MODSafe – Modular Urban Transport Safety and Security Analysis

Abstract

MODSafe – Modular Urban Transport Safety and Security Analysis – is a European project in the European Transport sector under the Seventh Framework Programme (FP7) for Research and Technological Development of the European Union.

The main purpose of the MODSafe project is to undertake research on major steps of the Safety Life Cycle of "Urban Guided Transport" (UGT) systems (covering Light Rail Systems, Metros and Trams) in Europe. Even if the rail safety landscape in urban guided transport is highly diversified, the sector should benefit from some kind of harmonization. Furthermore, security items are analysed in MODSafe as well since they are considered more and more as vital for the urban transport sector. The 22 partners are from industry, associations, R&D organisations, consultants and operators.

The MODSafe project successfully started in 2008 with state of the art evaluations and initial models. Hazard analyses, safety requirements as well as functional and object models have been developed together with a safety life cycle approach proposal and a generic acceptance, approval and certification proposal. As regards the security sector, the existing means and technologies for security systems have been analysed, and strategies and measures for improvement have been defined.

As an outlook to the project closure in August 2012, one can expect reasonable suggestions for the future, aiming to contribute to the European drive for harmonisation and to simplify the upgrade or new construction of urban guided transport systems. Cross-Acceptance is also one of the key attempts of all parties involved, manufacturers and suppliers, operators or safety authorities. This paper briefly presents the MODSafe key findings and results.

1. Introduction

In Europe, light rail, metros and trams are characterized by a diversified landscape of safety requirements, safety models, roles and responsibilities, safety approval, acceptance and certification schemes; however, there are convergences between some architectures and systems.

There are no standardized procedures at the European level for bringing urban guided transport systems 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 railway application standards EN 50126/50128/50129 currently under revision.

Urban guided transport stakeholders believe that the development of European (and even worldwide) references to be used on a voluntary basis should be encouraged, in order to facilitate the decision making process involving relevant national authorities and the various stakeholders. The MODSafe project aims at delivering guidance targeting safety and security aspects in that regard.

MODSafe has been structured in multiple work packages related to the key aspects which are:

- safety (hazard analysis, hazard mitigation measures / safety functions, allocation of safety requirements, function and object model / allocation of safety functions to technical objects),
- processes (life cycle and approval, acceptance and certification) and
- security.

The work packages start with a survey on the state of the art (standards, methodologies, results from previous projects, proven praxis from industry and operation, experience from other sectors, etc.) throughout the European countries. The state of the art results and additional findings are compared to identify the differences and similarities, the potential gaps and synergies. Finally, respective suggestions are made for the future in the light of the project objectives.

2. Survey, Comparison and Suggestions on Safety

Aiming to facilitate approval and certification of urban rail technologies and cross acceptance within the European Community requires comparable safety targets and measures. The initial steps of an urban guided transport system life cycle from a safety perspective are the risk analysis and modelling tasks, forming the base for the safety requirements of the urban guided transport system and / or its sub-systems. The initial survey looks at the state of the art for the risk analysis approaches in the EU.

The following sections provide a brief description of the results of the safety survey and comparison, starting with a preliminary hazard list and compilation of mitigation measures / safety functions to cope with these hazards, followed by an allocation of safety requirements and typical system architecture / function and technical object model.

The initial MODSafe objective was the preparation of a Preliminary Hazard List as an input for a preliminary hazard analysis used for identifying at the system level its safety critical areas. The concept and methodology of a hazard analysis have been outlined, and existing hazard analyses used in the European transportation sector by operators, suppliers and research institutes have been reviewed. Furthermore, results from European research projects have been screened. Information has then been consolidated into a shared preliminary hazards analysis concept, methodology and database.

Obviously, MODSafe could not check all failure modes and possible hazards leading to a failure in all grades of automation and for all existing operating systems. However a method has been presented on how to check a more specific hazard analysis for consistency.

In modern urban guided railway systems the responsibilities of operation staff and the man based procedures are more and more replaced by technical tools and software. Therefore, the basic functions of train operation for the different Grades of Automation (GOA) have been considered. The safety model as shown in the following figure starts with the identification of hazards within normal system operation.

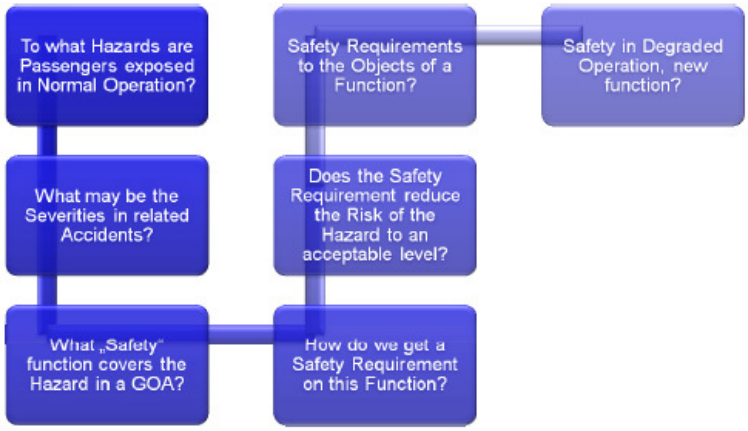

Figure 1: MODSafe Safety Model

To each hazard, a related accident category is determined and the severity of this accident is evaluated. Furthermore, generic functions are determined that cover the hazard. Realizations of this safety function can be matched to different Grades of Automation in order to facilitate the application of the hazard analysis to a specific operation system.

The main results achieved are a consistent final hazard analysis and the corresponding risk analysis. The hazard analysis deals with the global urban guided transport system including train, traction power system, track, station equipment, passenger information system, communication system, control/command and supervision of train movement system, etc.

In order to specify hazard control / mitigation measures (i.e. safety measures, safety functions or risk reduction measures) which would cope with the hazards identified, the existing generic safety functions identified from previous EC projects and other generic safety functions of the supply industry have been mapped against the hazard and risk analysis. The result is the hazards control and safety measures analysis. The mitigation measures employed to eliminate or control the risk can be either design measures or operational or maintenance processes and procedures. For each hazard within the scope of this analysis, it has been possible to find corresponding mitigation measures and safety functions. To some extent also non-technical safety measures like procedures were described.

The next step is the allocation of safety requirements to safety measures / safety functions. Based on an initial survey allowing to compare the risk analysis and safety requirements allocation methods of various standards and national regulations and based as well on the compilation of results of previous projects (MODURBAN, MODTRAIN), an analysis of safety requirements for continuous safety measures and functions as well as the equivalent for low-demand functions has been developed. The concept of Safety Integrity Levels (SIL) is used as a means of creating balance between measures to control random failures and to prevent systematic faults (see figure below). Safety Integrity Levels are used to group methods, tools and techniques which, when used effectively, are considered to provide an appropriate level of confidence in the realization of a system to a stated integrity level.

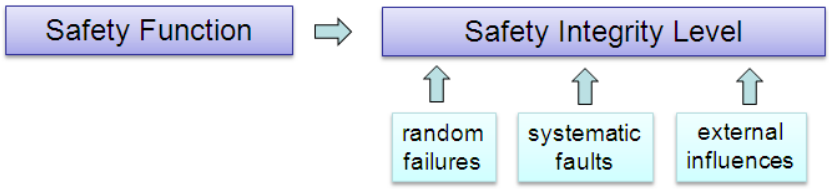

Figure 2: Concept of Safety Integrity Levels

Quantitative methods use exact (or ranges of) numerical values as an input for the calculation of safety targets, e.g. hazard frequency can be expressed in terms of events per hour, while qualitative approaches are using parameters to estimate risk, which are described in words, rather than exact numerical values, e.g. severity of consequences terms like catastrophic or critical. Methods using a risk based approach use parameters to describe risk (verbally or numerical value).

The level of risk is determined to derive safety requirements in form of safety integrity levels, using the risk graph or the risk matrix describing risk according to parameters. Alternatively, safety targets may be derived using reference systems. Another method is to calculate or estimate a global safety target and to break it down to functions defined for the system.

Deriving safety requirements / safety integrity levels according to the risk posed by a hazard or a failure of a continuous safety function, parameters are considered to estimate risk, namely the hazard occurrence frequency or severity of hazard consequences and other parameters like passenger exposure time, accident and consequence reduction possibilities. Risk reduction measures can be determined appropriately.

For low-demand functions, a safety integrity requirement allocation scheme can be used to determine a safety integrity level equivalent safety requirement, in terms of a maximum wrong side failure rate of the safety function. Determining an integrity level for a low demand mode function means, to first determine approximately the occurrence rate for the potentially unsafe event and its consequences and from this determine the integrity requirement as the probability value for the protection/safety system. Finally, the corresponding relation between wrong side failure rate and inspection / repair rate can be adjusted as needed.

Finally, MODSafe has developed a typical urban guided transport functional model, an object model (the technical objects performing the safety functions) and a combined object/-functional urban guided transport model. The origin of the majority of the MODSafe safety functions is the international standard IEC 62290 Railway applications - Urban guided transport management and command/control systems - Part 2: Functional requirements specification. The following figure shows an example of the main clustering of functions.

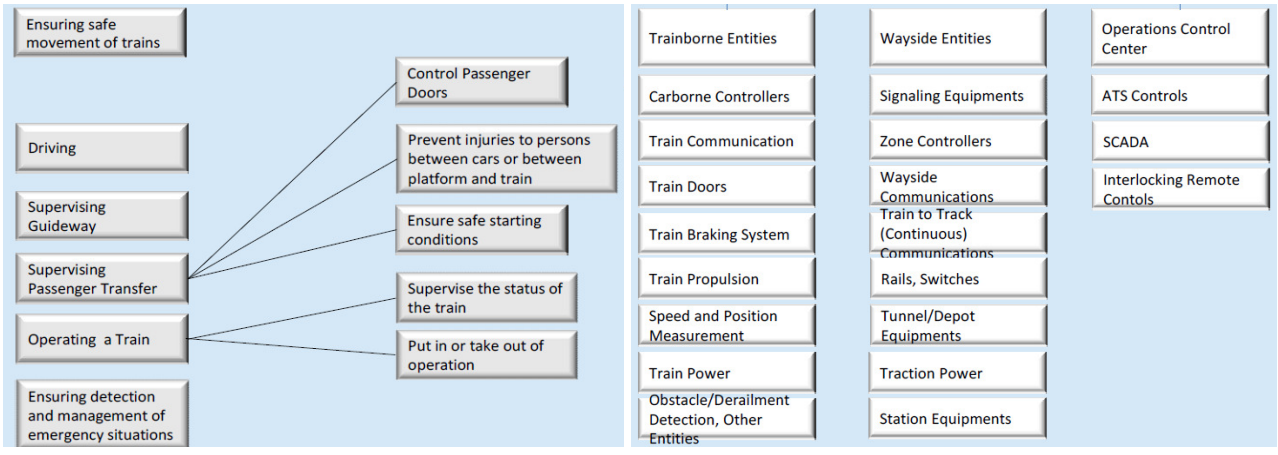

Figure 3: Functional Model and Object Model (extract)

For every function (in a certain Grade of Automation), all objects are screened. If it appears plausible, that an object may interfere in the realization of a function, then it is linked ("associated"). The selection of objects does not mean that the functions must consist of these objects. It shall rather express that if the object is used for the realization of the function, then it must respect the safety requirement of the Function or demonstrate to be

free of safety relevance for the function. The generic linking is therefore “over complete” in the sense, that it represents the maximum of possibly interfering objects and – for a concrete architecture – is likely that only a subset of the selected objects are retained. As a result, the link between the functions and the technical objects are arranged in the form of an allocation matrix, which is intended for use of operators and suppliers when it comes to technical realisation.

In conclusion it can be stated, that the MODSafe safety deliverables and suggestions - made of a preliminary hazard list, a list of typical mitigation measures / safety functions, an allocation of safety requirements / safety integrity levels and a mapping to a typical functional / object model - form a sound model reference and base for new or modified urban guided transport systems and its sub-systems, supporting the aim of facilitating systems certification and increasing future cross-acceptance throughout Europe.

3. Survey, Comparison and Suggestions on Processes

Aiming to enhance cross acceptance also requires comparable urban guided transport system life cycle approaches and processes for acceptance, approval and certification (AAC). The initial survey on processes looked at the state of the art for the safety lifecycle approaches in the EU, revealed the regulation background and analysed the main phases of the safety lifecycles. The comparisons then specifically seek to find differences and / or similarities in the processes of the different countries. The following sections provide a brief description of the results of the survey and comparison.

Safety Regulatory Authorities are in most cases orderly appointed on national or regional level. Where no respective authority is in charge, the regional government is in control. Countries with federal structures often have appointed Safety Regulatory Authorities on regional level for each federal state. Nearly every country follows rules and regulations for system approval, and differences lie in how to achieve this goal. Most often acts and decrees / regulations give guidance, sometimes in combination with European and / or national standards. The approval is sometimes regulated by standards only or by special rules and practices. Consequently, the activities of the appointed Safety Regulatory Authority are not uniformly spread within Europe. Liability for safety & orderly operation is mostly dedicated to the operator / responsible person / infrastructure provider.

In summary it can be stated that Safety Regulatory Authorities appointed to urban guided transport are commonly in use, and that their involvement differs in range and depth.

The legal basis is generally given with acts, royal decisions, decrees or regulations. The highest level of legislation is given by laws / acts in multiple countries. On the next lower level decrees and regulations have been established, specifying roles & responsibilities, processes & procedures, defining targets & requirements and partly referring to standards (e.g. from CENELEC). Some countries share a common basis. Other countries' decrees / regulations are exclusively in use on national level. In addition or exclusively, National standards / rules & guidelines, both for overall metro/light rail/tram systems and sub-systems such as Rolling Stock and Signalling may apply. The following "legislation pyramid" indicatively depicts the hierarchy of legislation with the related acts, decrees / regulations and standards in use.

In summary it can be stated, that a legal basis for the Safety Regulatory Authorities is mostly given with acts or decrees / regulations.

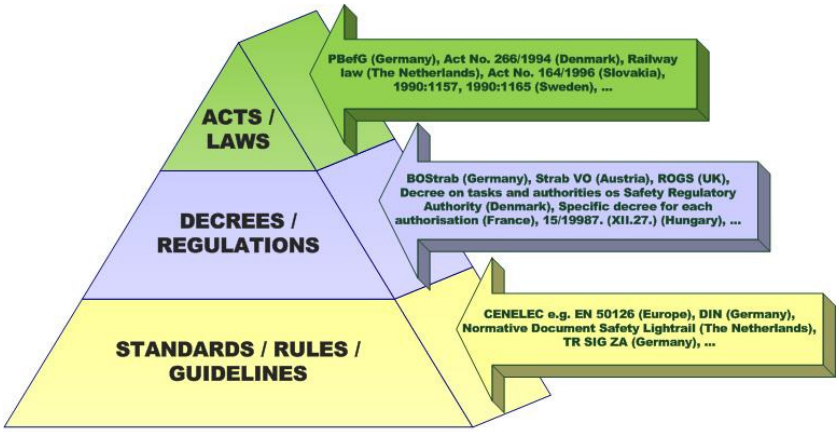

Figure 4: Legislation pyramid

A different degree of regulation was found throughout Europe. Safety Regulatory Authorities of countries with a high degree of regulation have detailed procedures in place, deviating in range, others have less detailed procedures. A country with a lot of experience in passenger service (light rails, metros and trams) and highly advanced systems (driverless operation) might have a higher complexity of regulation. It was found that light rail, metro or tram systems are not uniformly treated in terms of approval process and requirements. Procedures on installation & operation are not uniformly regulated but in practice commonly in use with a different level of operator involvement.

In summary it can be stated, that the degree of regulation differs throughout the countries and varies in scope and deepness depending on the nature of the system (light rails, metros or trams), grade of automation and with different level of involvement of Safety Regulatory Authorities and operators.

A trend on application of the CENELEC Standards was found throughout the European countries when matching the typical urban guided transport system phases with the life cycle phases of these standards. The typical phases “system conception and specification”, “design and manufacturing”, “installation and commissioning” and “operation and maintenance” were found to be easily linkable to the fourteen life cycle phases of EN 50126. Further survey results are that risk mitigation has to be addressed for obtaining system approval, but there is no common or regulated approach, although CENELEC gives guidance, and the involvement of an Independent Safety Assessor is not uniformly regulated but in practice commonly in use. Same applies for Verification & Validation activities prior to operation, acknowledging that the performance along the lifecycle differs in scope and depth. Examples can be given for cross-acceptance at European level. The CENELEC standards and their guidelines contribute to this increasing harmonisation.

In summary it can be stated, that CENELEC Standards are commonly – although not systematically - used as guidelines for obtaining system approval of urban guided transport systems.

Consequently, the proposal of a generic life cycle approach for urban guided transport systems is based on the CENELEC Standards and considers the interfaces between the different life cycle phases and respective phase related responsibilities.

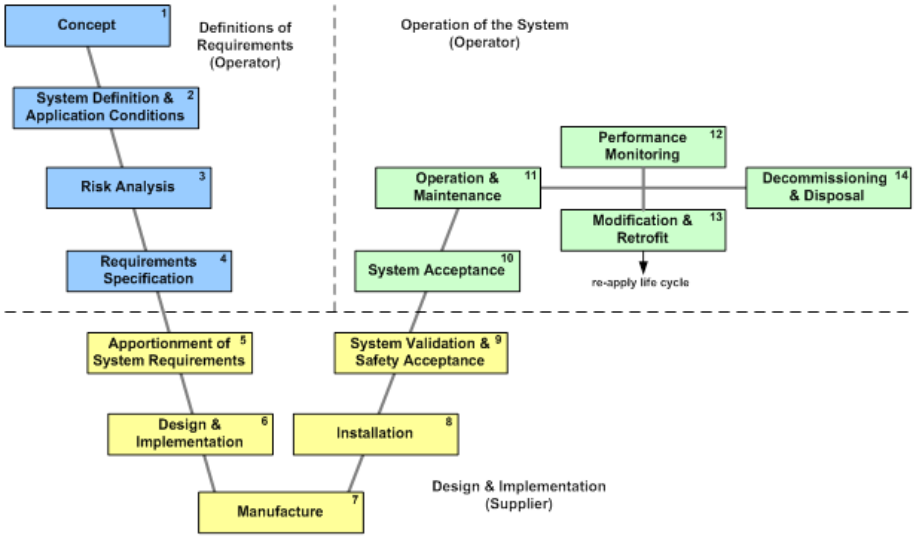

Figure 5: Life Cycle proposal

The survey identified that the acceptance, approval and certification procedures are characterised by high diversity. Diverse actors are involved and different procedures and different roles are applied in the field of urban guided transport systems. The diversity relates also to functional and safety requirements, safety models. Nevertheless various similarities can be observed.

Based on the analysis of various case studies selected from European countries, it was shown that certain activities are comparable, independently from which party is performing the activity and when and how much in detail. As an outcome of the MODSafe analysis and comparison, so-called elementary activity modules (definition of system/functional/safety requirements, demonstration of compliance thereof) have been identified which as part of the life cycle proposal.

For the proposal of a Generic Process for Acceptance, Approval and Certification, the elementary activity modules were assigned to the main actors in the process (namely the operator, the supplier, the authority and the independent safety assessor) to form the base for optimisation (e.g. optimisation depending on the Grades of Automation, the handling of different systems such as metros or trams, the focus on either the entire urban guided transport system or its technical sub-systems such as rolling stock or signalling.) The identified elementary activity modules are used for the depiction of the processes in so called cross-functional flow charts shown in the figures below.

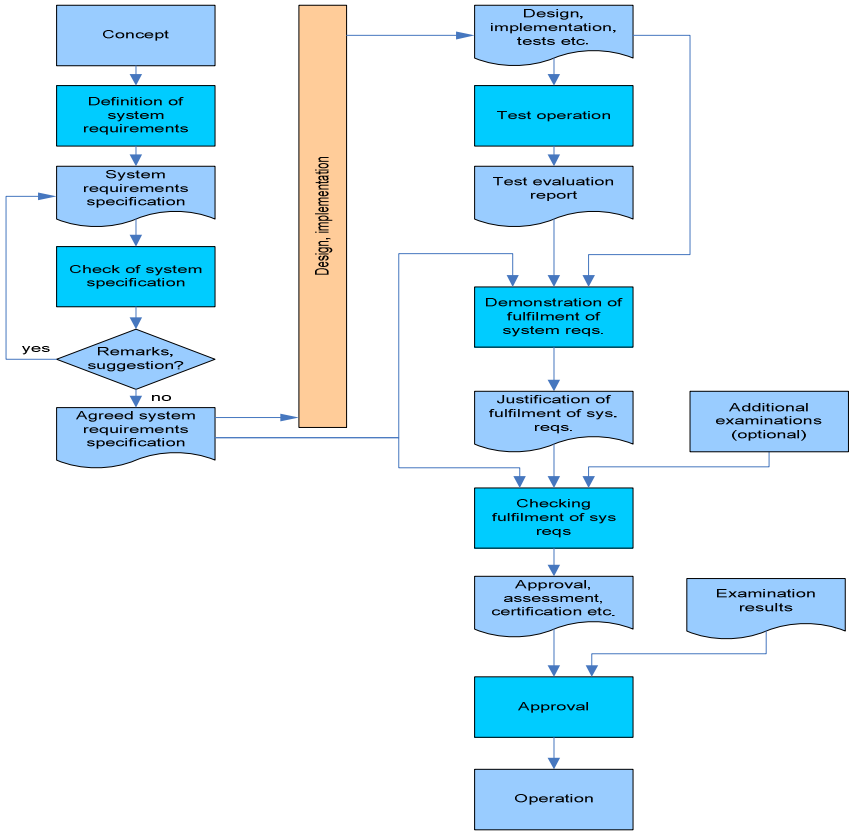

Figure 6: Generic Process proposal for Acceptance, Approval and Certification

Based on the generic process and elementary activity modules, it can be outlined that so far in Europe certain elementary activity modules

- are always performed and are performed always by the same participant (fixed allocations)
- are always performed, but they are performed by different participants/ organisations according to the different practices of different countries (variable allocations),
- are not performed in every case or not performed as formal responsibility (optional elementary activity modules).

The suggested allocation of responsibilities - depicted in the following figure - is therefore based on elementary activity modules, which are almost always performed. Generic roles and responsibilities of different parties in the acceptance, approval and certification processes are detailed in the figure, coming along with a description of the legal basis, the key roles and responsibilities as well as the typical activities. The variable allocation elementary activity modules and the optional elementary activity modules provide a "playground" for a case to case adaptation of AAC processes.

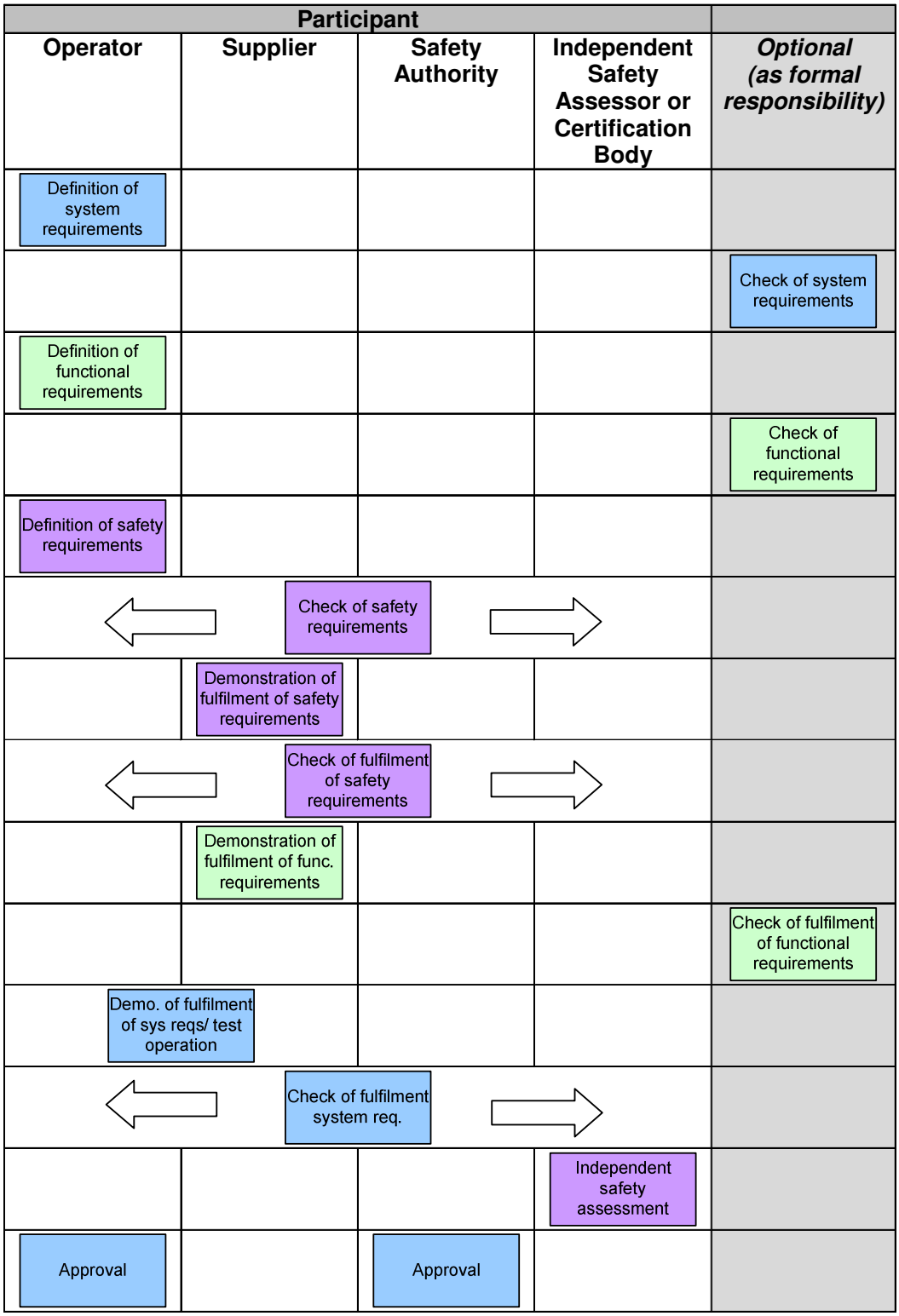

Figure 6: Generic Core Process proposal for Acceptance, Approval and Certification

4. Survey, Comparison and Suggestions on Security

The security survey described the state-of-the-art and identified best practices by reviewing across Europe the existing security policies, procedures, methodology and technologies supporting transport security in urban systems, as well as in aviation and long distance rail operations.

The security survey is based on the outcomes of some European projects in which operators played a significant role, in particular COUNTERACT (Cluster Of User Networks in Transport and Energy Relating to Anti-terrorist ACTivities). COUNTERACT is a European project funded under the Sixth Framework Programme whose main objective was to improve security against terrorist attacks targeting public passenger transport, intermodal freight transport and energy production and transmission infrastructure. Inside the project, a review of existing security policies, procedures, methodology and technologies to identify the best practices has been performed.

MODSafe listed countermeasures linked to person's integrity (passengers, staff and infrastructure) and associated technologies, in order to prevent crime in general and to respond to any kind of criminal acts. With regard to rail transport, research has shown that there is no specific European legislation. Moreover, differences between security measures and technologies for urban guided systems compared to long distance rail systems can be identified.

Consequently, the survey and comparison showed that countermeasures and technologies vary from one sector of activity to another and are often not comparable. The technologies implemented for example in aviation security domain are not usually adaptable to urban guided transport systems as many of them are strictly related to the structure of airports and aircrafts and their intrinsic characteristics.

Based in an initial review of existing means and measures for security systems, the work focused first on the assessment of the relevant regulations and norms implemented at the European Union and member state levels. This analysis has shown that a very limited level of standardisation specific to security has been achieved at the European level with regard to public transport and to the rail sector, either for heavy rail or for urban rail systems.

In the next step of work, the existing technologies for prevention have been evaluated. In particular:

- all type of laws and legal requirements, their hierarchical level and interdependencies,
- techniques, methods and tools used by the operators and manufacturers to satisfy legal requirements,
- technologies considering all levels of means and measures for preventive actions.

The works resulted in guiding principles for security and emergency prevention and management in terms of proposals and recommendations and high end considerations inclusive of terrorism, cyber warfare, organized crime and everyday crime - towards potential future harmonisation and standardization in the security section.

Further analysis of threats related to security aspects and classification of risks associated to security aspects resulted in the determination of possible means in order to mitigate the relevant risks. The analysis resulted in a list of security threats which relate to any kind of crime and malicious actions perpetrated within the limits of the urban rail guided transport system (including fight against terrorism). Threats covered are those linked to person's integrity (including customers and staff of the rail company), threats to the rail systems assets and property of the rail operator and threats to information systems used in the public transport network.

The analysis of threat-related scenarios and subsequent critical infrastructure components in Urban Guided Transport systems focused on physical security, the part of security concerned with measures and concepts designed to safeguard personnel, prevent unauthorised access to equipment, installations, materiel, and documents and safeguard them against espionage, sabotage, damage and theft (including cyber security).

The identification of all security means and measures which relate to the threats in Urban Guided Transport Systems (including terrorism, cyber threats, organized crime and everyday crime) looked into various European policies, communications and reports as well as dispositions adopted by Member States (e.g. decrees, directives, policies and anti-terrorist plans) and proposed means and measures for improved Urban Guided Transport Systems in a top-down approach from the corporate level (PTO, police forces, agencies, private security) to the field level.

This analysis of the existing threat scenarios in the urban guided transport sector related to security aspects revealed some needs, which were used as the base for the proposals for mitigating security risk and threats. A comparison and structuring effort delivered terms and abbreviations related to security in UGT systems; lists of potential threats, targets and threat-related scenarios; means to extrapolate critical infrastructure components in the same; and recommendations.

The final results are urban guided transport security fundamentals in terms of proposals and recommendations for security strategies and security means and measures for Urban Guided Transport systems towards potential future harmonisation and standardization in the security section.

5. Conclusion and Outlook

The MODSafe overall objective was to provide guidance on how to improve the functioning of the internal market through recommendations on safety and security issues which would be applicable to all Urban Guided Transport operators and which would at the same time let competent authorities adapting them to the particularities of their local situation. At the end of the project, it can be ensured that the application of the MODSafe work packages' deliverables and outcomes will provide adequate support for manufacturers, operators and safety authorities in that regard.

The MODSafe results may also influence the potential future voluntary standardisation for Urban Guided Transport. MODSafe however also shows the limits of standardization for technical safety functions and objects, as pointed out during the consensus building process.

More generally, the networks and connections created for this project (e.g. network of operators, urban rail suppliers as well as transport research institutions and other related parties like an independent safety assessor) help to establish an ongoing, target-oriented discussion, to reveal common goals and to allow for a better understanding of different European procedures and needs.

MODSafe provides reasonable suggestions for the future, aiming to simplify the upgrade / modernization or new construction of urban guided transport systems and sub-systems, and to facilitate cross-acceptance of products for the benefit of all parties involved.

References

ModUrban D93 - ModUrban Deliverable Report D93

Conformity Assessment, Guidelines for Functional and Technical Specifications

MODSafe Modular Urban Transport Safety and Security Analysis
Deliverable D2.2 - Consistency Analysis and Final Hazard Analysis

Deliverable D2.3 - Risk Analysis

Deliverable D3.2 - Hazard Control and Safety Response Measures Analysis

Deliverable D4.2 - Analysis of Common Safety Requirements Allocation for continuous safety functions

Deliverable D4.3 - Analysis of On Demand Functions and Systematic Failures

Deliverable D5.1 - Urban Guided Transport Object Safety Model

Deliverable D5.2 - Functional and Combined Object/Functional Guided Transport Model

Deliverable D5.3 - Safety Attributes Allocation Matrix

Deliverable D6.3 - Proposal of a common safety life cycle approach

Deliverable D7.4 - Proposal of typical optimized AAC process

The deliverables and further details can be found on the project website www.modsafe.eu