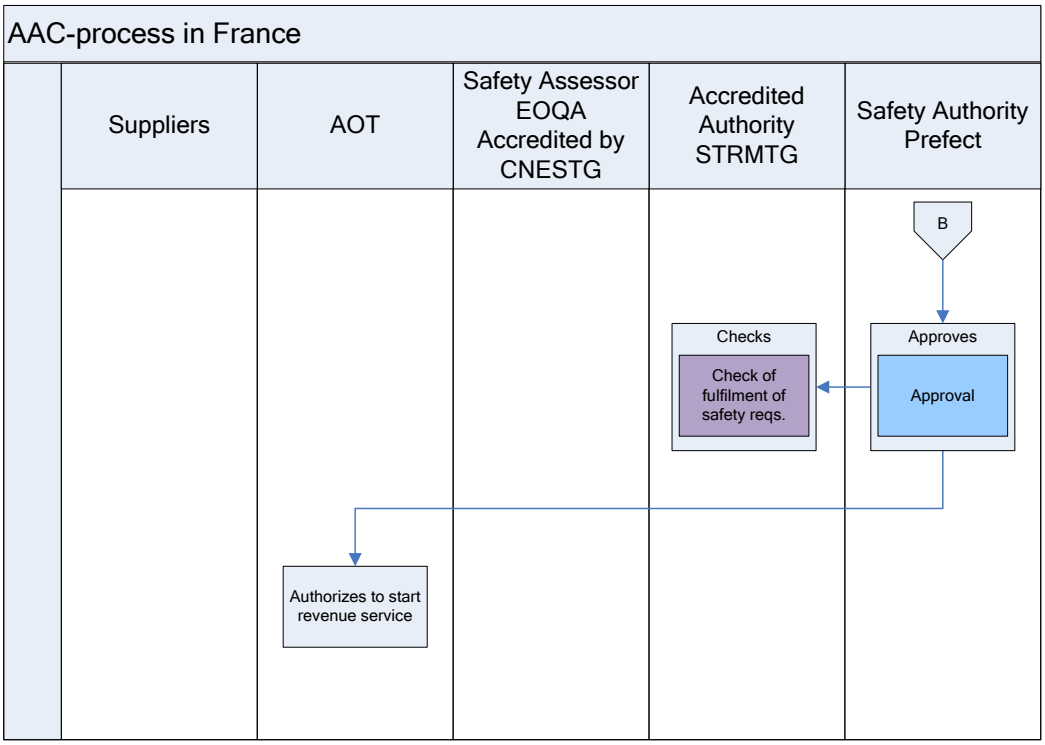


Figure 3– Approval Process France

3.1.2 Allocation of EAMs to participants France

EAM	Participant				
	Operator* (AOT)	Supplier	Safety Authority	Independent Safety Assessor	Independent body
Definition of system requirements	Resp.				
Check of system requirements	Resp.				
Definition of functional requirements	Resp.				
Check of functional requirements	Resp.				
Definition of safety requirements	Resp.				
Check of safety requirements			Resp.**		
Demonstration of fulfilment of safety requirements		Resp.			
Demonstration of fulfilment of func. requirements		Resp.			
Demo. of fulfilment of sys reqs/ test operation		Resp.			
Check of fulfilment of safety requirements	Resp.		Resp.**		Resp.*** (optional)
Check of fulfilment of functional requirements	Resp.				
Check of fulfilment system req.	Resp.				
Independent safety assessment				Resp.	
Approval			Resp.		

Table 1 – EAM's linked to participants in France

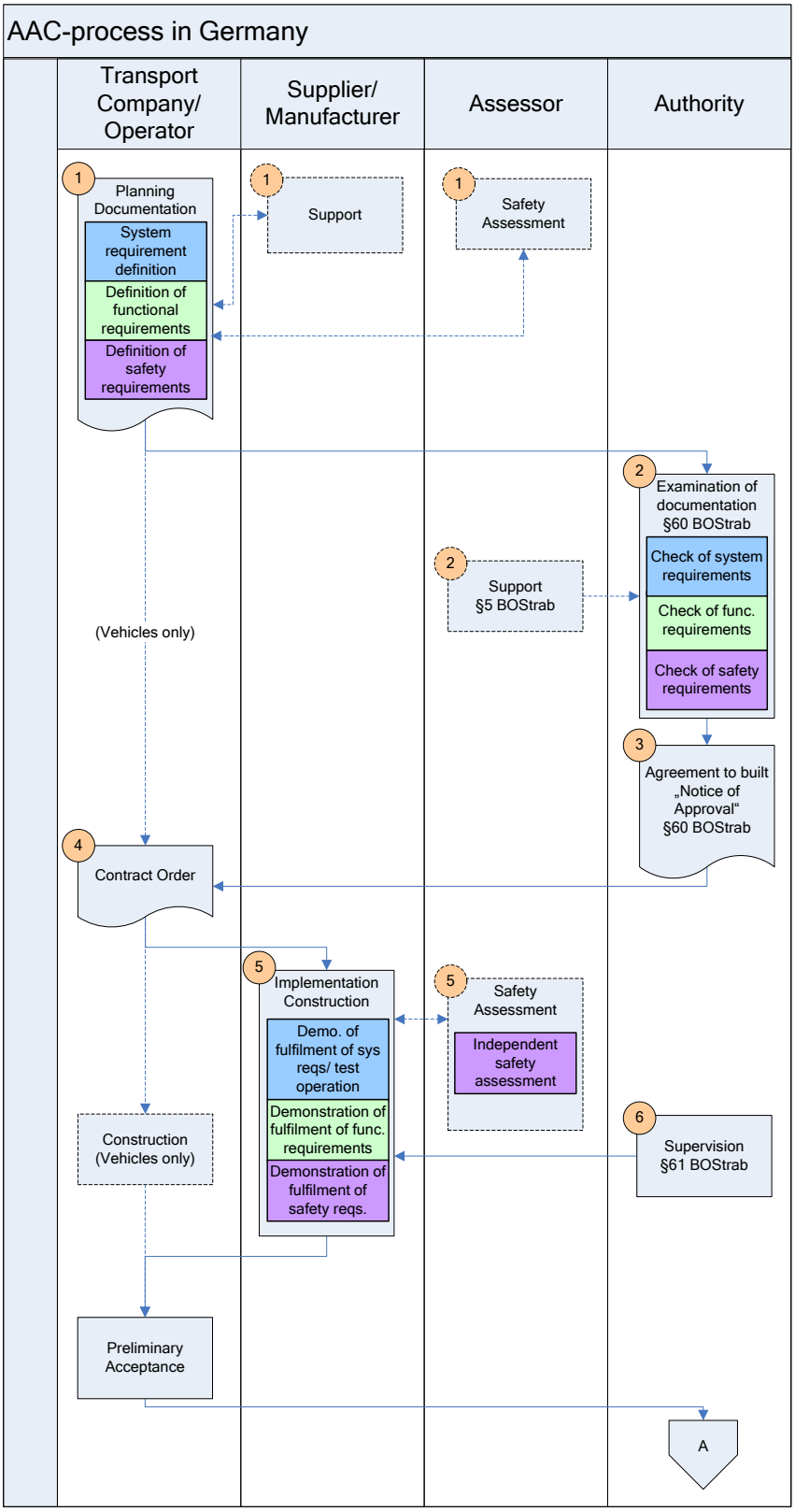
* Under ‘operator’ the AOT is meant in this table
** In case of France we can distinguish between Safety Authority/Préfect and Accredited Authority (STRMTG). For details refer to [MODSafe D7.2]
*** Some parts of a system can sometimes be certified by an independent certification body.

3.1.3 Analysis

The main steps of the French approval process can be covered by EAMs, however not each EAMs are used in the process.

3.2 Case study Germany

3.2.1 Process description with EAMs Germany



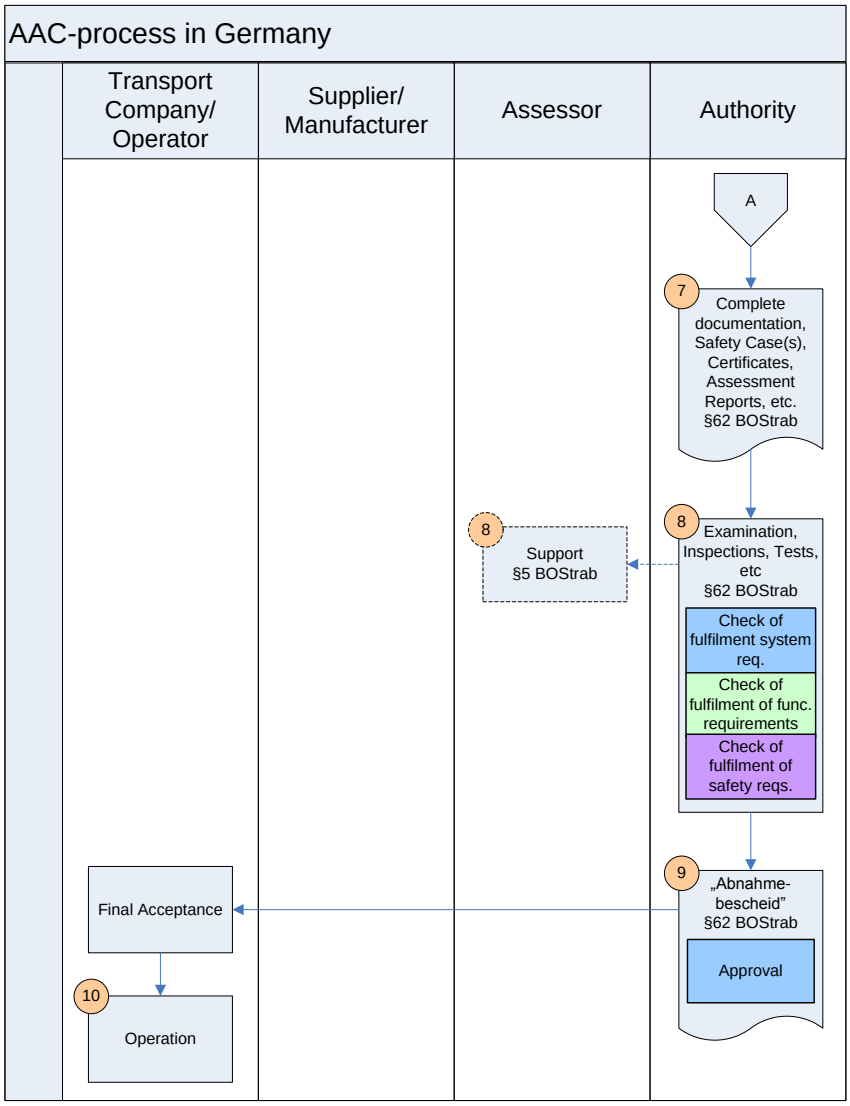


Figure 4 – Approval Process Germany

Note: the numbers in circles refer to more detailed description of the given phase, which is described in [MODSafe D7.2].

3.2.2 Allocation of EAMs to participants Germany

EAM	Participant				
	Operator	**Supplier**	**Safety Authority**	**Independent Safety Assessor**	**Independent body**
Definition of system requirements	Resp.	Consulted (optional)		Consulted (optional)	
Check of system requirements			Resp.	Consulted (optional)	
Definition of functional requirements	Resp.	Consulted (optional)		Consulted (optional)	
Check of functional requirements			Resp.	Consulted (optional)	
Definition of safety requirements	Resp.	Consulted (optional)		Consulted (optional)	
Check of safety requirements			Resp.	Consulted (optional)	
Demonstration of fulfilment of safety requirements		Resp.	Informed		
Demonstration of fulfilment of func. requirements		Resp.	Informed		
Demo. of fulfilment of sys reqs/ test operation		Resp.	Informed		
Check of fulfilment of safety requirements			Resp.	Consulted (optional)	
Check of fulfilment of functional requirements			Resp.	Consulted (optional)	
Check of fulfilment system req.			Resp.	Consulted (optional)	
Independent safety assessment				Resp. (optional)	
Approval			Resp.		

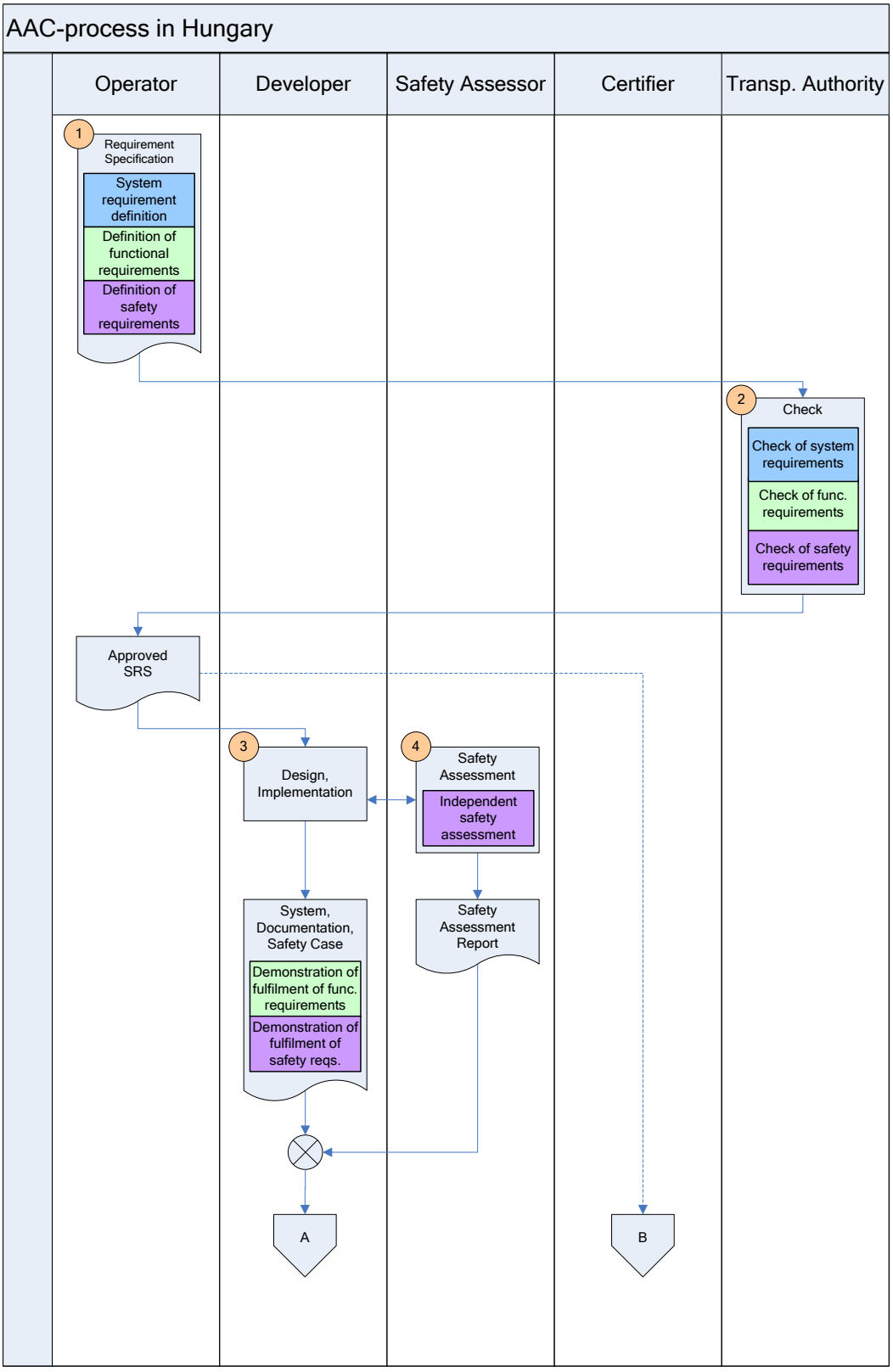
Table 2 – EAM's linked to participants in Germany

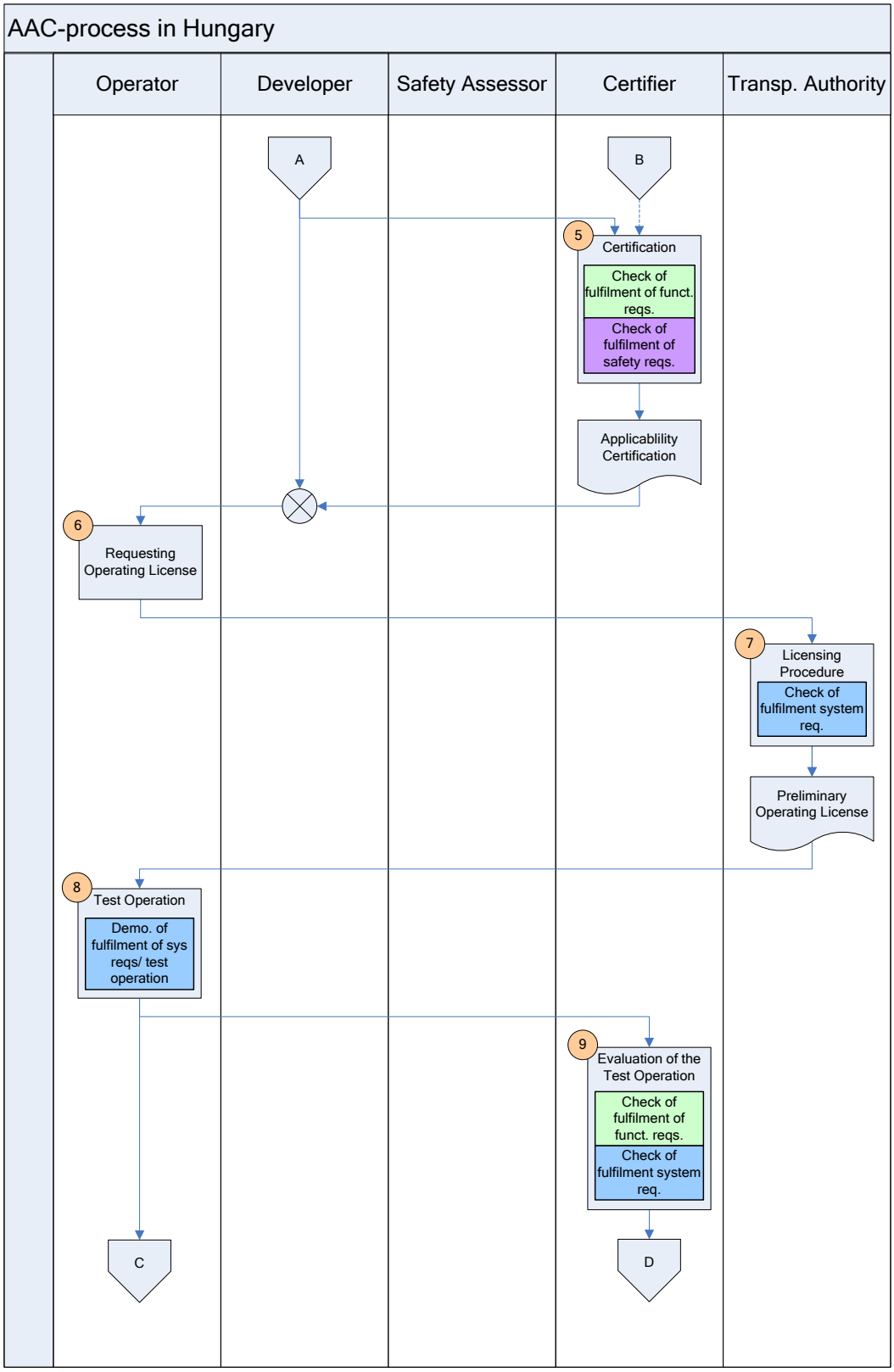
3.2.3 Analysis

Analysing the flowchart and the table it can be concluded, that all of the EAMs are used in the German AAC procedure, and all of the relevant activities are covered by one or more EAMs. The German case includes supports between parties of the procedures. This may be the case for other countries too, but not necessarily presented in the flowcharts.

3.3 Case study Hungary

3.3.1 Process description with EAMs Hungary




AAC-process in Hungary
Operator
Developer
Safety Assessor
Certifier
Transp. Authority
A
B
5
Certification
Check of fulfilment of funct. reqs.
Check of fulfilment of safety reqs.
Applicablility Certification
6
Requesting Operating License
7
Licensing Procedure
Check of fulfilment system req.
Preliminary Operating License
8
Test Operation
Demo. of fulfilment of sys reqs/ test operation
9
Evaluation of the Test Operation
Check of fulfilment of funct. reqs.
Check of fulfilment system req.
C
D

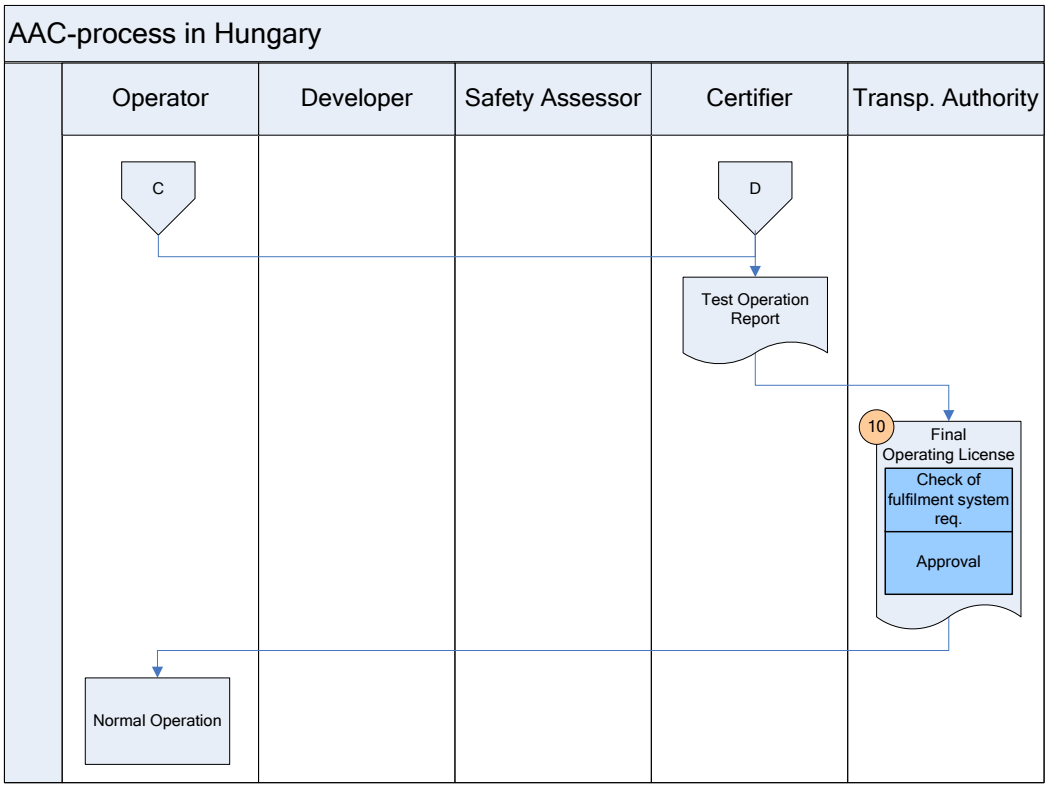


Figure 5 – Approval Process Hungary

Note: the numbers in circles refer to more detailed description of the given phase, which is described in [MODSafe D7.2].

3.3.2 Allocation of EAMs to participants Hungary

EAM	Participant				
	Operator	**Supplier**	**Safety Authority**	**Independent Safety Assessor**	**Independent certification body**
Definition of system requirements	Resp.				
Check of system requirements			Resp.		Consulted (optional)
Definition of functional requirements	Resp.				
Check of functional requirements			Resp.		Consulted (optional)
Definition of safety requirements	Resp.				
Check of safety requirements			Resp.		Consulted (optional)
Demonstration of fulfilment of safety requirements		Resp.			
Demonstration of fulfilment of func. requirements		Resp.			
Demo. of fulfilment of sys reqs/ test operation	Responsible		Informed		Informed
Check of fulfilment of safety requirements					Resp.
Check of fulfilment of functional requirements					Resp.
Check of fulfilment system req.	Resp.				Resp.
Independent safety assessment				Resp.	
Approval			Resp.		

Table 3 – EAM's linked to participants in Hungary

3.3.3 Analysis

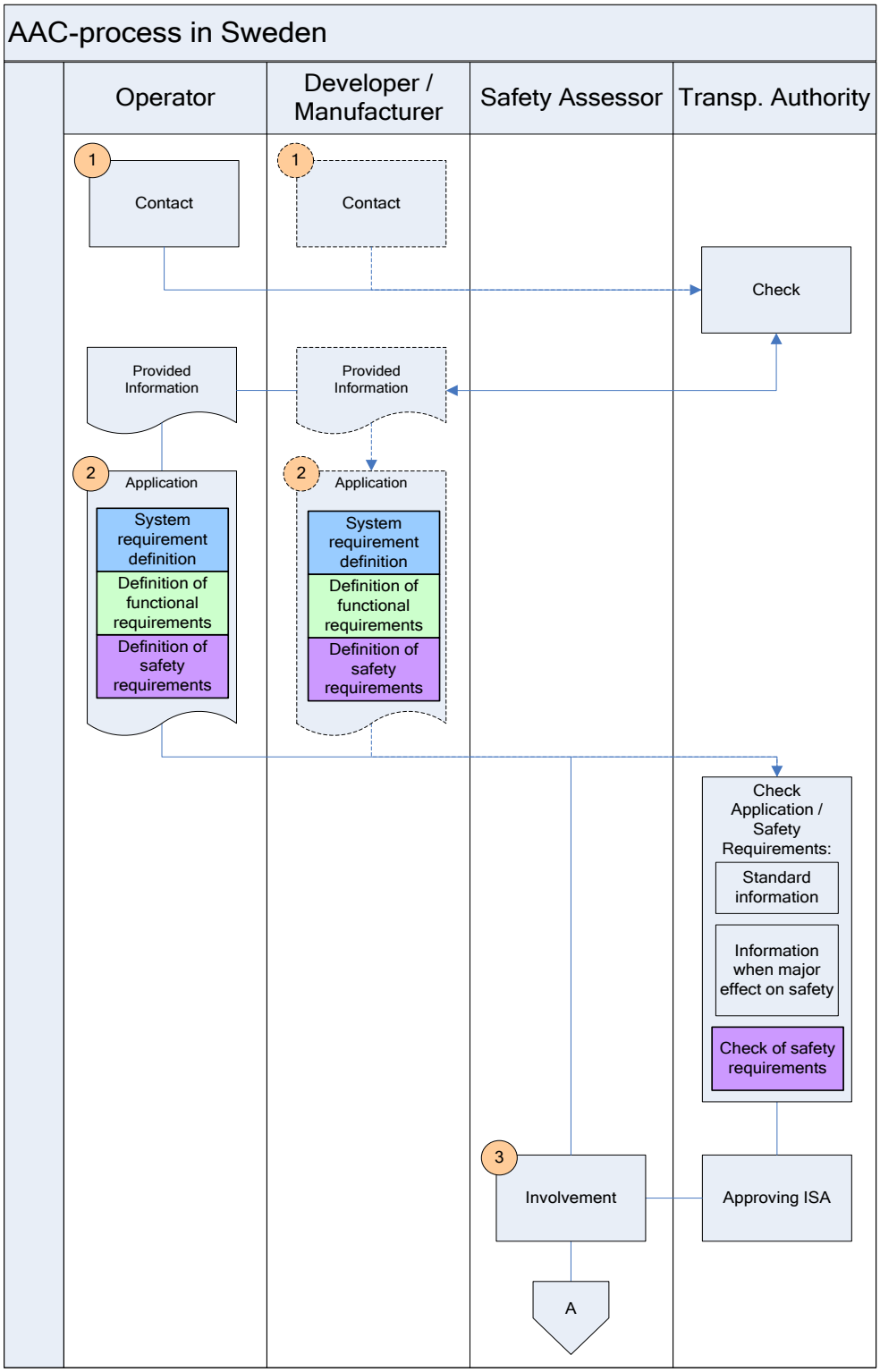
From the flowcharts it can be seen that the EAMs cover most of the activities, however some EAMs are treated together and do not form separate phases. E.g. the requirement specification (No. 1 in the figure) includes system, functional and safety requirements as well.

On the other hand, some EAMs appear in more phases. E.g. the checking of fulfilment of functional or system requirements is carried out already before the test operation, but the examinations terminate only after the evaluation of the test operation.

Looking at the allocation table it can be stated, that all of the EAMs appear somewhere in the process and all of the relevant phases – connecting to AAC procedures – are covered by one or more EAMs.

3.4 Case study Sweden

3.4.1 Process description with EAMs Sweden



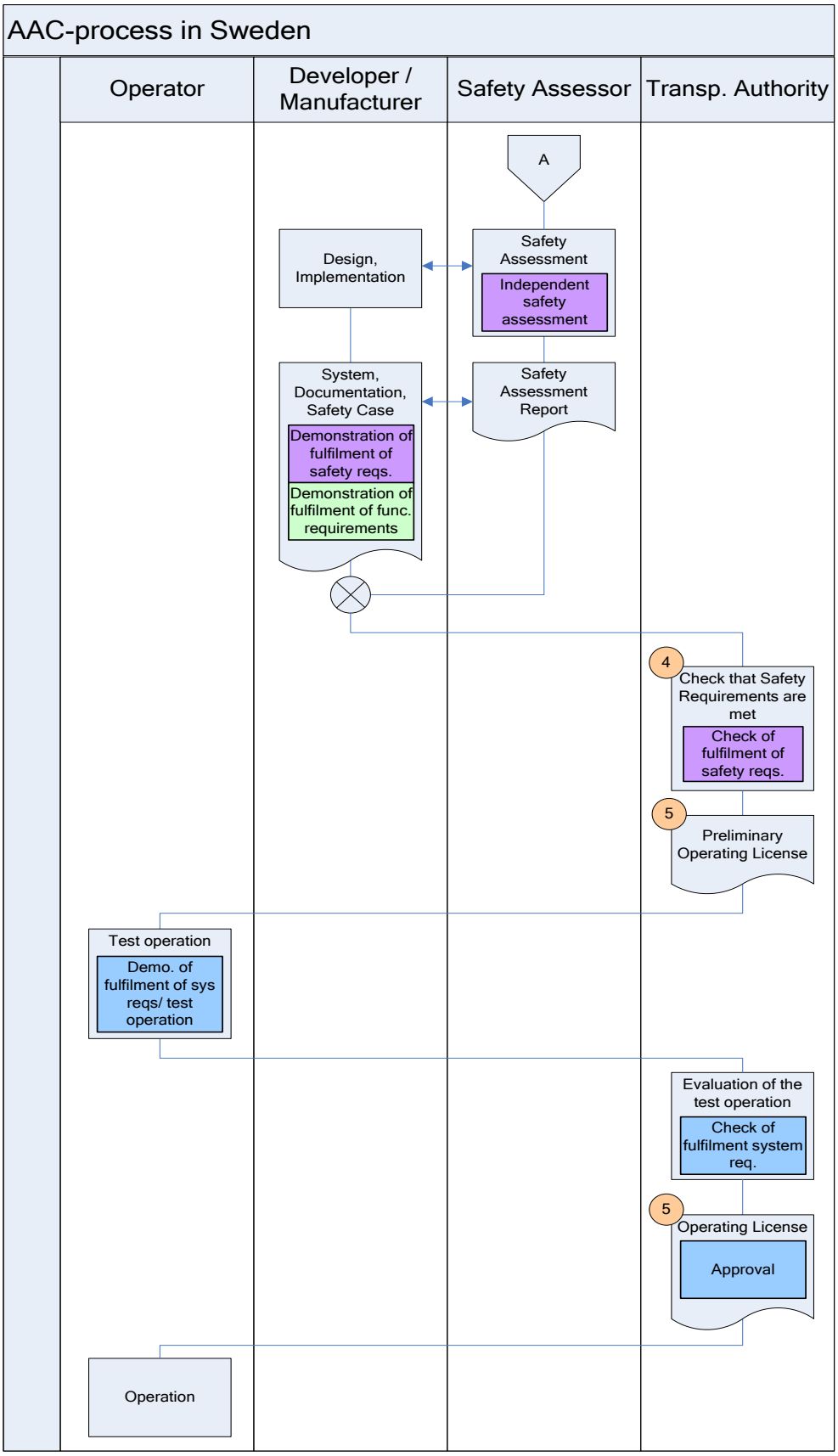


Figure 6 – Approval Process Sweden

Note: the numbers in circles refer to more detailed description of the given phase, which is described in [MODSafe D7.2].

3.4.2 Allocation of EAMs to participants Sweden

EAM	Participant				
	Operator	Supplier	Safety Authority	Independent Safety Assessor	Independent body
Definition of system requirements	Resp.	Resp. (alternat.)			
Check of system requirements					
Definition of functional requirements	Resp.	Resp. (alternat.)			
Check of functional requirements					
Definition of safety requirements	Resp.	Resp. (alternat.)			
Check of safety requirements			Resp.		
Demonstration of fulfilment of safety requirements		Resp.			
Demonstration of fulfilment of func. requirements		Resp.			
Demo. of fulfilment of sys reqs/ test operation	Resp.				
Check of fulfilment of safety requirements			Resp.		
Check of fulfilment of functional requirements					
Check of fulfilment system req.			Resp.		
Independent safety assessment				Resp.	
Approval			Resp.		

Table 4 – EAM's linked to participants in Sweden

3.4.3 Analysis

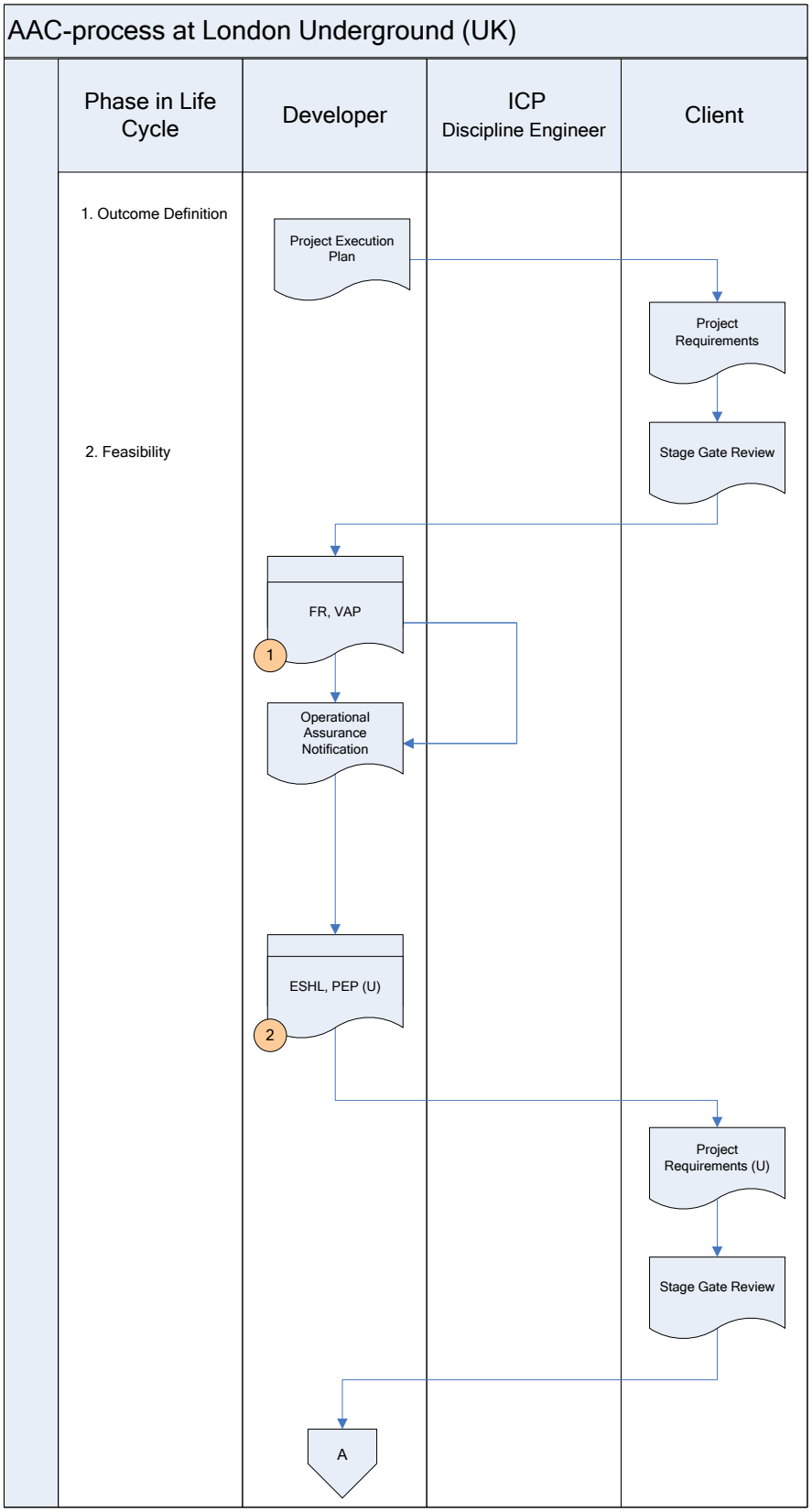
The Swedish AAC procedure can also be covered to a high degree with EAMs. In this case it is interesting that the roles are not allocated strictly to some parties, e.g. the definition of system/functional/safety requirements can be done either by the operator or by the developer.

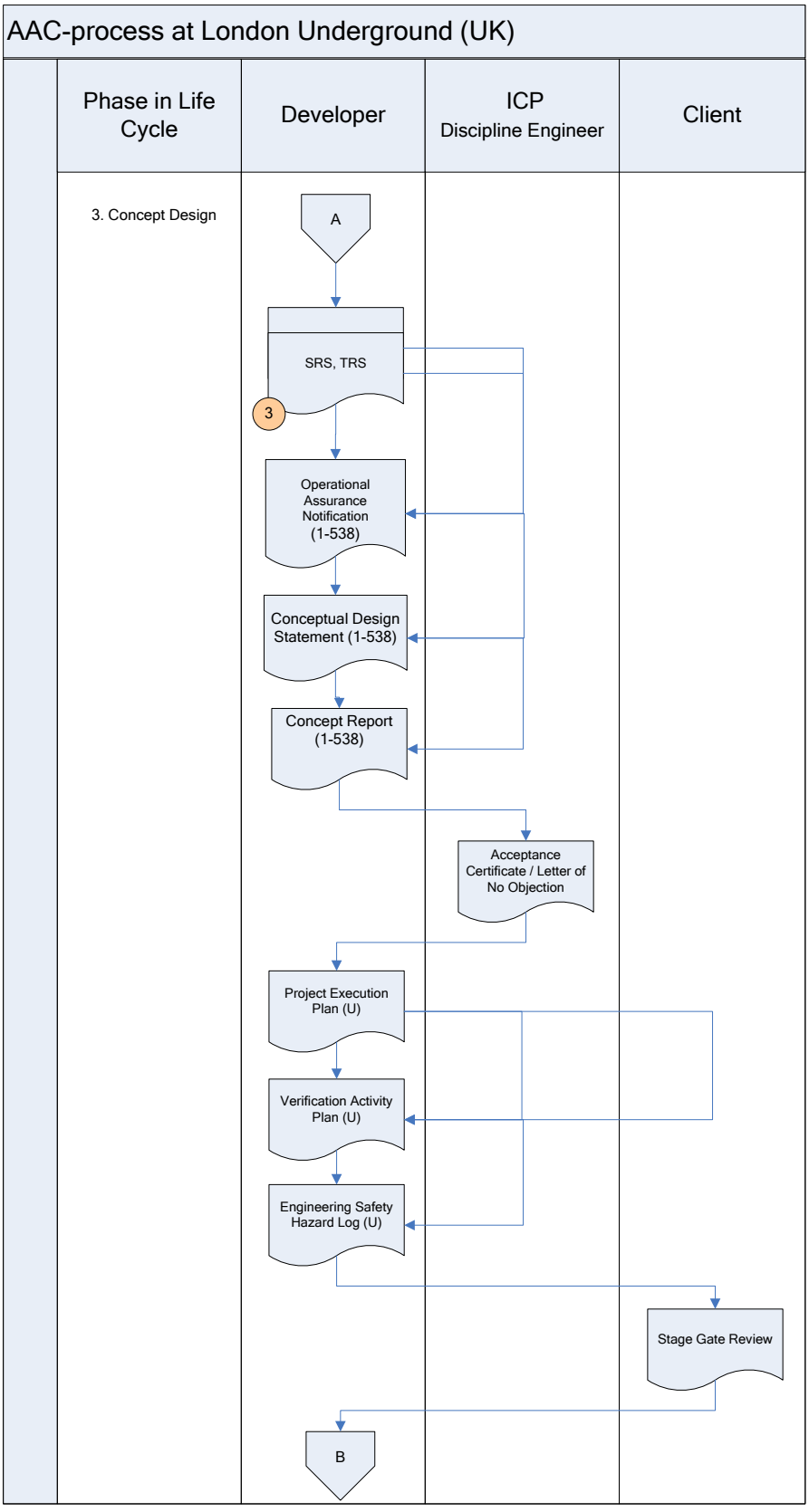
It can also be stated, that all of the relevant activities in the process are covered by one or more EAMs, however there are EAMs, which do not appear in the Swedish practice.

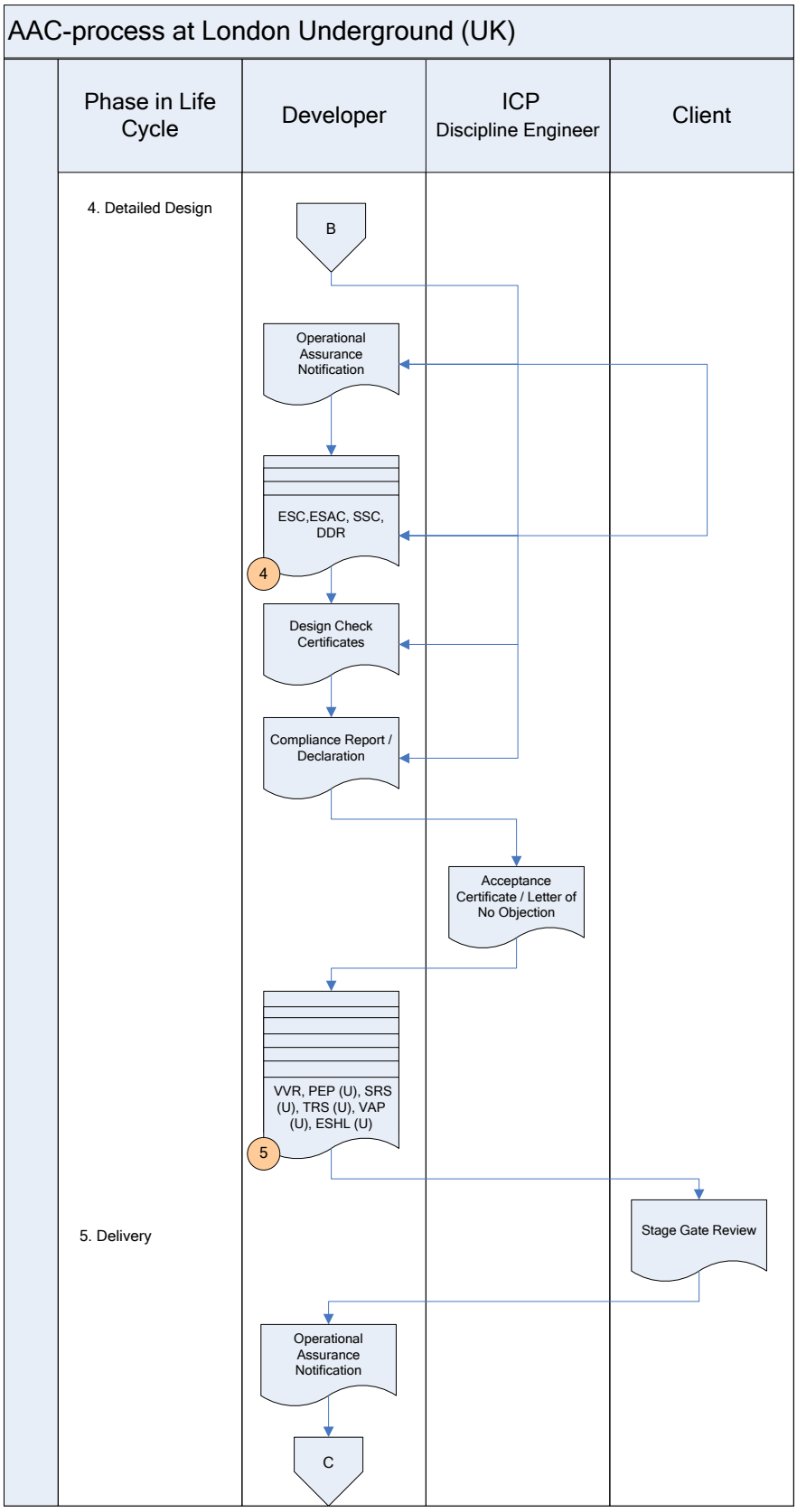
3.5 Case study United Kingdom (London Underground)

The acceptance, approval and certification process of London Underground (UK) follows partly different practice. Within the UK, legislation has been passed which allows the Transport Operator to act as the Safety Authority and therefore approval for change is an internal function (refer to [MODSafe D7.2], sub-clause 4.4.1).
The description of the LU AAC process (as it was done in [MODSafe D7.2]) is quite long. Therefore it seems to be more reasonable to follow a different representation technique for the investigation on the coverage of the process by EAMs. In spite of the different representation, the link of the EAMs can be done to the flowchart-type description of the AAC process of LU. To ease this, the flowchart of the LU AAC process is repeated here from [MODSafe D7.2]

3.5.1 Process description United Kingdom (London Underground)




AAC-process at London Underground (UK)
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


AAC-process at London Underground (UK)
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

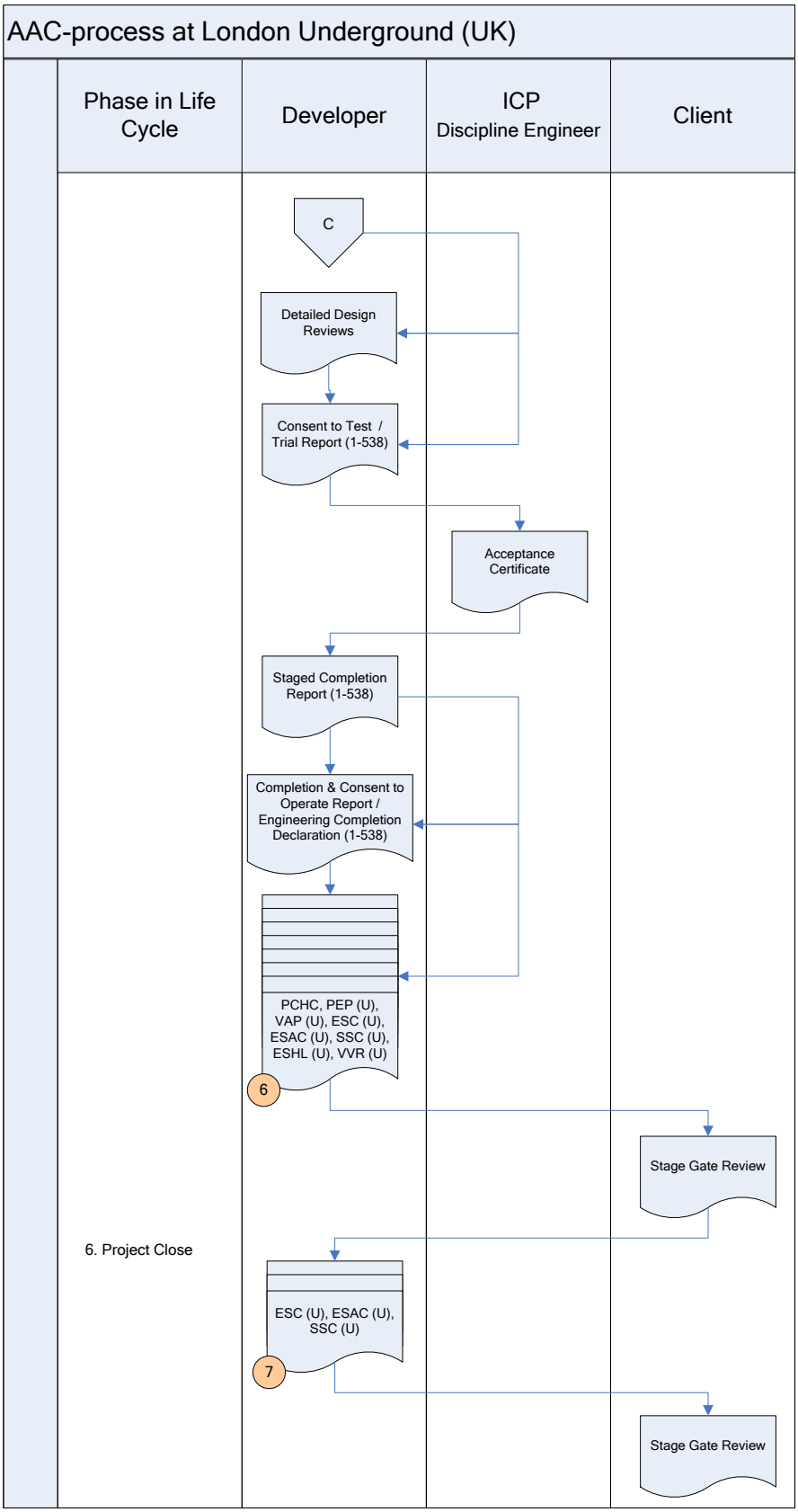


Figure 7 – Approval Process United Kingdom (London Underground)

Note: the numbers in circles refer to more detailed description of the given phase, which is described in [MODSafe D7.2].

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)

3.5.2 Process description with EAMs United Kingdom (LU)

In this sub-clause the EAMs are linked to the main phases of the United Kingdom (LU) AAC process. The AAC process at LU is divided into six main phases. These are:

1. Outcome Definition
2. Feasibility
3. Concept Design
4. Detailed Design
5. Delivery (Installation)
6. Project Close (Completion / Handover)

In the following table the EAMs are linked to these project phases.

Some remarks to the interpretation of the table:

- Name of relevant project documentations are marked with blue text to help interpretation.
- Project team also have integration responsibilities for example integrating new signalling system with the train.
- Appointment of Independent Competent Person (and ISA if necessary) is a Legal Requirement
- Figure 7 shows the role of Developer. In Table 5 below, the Developer role has been further broken down to show the roles “Supplier and Project Delivery”. The Project Delivery team are tasked with working with the supplier to deliver the project. The Project Assurance role is also part of the Project Team but remains independent of delivery and contains the ICP/ISA function.
- There is a legal requirement for a Safety Verification Scheme to be established for each Project at the beginning – this is the purpose of the Verification Activity Plan – and this is checked by the Transport Operator who acts as Safety Authority before Concept Design is commenced.

		Participant			
Phase in lifecycle	**EAM**	**Supplier**	**Project Delivery**	**Project Assurance (ICP/ISA)**	**Client (Railway Operator)**
1. Outcome Definition Relevant PMF Products: • Project Requirements • Project Execution Plan	Definition of system requirements Definition of functional requirements Definition of safety requirements Check of system requirements Check of functional requirements Check of safety requirements Independent safety assessment		Check of Project Requirements Produce Project Execution Plan	Check of Project Requirements Check of Project Execution Plan	Definition of Project Requirements which contain the high level System Reqs and Safety Reqs… Check of Project Execution Plan
2. Feasibility Relevant PMF Products: • Verification Activity Plan • Eng Safety Haz Log	Independent safety assessment		Produce Verification Activity Plan Produce Eng Safety Haz Log	Check of Verification Activity Plan Check of Eng Safety Haz Log	Check of Verification Activity Plan

		Participant			
Phase in lifecycle	**EAM**	**Supplier**	**Project Delivery**	**Project Assurance (ICP/ISA)**	**Client (Railway Operator)**
3. Concept Design Relevant PMF Products – • System Req Spec (SRS) • Conceptual Design Statement (CDS) • Concept Report (CR) • Eng Safety Haz Log • Acceptance Cert	Definition of system requirements Definition of functional requirements Definition of safety requirements Check of system requirements Check of functional requirements Check of safety requirements Independent safety assessment	Produce Concept Design which satisfies System, Functional & Safety Requirements (outputs are CDS, CR, Eng Safety Haz Log)	Definition of System Req (SRS), Functional Req (SRS*), Safety Req. (SRS & Eng Safety Haz Log) + (Concept report & Conceptual Design Statement) * *Functional requirements contain 2nd order safety requirements such as reliability and operability and also degraded modes. These are important aspects for an underground mass transit railway.*	Check of System Req (SRS), Functional Req (SRS), Safety Req. (SRS & Eng Safety Haz Log), + (Concept report & Conceptual Design Statement) Issue of (Acceptance Certificate / Letter of No Objection)* * *This Acceptance Cert / Letter is the output that demonstrates that the project can move to the next phase*	

		Participant			
Phase in lifecycle	**EAM**	**Supplier**	**Project Delivery**	**Project Assurance (ICP/ISA)**	**Client (Railway Operator)**
4. Detailed Design Relevant PMF Products: • Eng Safety Case • Eng Safety & Assurance Case • System Safety Case • Detailed Design Review • Design Check Cert • Compliance Report • Verification & Validation Report (VVR) • Acceptance Cert	Check of system requirements Check of functional requirements Check of safety requirements Independent safety assessment	Produce Detailed Design (with evidence which demonstrates how all requirements are met)	Check* of System Req , Functional Req , Safety Req. (ESC, ESAC, SSC, DDR, DCC, CR, VVR) * *Checking is done by the internal project team – V&V department.*	Check of System Req , Functional Req-, Safety Req. (ESC, ESAC, SSC, DDR, DCC, CR, VVR) Issue of (Acceptance Certificate / Letter of No Objection)* * *This Acceptance Cert / Letter is the output that demonstrates that the project can move to the next phase*	

		Participant			
Phase in lifecycle	**EAM**	**Supplier**	**Project Delivery**	**Project Assurance (ICP/ISA)**	**Client (Railway Operator)**
5. Delivery (Installation) Relevant PMF Products: • Consent to Test / Trial Report (CTR) • Staged Completion Report • Completion & Consent to Operate Report (CCOR) • Project Completion & Handover report	Demonstration of fulfilment of SR Demonstration of fulfilment of func. requirements Demo. of fulfilment of sys reqs/ test operation Check of fulfilment of safety requirements Check of fulfilment of functional requirements Check of fulfilment system req. Independent safety assessment Approval	Install & Test Systems / Equipment Demo of fulfilment of System Req, Functional Req, Safety Req / Test Operation* ** Supplier has to support the demonstration activity as well.*	Check* of fulfilment of System Req, Functional Req, Safety Req (ESC, ESAC, SSC, DDR, DCC, CR, VVR) ** Checking is done by the internal project team, demonstration is done by the supplier and part of the project team.* Demo of fulfilment of System Req, Functional Req, Safety Req / Test Operation (ESC, ESAC, SSC, DDR, DCC, CR, VVR, CTR, CCOR),	Independent Safety Assessment (review of ESC, ESAC, SSC, DDR, DCC, CR, VVR,CTR, CCOR) Approval (Issue of Acceptance Certificate / Letter of No Objection) * ** This Acceptance Cert / Letter is the output that demonstrates that the project can move to the next phase*	Approval (Acceptance of CTR, CCOR)* **Legal Requirement, CCOR = Approval to operate the system with passenger service*

		Participant			
Phase in lifecycle	**EAM**	**Supplier**	**Project Delivery**	**Project Assurance (ICP/ISA)**	**Client (Railway Operator)**
6. Project Close (Completion / Handover) Relevant PMF Products – • Finalisation of ESC, ESAC, SSC...	Approval		Check* of fulfilment of System Req, Functional Req, Safety Req (ESC, ESAC, SSC) * *Checking is done by the internal project team, demo is done by the supplier part of the team*		"Approval" to close / complete Project (note approval not the same as detailed in the stage above)

Table 5 – EAM's linked to project phases United Kingdom (London Underground)

3.5.3 Allocation of EAMs to participants United Kingdom (LU)

EAM	Participant				
	Operator (Client)	Supplier	Project Delivery	Project Assurance (ICP/ISA)	
Definition of system requirements	Resp.				
Check of system requirements			Resp.	Resp.	
Definition of functional requirements	Resp.				
Check of functional requirements			Resp.	Resp.	
Definition of safety requirements	Resp.				
Check of safety requirements			Resp.	Resp.	
Demonstration of fulfilment of safety requirements		Resp.	Resp.		
Demonstration of fulfilment of func. requirements		Resp.	Resp.		
Demo. of fulfilment of sys reqs/ test operation		Resp.	Resp.		
Check of fulfilment of safety requirements			Resp.		
Check of fulfilment of functional requirements			Resp.		
Check of fulfilment system req.			Resp.		
Independent safety assessment				Resp.	
Approval	Resp.				

Table 6 – EAM's linked to participants United Kingdom (LU)

3.5.4 Analysis

As already stated, the AAC process of LU differs from other process examined in this document. Within the UK, legislation has been passed which allows the Transport Operator to act as the Safety Authority and therefore approval for change is an internal function. The EAMs can be linked quite easily to participants; however the link is not evident to different phases of projects.

3.6 Evaluation of case studies

With these examples it could be validated that the EAMs can be used in the description of AAC procedures, however it is not always possible to describe existing processes perfectly, using only the elementary activity modules, as differences between national regulations are still evident.

The results of the comparison of analyses are shown in the following table.

Case study	Main steps are covered by EAMs? [yes/no]	Number of EAMs used [No. / No. of EAMs]	Notes
France	yes	14/14	-
Germany	yes	14/14	Flowchart indicated support between parties of the process
Hungary	yes	14/14	Some EAMs are carried out in more phases
Sweden	yes	11/14	Some EAMs are not dedicated strictly to one participant.
United Kingdom (London Underground)	yes	14/14	Organisational structure is rather different

Table 7 - EAM's comparison results

From the allocation tables it can be concluded that the EAMs "Check of functional requirements" and "Check of system requirements" are in more cases not carried out in the AAC processes. This can be interesting as an optimisation option, if less complex processes are aimed.

It also can be stated that an independent assessor is in all case studies applied, however another independent body is only in the Hungarian case involved. It must be noted, that in Hungary the role of the independent assessor and the independent certifier is overlapping.

The case studies presented in the chapter are intended to be generic approaches, in the sense of not taking into account the type of the system to be accepted, certified or approved, i.e. tramway systems and metro system with different grades of automation were not considered. This is due to the generic nature of the used EAMs, and the descriptions apply in principle for all types of systems. Possible differences of different types of systems are treated in MODSafe D7.4.

Furthermore the case studies and the generic AAC process descriptions do not deal with the involvement of different authorities (like road traffic authorities in case of tramway systems or fire department in general) in AAC process.

4 Description of a generic AAC procedure

4.1 Description of generic processes at different hierarchy levels

In this [MODSafe D7.2] the identified EAMs were organized on one hand according to the level of hierarchy. Three hierarchical levels were defined, such as:

- system level,
- level of functionality and
- level of safety.

At system level such properties are treated, which can be interpreted at the highest level of a system. E.g. system requirements are such requirements, which can be fulfilled at system level. Furthermore, systems are designed to perform specified function(s). The properties of these functions are treated at functional level. If a function is a safety function, then safety requirements are to be fulfilled. Safety properties of systems are handled at safety level. Nevertheless, a system is composed from all of the safety properties, the functional performance and some additional system properties as well.

In the following sub-clauses the generic AAC process is described at different levels of hierarchy. Note that the following sub-clauses focus on the activities connected to acceptance, approval and certification; therefore other activities are not treated in details. The description of inputs and outputs of each EAM can be found in [MODSafe D7.2].

On the figures of the following sub-clauses the darker background colour of the boxes indicate the EAMs, while boxes with lighter background colours show connecting processes or documentations, which are inputs and outputs for EAMs.

4.1.1 Generic AAC process at system level

At the system level the process starts with a concept, and based on this the system requirements can be defined. Note that system requirements include functional requirements as well as safety requirements; the processes of dealing with these aspects is described in later sub-clauses. The system specification is checked (verified) and if it is acceptable (agreed system specification), it can serve as a basis for the design and implementation.

The supplier of the system has to demonstrate that the defined system requirements are met. For this often a test operation is carried out. The demonstration of fulfilment of system requirements is often checked. The fulfilment of system requirements incorporates the fulfilment of functional requirements and safety requirements as well. These aspects are covered in the next sub-clauses. If all requirements are met the system may be approved, which is the final act before putting the system into operation.

The whole process is described in Figure 8.

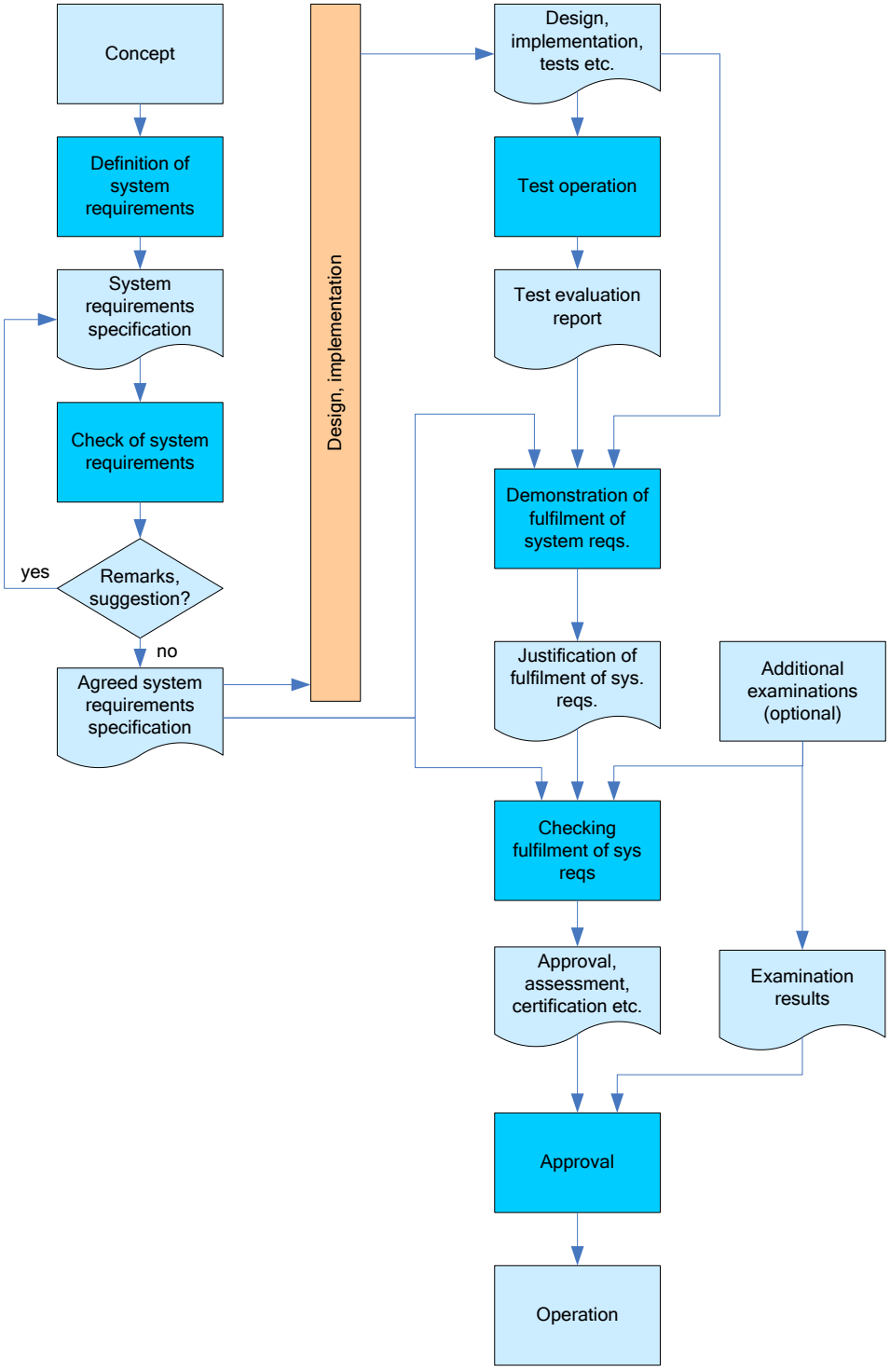


Figure 8 – Generic AAC process at system level

4.1.2 Generic AAC process at the level of functionality

The process of acceptance, approval and certification at the level of functionality is very similar to the one of the system level. At the functional level the starting point is the system requirements, from which the functional requirements can be specified. This specification is usually checked (verified) and results in an agreed specification of functional requirements. This serves as a basis for the design and the implementation.

The supplier has to demonstrate the fulfilment of the functional requirements, and the demonstration or justification is usually checked by the user of the system (as a minimum), which is the operator in the case of urban guided transport systems.

The whole process is depicted in Figure 9.

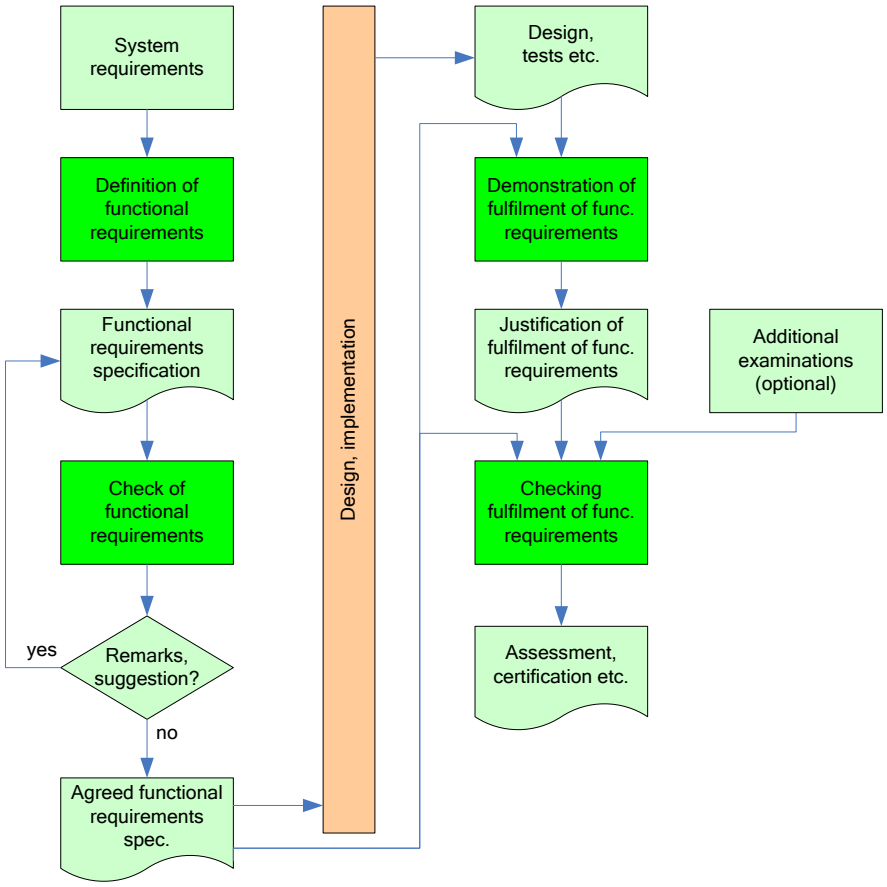


Figure 9 – Generic AAC process at the level of functionality

4.1.3 Generic AAC process at the level of safety

Safety requirements can be defined based on the functions of a system, using a hazard and risk analysis. In case of safety requirements there is a strong need to check, whether the safety requirements were defined in an appropriate way and the results are acceptable. The agreed safety requirement specification is a clear basis for later design and implementation phases, as it determines system architecture properties as well as the methods that shall be used during the development.

The supplier of the system has to demonstrate that the safety requirements are met. This demonstration or justification must be usually assessed before it can be stated that all safety requirements are fulfilled. The Independent Safety Assessment follows the whole development process, and can result in an assessment report. This report can be used in course of system approval.

The whole process is depicted in Figure 10.

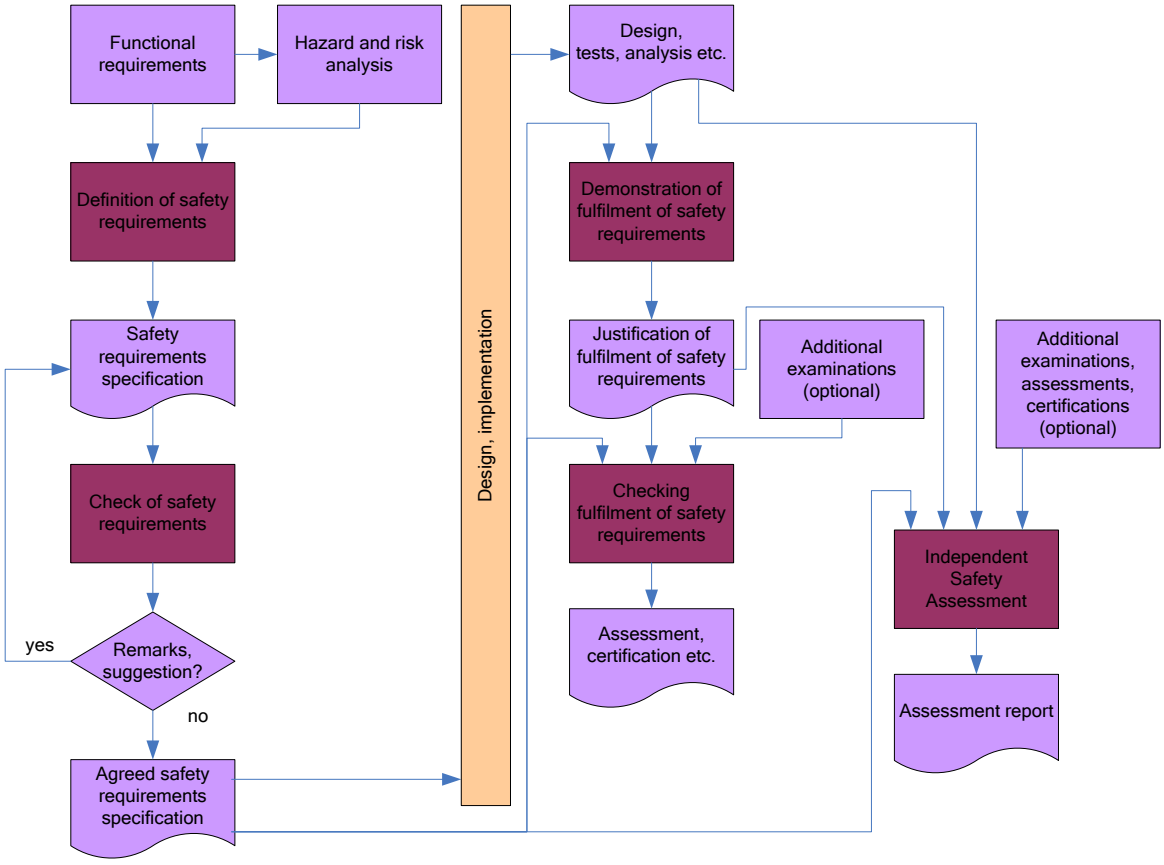


Figure 10 – Generic AAC process at the level of safety

4.2 Allocation of EAMs to main participants of the processes

In this sub-clause the EAMs, identified in [MODSafe D7.2] are allocated to the main participants of acceptance, approval and certification procedures. These participants were identified in [MODSafe D7.1] as follows (some of them are optional):

- the operator
- the supplier,
- the authority,
- an Independent Safety Assessor and/or an Independent Certification Body.

For the possible link of activities to participants a table is used, showing all elementary activity modules and all the participants. The sequence of the EAMs follows the timeline of the lifecycle phases, as described in [MODSafe D7.2]. In the table, as it is a generic allocation only the responsibility is shown. Different practices of different countries (based on the case studies) are also marked (with the abbreviation of the given country). This means that the table contains common practices in Europe as well as differences. Common practices are marked with green background colour in the adequate cells.

The type of allocation is also shown in Table 8 below. This can be a ‘legal obligation’ (resulting from a law or act etc.), it can be originated from a contract or it can be a ‘good practice’. If an activity is not common in every country, then it is also remarked.

		Participant			
EAM	**Type of allocation/ comment**	**Operator (AOT in France)**	**Supplier**	**Safety Authority**	**Independent Safety Assessor or Certification Body**
Definition of system requirements	legal obligation	Resp.			
Check of system requirements	not common (e.g. not in S)	Resp. (F)	Resp. (UK)***	Legal resp. (D, H)	Good practice resp. (UK)
Definition of functional requirements	legal obligation	Resp.			
Check of functional requirements	not common (e.g. not in S)	Resp. (F)	Resp. (UK)***	Legal resp. (D, H)	Good practice resp. (UK)
Definition of safety requirements	legal obligation	Resp.			
Check of safety requirements	legal obligation	Resp. (UK)	Resp. (UK)***	Resp. (D, F, H, S)	Good practice resp. (UK)
Demonstration of fulfilment of safety requirements	legal obligation		Resp.		
Check of fulfilment of safety requirements	legal obligation	Resp. (F)	Resp. (UK)***	Resp. (D, F, S)	Resp. (F****, UK, H)
Demonstration of fulfilment of func. requirements	contract		Resp.		
Check of fulfilment of functional requirements	not common (e.g. not in S)	Resp. (F)	Resp. (UK)***	Resp. (D)	Resp. (H)
Demo. of fulfilment of sys reqs/ test operation	contract	Resp. (shared)*	Resp. (shared)*		
Check of fulfilment system req.	contract and/or legal obligation	Resp. (F, H, UK)	Resp. (UK)***	Resp. (D, S)	Resp. (H)
Independent safety assessment	legal obligation or good practice				Resp. (ISA)
Approval	not always formal (e.g. Belgium)	Resp. (UK)**		Resp.	

Table 8 - Generic allocation of EAMs to participants

* the operator and the supplier are working together as a project team, which is within the operating company, with different responsibility
** operator in the UK acts as Safety Authority, refer to sub-clause 3.5.
*** in UK Project Delivery Team and Supplier are responsible for check of safety requirements, functional requirements and system requirements
**** in France system parts can sometimes be certified by a certification body

4.3 Typical activities of participants

According to the results of sub-clause 4.2 in this sub-clause the typical activities of different parties is demonstrated. Note that this demonstration is based on common practices; however differences in some countries are still possible.

4.3.1 Operator

In a generic AAC process the operator has to perform the following EAMs (marked with colours):

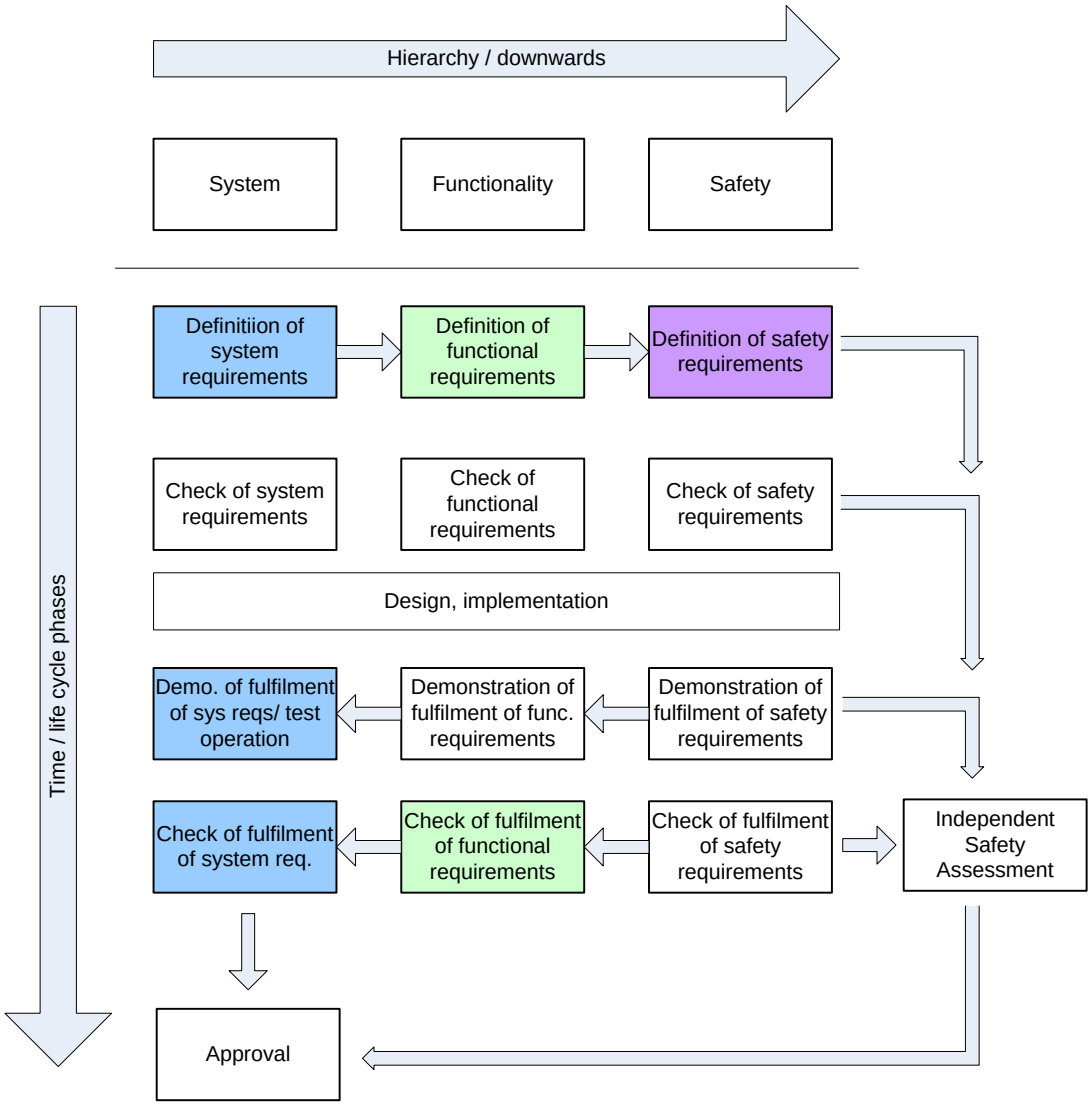


Figure 11 – Generic tasks of operators

4.3.2 Supplier

In a generic AAC process the supplier has to perform the following EAMs (marked with colours):

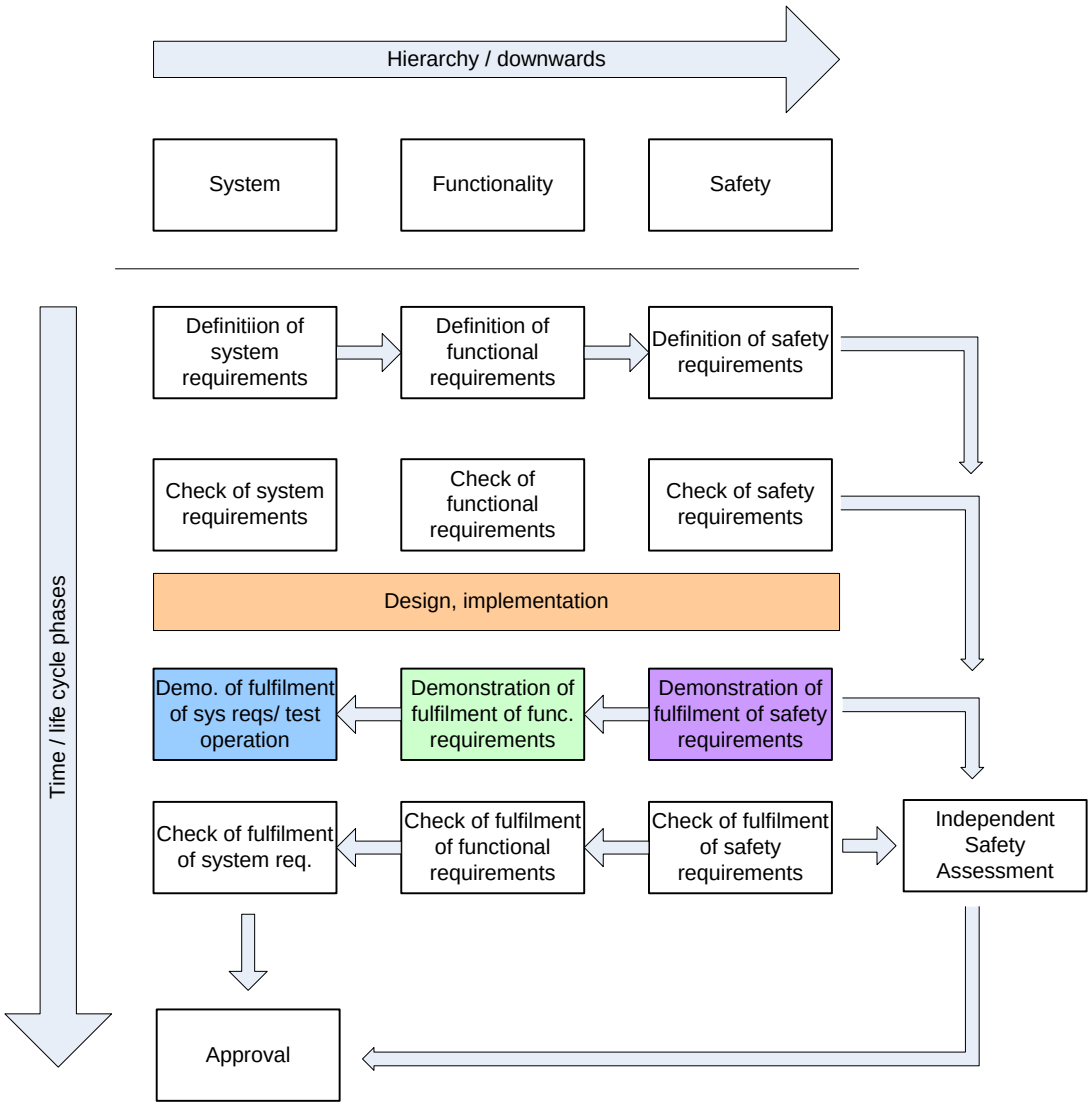


Figure 12 – Generic tasks of suppliers

4.3.3 Authority

In a generic AAC process the authority has to perform the following EAMs (marked with colours):

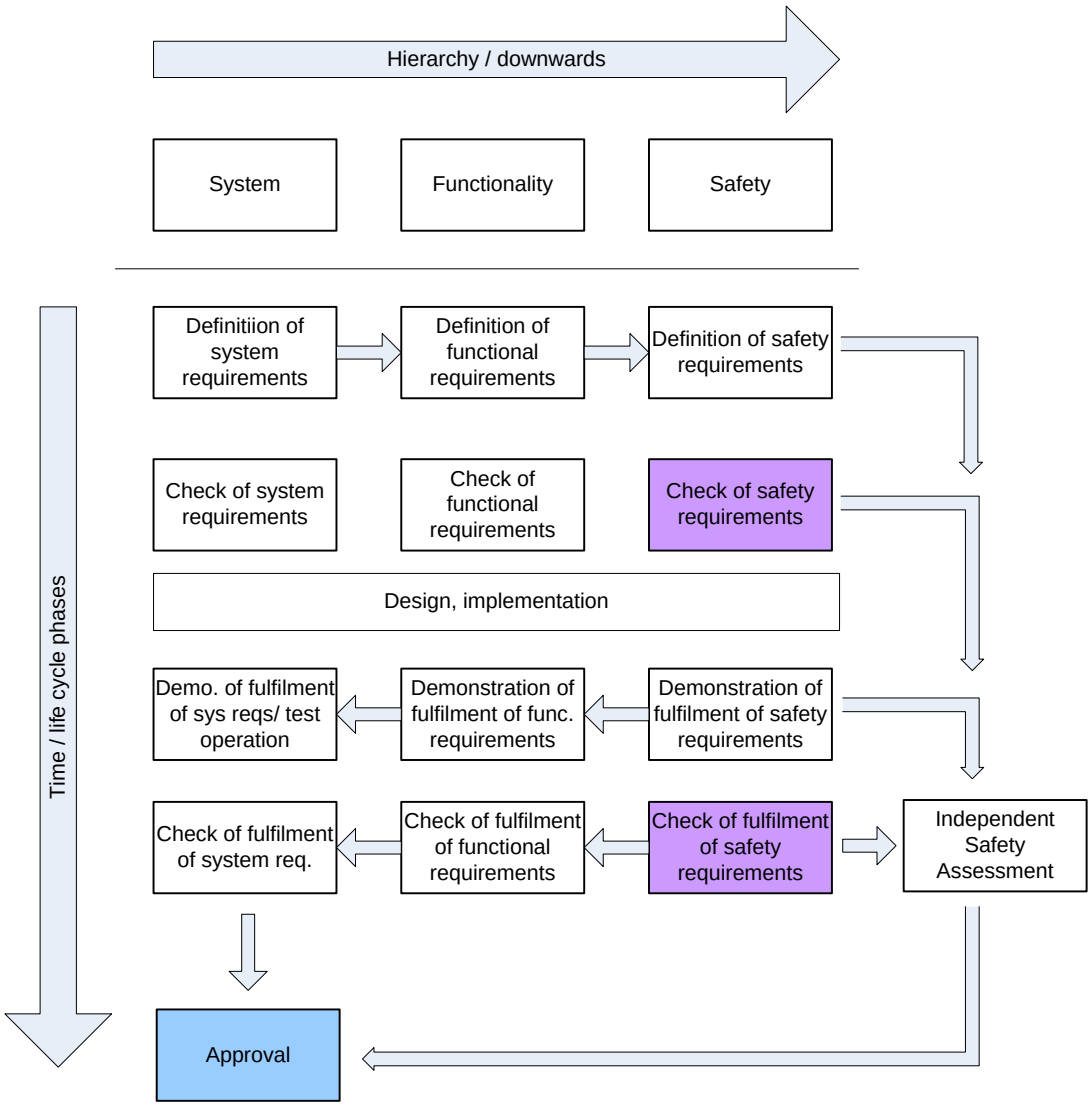


Figure 13 – Generic tasks of an authority

4.3.4 Independent Safety Assessor or Certification Body

In a generic AAC process the independent body, typically an Independent Safety Assessor has to perform the following EAMs. The striped colouring designates typical activities that can be performed either by the ISA or the certification body, whereas full colouring designates the activity that can only be performed by the ISA.

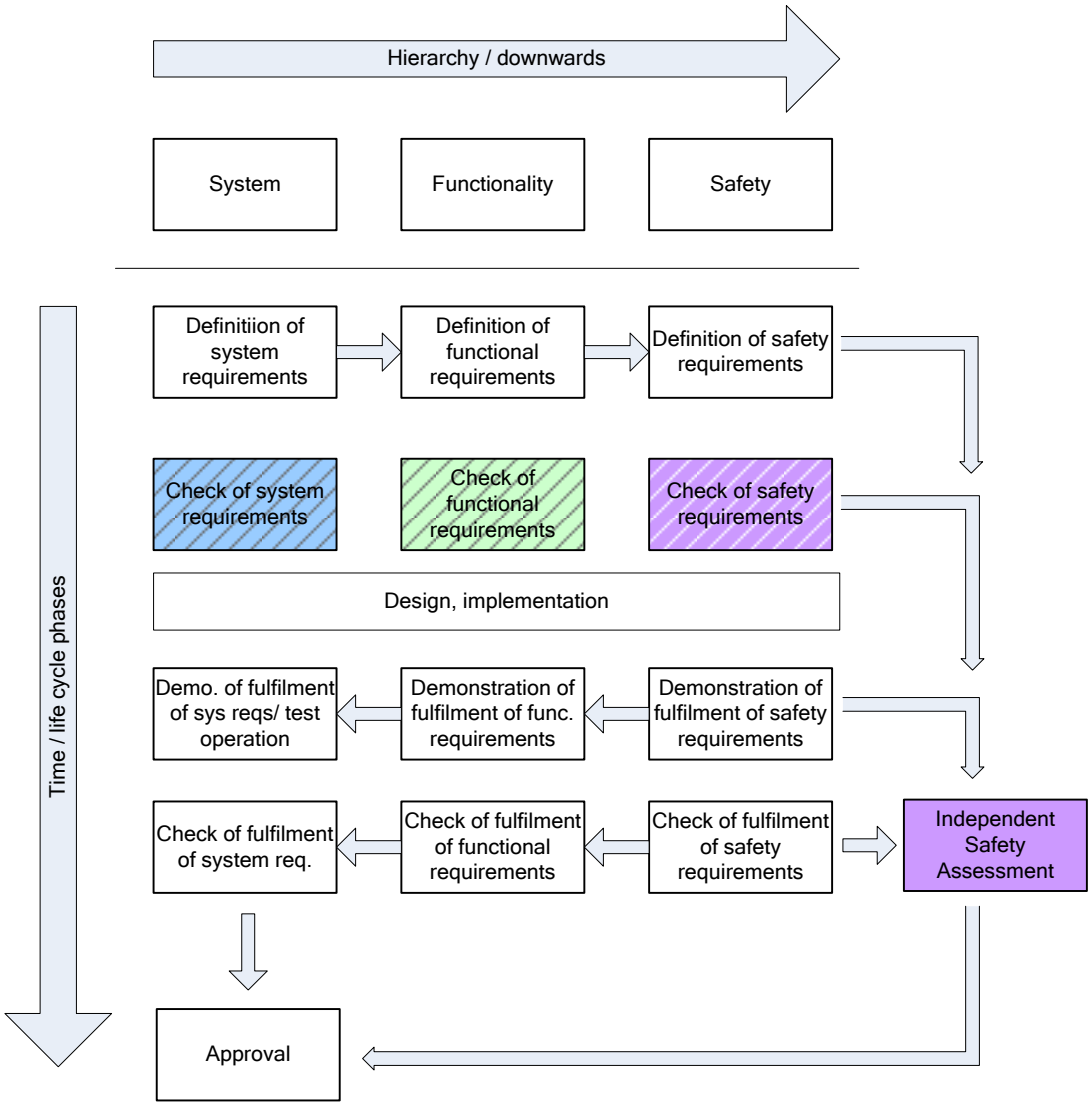


Figure 14 – Generic tasks of independent bodies

4.4 Qualification of independent bodies

An important issue is in AAC procedures the necessary qualification of independent bodies, such as certification bodies or Independent Safety Assessors. This sub-clause gives an overview about some qualification criteria for

- Inspection Body according EN ISO/IEC 17020 [EN ISO/IEC 17020]
- Certification Body according to EN 45011 (ISO/IEC Guide 65, will be substituted by EN ISO/IEC 17065 by mid of 2012) [EN 45011]
- Independent Safety Assessor according CENELEC standards for railway applications [CENELEC]

4.4.1 Inspection Body

Main qualification criteria of an inspection body are the credible demonstration of competence, independence, impartiality and integrity. This has to be demonstrated towards a national accreditation organisation of the country (e.g. DAkkS in Germany or UKAS in the United Kingdom) in which the legal entity is registered.

In general the personnel of the inspection body shall be free from any commercial, financial and other pressures which might affect their judgement. Procedures shall be implemented to ensure that persons or organisations external to the inspection body cannot influence the results of inspections carried out.

The independence shall be assured to the extent that is required with regard to the conditions under which it performs its services. It is distinguished between three normative types of inspection bodies:

Type A:

- providing third party services,
- the inspection body shall be independent of the parties involved,
- shall not engage in the design, manufacture, supply, installation, use or maintenance of the items inspected, or similar competitive items,
- all interested parties shall have access to the services of the inspection body,
- there shall not be undue financial or other conditions,
- procedures shall be administered in a non-discriminatory manner.

Type B:

- forms a separate and identifiable part of an organization involved in the design, manufacture, supply, installation, use or maintenance of the items it inspects and has been established to supply inspection services to its parent organization (in-house services),
- clear separation of the responsibilities of the inspection personnel from those of the personnel employed in the other functions,
- shall not engage in the design, manufacture, supply, Installation, use or maintenance of the items inspected, or similar competitive items,
- inspection services shall only be supplied to the organization of which the inspection body forms a part.

Type C:

- is involved in the design, manufacture, supply, installation, use or maintenance of the items it inspects or of similar competitive items and may supply inspection services to other parties not being its parent organization (in house),
- shall provide safeguards within the organization to ensure adequate segregation of responsibilities and accountabilities in the provision of inspection services.

4.4.2 Certification Body

Main qualification criteria of a certification body are the credible demonstration of competence, independence, impartiality and integrity. This has to be demonstrated towards a national accreditation organisation of the country (e.g. DAkkS in Germany or UKAS in the United Kingdom) in which the legal entity is registered.

In general the personnel of the certification body shall be free from any commercial, financial and other pressures which might affect their judgement. Procedures shall be implemented to ensure that persons or organisations external to the certification body cannot influence the results of evaluations carried out.
The certification can only be performed by a third party and independent legal entity.

4.4.3 Independent Safety Assessor (ISA)

There are no legal requirements or accreditations schemes to be recognized as ISA or assessment organisation. An assessor may be a single person or a legal entity (assessment organisation).
According CENELEC Guide for EN 50129 – Part 2 [TR 50506-2] the safety authority shall accept the ISA or the safety assessment organisation. The independent safety assessor could be either a member of the in-house organisation (e.g. assessment centre) or an independent external organisation. The degree of the independence of the assessor from the development and RAMS process shall be proven and accepted by the safety authority in charge of the approval. The assessment organisation should have an accreditation in accordance with EN ISO/IEC 17020.

5 Conclusion and further work

In this deliverable a typical AAC model was introduced. The model is based on practical experiences gained from different case studies. It was shown that the Elementary Activity Modules (identified in [MODSafe D7.2]) can be applied for the description of different acceptance, approval and certification processes. Furthermore the EAMs were linked to the participants of AAC processes.
The typical processes at different levels of system hierarchy (system, functionality and safety) are described with help of EAMs (sub-clause 4.1). Based on a comparison and compilation a typical allocation of EAMs to participants was provided (sub-clause 4.2), and based on this typical roles and responsibilities of different partners in different EAMs are also presented (sub-clause 4.3.).

5.1 Outlook to D7.4

In the final deliverable of work package 7, a typical, optimised AAC process is proposed, with a core process and with optional, additional activities linking to the core process. For the description of this optimised process the EAMs are applied.

In D7.4 first the main technical factors are identified which have impact on AAC procedure. Such factors include:

- the type of the system (tramway, metro or light rail),
- the complexity of the system (i.e. number of subsystems),
- level of safety,
- grade of automation (GOA),
- existing and already in operation system or a completely new system,
- in case of system modifications: the relevance of change (minor/major),

Following the identification of the impact factors a core process is proposed, as a minimum requirement for AAC procedures of UGT systems. The core process is composed from the mostly used EAMs. After this the impact of different factors on the core process is investigated. In course of this it is examined how the factors influence the process, i.e. which additional activities (EAMs) are necessary e.g. for higher level of safety and which independency of different parties is required in different cases. This allows proposing different processes for different types of systems, for different complexity, safety etc. An optimal allocation of tasks to different participants is discussed as well as the involvement of the authority. Regarding the involvement of the authority, the legal basis of the appointment and the role of the authority in managing risk criteria is also discussed.