Newsletter **Issue 3**

MODSafe

Modular Urban Transport Safety and Security Analysis

MESSAGE FROM THE COORDINATOR

The MODSafe project has reached the last year of its four years project duration and practically all the deliverables have been handed in.

For the safety aspects, a hazard and risk analysis, safety requirements and functional model development have been completed. For the process aspects, a life cycle and future certification approaches have been proposed. For what concerns security, the existing means and technologies for security systems have been analyzed.

The project deliverables that are available so far have raised increasing interest from the sector, which goes hand in hand with the projects' dissemination activities.

As the end of the project is a few steps away, one can expect the finalization of reasonable suggestions that aim at simplifying the upgrade or new construction of urban guided transport systems. Cross-Acceptance is one of the key aspects which will benefit all parties involved, including operators, manufacturers and suppliers and safety authorities.

As the Coordinator of the project, I am pleased to present the third and final Newsletter, which provides a brief overview on the latest project results and deliverables. The newsletter together with the projects' web page www.modsafe.eu as well as further publication and exploitation effort, aim at promoting the project and its beneficial results.

Should you have any comments or questions, please do not hesitate to contact me at modsafe@de.tuv.com

IN THIS ISSUE

WHAT'S NEW?

Safety Model for Urban Guided Transport Systems

Contrary to mainline railways, the Urban Guided Transport Systems remain often highly individual entities due to their local specificities and their spatial independence from each other. This is particularly true concerning Safety Requirements, Safety Targets Allocation and also Safety Acceptance and Approval Schemes, where every country, and sometimes even every municipality, employs their own rules.

In order to help form a more common understanding on this topic among different stakeholders, i.e. operators, industrial suppliers and safety authorities, four Work Packages (WP) dealing with Safety Requirements and Safety Target Allocation have been set up in MODSafe.

The major objectives of these WPs include the definition of a complete and generic Systems Hazard Analysis, a Functional and Objects Safety Model, a process for Allocation of Safety requirements to Functions/Objects and also an analysis and comparison of Security Requirements and Measures. The analyses were performed for different Grades of Automation ranging from classical manual train operation up to fully automated and unattended train service.

Following the idea of the system lifecycle of railways according to EN50126 **a Hazard Analysis was performed in WP2**. In order to allow usability among different operators, the analysis focussed on the identification of typical system and subsystem hazards but still tried to remain at a generic level. A list of approximately 1,300 entries was created and consolidated with analyses from other projects. It covers hazards from major technical or operational categories, such as Train Movement, Train Interior, Train-Station Interface (with train in station), Train-Station Interface (without train in station), Depot, Operation Control Centre (OCC), Maintenance, Emergency - Evacuation and Environment (force of nature). This hazard analysis includes the different causes, accidents and consequences for each hazard and serves as a foundation for the next safety WPs which focus on the Risk Analysis and Safety Measure definition to prevent from the identified hazards.

The definition of adequate Safety Measures are subject to detailed analyses in WP4 (Safety Requirements). Different safety requirement allocation methods are compared, e.g. risk matrix or risk graph. This also includes a description of relevant standards and guidelines as well as actual methods used by urban railway operators. **A check if the defined safety functions and measures cover the identified hazards was performed by WP3.**

Regarding the overall findings so far, we can conclude that **for functions working in a continuous mode of operation, which are most of today's train control functions, all analyzed methods yield the same results. But for safety functions with an on demand character, i.e. they are used only at rare occurrence; the results are not necessarily comparable.**

Based on normative references such as IEC62290 a model of typical safety functions, e.g. overspeed protection, collision protection, etc. had been specified and safety integrity requirements have been allocated to the different functions. **While for most functions a specific safety integrity requirement, e.g. SIL, could be allocated it was found that some safety functions strongly depend on the specific context of each operator**, making it difficult to specify generic safety requirements. Thus, the proposed safety integrity requirements shall be taken as basic reference for independent and specific analyses of an operator.

Taking into account the functional model from WP4, **a combined Function-Object-Model was developed in WP5** to show the interrelationship between safety functions and the technology, i.e. the components of a train control system. Specific safety requirements could be transferred from the functional level to the implementation level with safety integrity requirements assigned to technical components. In principle a matrix was created containing the safety functions as well as typical objects forming the overall train control system. Each entry in the matrix could be read as the safety requirement for a certain component in case the component is involved in the realization of a certain safety function. Since train control system architectures may of course differ, **no generic safety requirement could be put on specific components, but the relationship had been demonstrated in principle.**

For more information
Pr. Sven Scholz sven.scholz@telsys.de

Common Life Cycle Approach Proposal

Based on a MODSafe survey and comparison, WP6 **identified differences and similarities in the process of the different EU countries, analysed the regulation background** and **the main phases of the safety life cycles.**

Today the CENELEC railway application standards EN 50126 series (also transferred at international IEC level) are implemented in practically every new rail technology project including light rail, tram and metro systems. Their goal is to develop compatible rail systems and to enable cross-acceptance of generic approvals by the different railway authorities. The overall procedure of the railway standard EN 50126 is based on the life cycle model. The life cycle model distinguishes between different phases. Each phase contains well defined, phase-related tasks, which are general, RAM (Reliability, Availability, Maintainability) and safety tasks.

The CENELEC railway application standards are now subject to review and revision. The life cycle model introduced in EN 50126 has allowed operators and suppliers to adopt the fourteen life cycle phases of the standards and map their processes on them. The implemented life cycle model is well accepted today and has proven its suitability for more than a decade. Therefore, **a change of the life cycle model is not expected in the new revision of EN 50126.**

The **common life cycle approach proposal for urban guided transport (UGT) systems is defined in Deliverable D6.3.** This approach:

- is applicable to urban guided transport systems as well as for sub-systems, as well as operation and maintenance aspects;
- is based on the life cycle as defined in EN 50126;

- considers input and output per life cycle phase as specified in EN 50126;
- considers activities per life cycle phase as specified in EN 50126;
- does NOT intend to copy and paste EN 50126 clauses;
- considers guidelines and code of practices as far as reasonable;
- specifies interfaces, roles and responsibilities within the life cycle approach;
- introduces principle processes and aspects per life cycle approach phase.

As a general rule, each life cycle approach phase requires the proper closure and the availability of the respective deliverables and documentation of the previous life cycle approach phase.

D6.3 describes **the roles and responsibilities as well as the principle activities for each of the life cycle phases.**

In phases 1 to 4 of the Life cycle approach, it is the Operator's responsibility to specify the requirements of the (new or modified) urban guided transport system.

In phases 5 to 9, it is the Supplier's responsibility to build the system as specified. This includes the Supplier validation and acceptance of the system.

In phase 10, the Safety Authority's licenses the commercial operation.

Finally, phases 11 to 14 (which are under the Operator's responsibility) cover the operation and maintenance of the system (including performance monitoring and potential modification and retrofit) as well as the potential decommissioning and disposal.

When considering phase 10, the standard EN 50126 "does not define an approval process by the safety regulatory authority". The standard is applicable "for use by Railway Authorities and railway support industry" (ref. section Scope of the standard) and therefore offers a sound basis for the definition of an approval process which takes the specific needs and local specialities under consideration.

The approval process should be based on the life cycle approach model as defined in MODSafe. The CENELEC approach and process requires an appropriate safety management concept. Like the well-known quality management concept ISO 9001, the CENELEC safety management concept establishes the assumption that the level of safety of a complex product can seldom be proven simply by testing the finished product - especially with regard to electronic software and hardware components this is impossible. Safety just like quality has to be an integral part of the design and production process in order to lead to products that possess a suitable level of safety. Furthermore, the required level of safety of a product is hugely dependent on the system it will be embedded in.

The CENELEC safety management system therefore lends itself for combination with more prescriptive safety standard or regulation series, which may differ throughout the European Member States.

In conclusion, it can be stated, that **CENELEC and further appropriate national safety standards or regulations form a sound basis for the approval process of new or modified UGT systems. Respective safety concepts and a safety demonstration / approval process can be derived thereof.**

For more information
Peter Wigger wigger@de.tuv.com

Acceptance, Approval and Certification

Just like life cycle approaches, Acceptance, Approval and Certification (AAC) procedures are characterized 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 rail systems.

The main objective of WP7 is to make the diversity transparent for participants of these processes (suppliers, operators, etc.) by **developing and proposing a typical optimised framework for the AAC-procedures**, which is based on an analysis of current AAC-procedures in Europe and which is composed by so-called "elementary activity modules". Such typical optimised framework could offer relevant authorities a common reference in Europe and therefore facilitate the creation of new urban rail systems.

A typical optimised framework AAC-procedure is proposed following an analysis and a synthesis process. The **analysis phase** consisted of two steps. First the current AAC-procedures in different countries and cities of Europe was reviewed. Secondly, in this survey the main participants were identified and as a result, a list of elementary activity modules were provided. In the **synthesis phase** first a typical model of an AAC-procedure will be drafted based on the elementary activity modules, and in a second step, based on the typical model, a typical optimised framework AAC-procedure will be proposed.

At this stage the project has completed the analysis phase.

Firstly a questionnaire was elaborated together with WP6. The questionnaire was sent to different countries of Europe to provide a wide survey of the **current state of acceptance, approval and certification procedures**.

In this questionnaire, a number of questions were asked. For example: *are there Safety Regulatory Authorities appointed for Metro/ Trams in your country?* The results were classified in four categories:

- No authority or supervisory body: in this case the safe operation is not supervised by an independent body, it is the operator of the transportation system that is responsible for the correct operation. This may be the case often for tram systems, or tram systems with a limited speed, but in some cases (e.g. Belgium) it applies also for metro systems.

- Local supervisory body: in other cases the operator is supervised by a local authority or in other terms by the city in which the transportation operation is carried out. This may be the case for both trams and metros (e.g. Estonia).

- State authorities: countries, which have a federation governmental structure (like Austria or Germany), have usually individual regulatory authorities in different federal states.

- National level authority: in other cases the country has a central, national regulatory authority, which is usually a governmental organisation.

Other questions included: are *there any national functional, technical or operational requirements to be fulfilled for obtaining system approval?* What *involvement* of *Independent Safety Assessors?* How far do *investigations carried out by the Safety Regulatory Authorities* go?

If we examine the current practices and especially the case studies on the approval, acceptance and certification procedures of urban rail systems, we can state that there must be **at least two key players in these processes**: the operator and the supplier. There are additional players that can be involved in these processes, like an authority or an independent body.

The **"elementary activity modules"** (EAM) are activities, that are identical in approval, acceptance and certification processes of different countries, but that may be carried out by different parties with different levels of independency and 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 effectively achieved if different procedures of different countries or cities can be compared. The comparison will deliver adequate results if the different processes are described in the same way, i.e. using the same description mean.

These "elementary activity modules" can be organised according to different views: timeline of the life cycle and the hierarchy of the system, i.e. system level, level of functionality and safety.

According to the timeline similar activities can be identified: **definition of requirements, check of requirements, demonstration of fulfilment of requirements and check of fulfilment of requirements.** This sequence of activities can be found at system level, functional level and safety level, with slight differences.

The act of approval is an important elementary activity module, and it can be interpreted mainly at system level. The activity of safety assessment is a parallel activity, which is linked mainly to the safety level.

For more information
saghi.balazs@mail.bme.hu

Security in Urban Guided Transport Systems

The main objective of WP8 is to identify, categorise and assess the relevant technologies for security surveillance and prevention and to integrate them in an overall security model.

Task 8.1 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 resulting deliverable **D 8.1** (completed in May 2010) covered countermeasures linked to person's integrity (passengers, staff and infrastructure) and associated technologies, in order to **prevent crime** and to **respond to criminal acts**.

With regard to long distance rail transport, research has shown that there is no specific European legislation. Moreover, few differences between security measures and technologies for urban guided systems compared to long distance rail systems can be identified.

When considering measures applicable to aviation, D 8.1 showed that countermeasures and technologies vary from one sector of activity to another and are often not comparable. In particular, the technologies implemented in aviation security are not transferable to urban rail guided transport systems, as many of them are strictly related to the structure of airports / aircrafts. For all these reasons, the aviation security has not been considered relevant for the subsequent tasks of WP8.

Task 8.2 first assessed the relevant regulations and norms implemented at European and Member States level. This analysis showed that **a very limited level of standardisation specific to security has been achieved at European level** with regard to public transport and to the rail sector, both for heavy rail and for urban rail systems. However, other standards exist which partly cover security (mainly those addressing safety).

Then, an evaluation of the existing technologies for prevention was developed, followed by a hierarchy of legal references. Later, techniques, methods and tools used by the operators and manufacturers to satisfy legal requirements in the area of design and training were reviewed. Finally, technologies were assessed by considering all levels of means and measures for preventive actions, for minimising the effects and for protecting passengers and staff.
This led to the definition of guiding principles with regard to preliminary requirements for technology procurement and application. The resulting deliverable **D 8.2** was finalised in February 2011.

The activities performed in **task 8.3** are now focusing on the security strategies in Urban Guided Transport systems. In particular, deliverable **D 8.3** addresses strategic recommendations for improved Urban Transport Security (UTS) in terms of high end considerations inclusive of terrorism, cyber warfare, organised crime and everyday crime.

For what concerns **WP9**, its main objective is to build up an integrated security model for guided transport in urban areas in the form of guiding principles.

Task 9.1 aimed at analysing the existing threats to urban rail guided transport systems. The resulting deliverable **D 9.1** (completed in February 2010) produced 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 persons 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.

Task 9.2 focused on potential threat-related scenarios and subsequent critical infrastructure components in Urban Guided Transport systems.

The resulting deliverable **D 9.2** (completed in February 2011) 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). Its scope is deliberately restricted to antiterrorism.

The deliverable D 9.2 concludes with **findings and recommendations supporting targeted solutions for the improvement of UGT security**.

Task 9.3 identified all security means and measures which relate to the threats in UGT (including terrorism, cyber threats, organised crime and everyday crime).

D 9.3 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 UTS in a top-down approach from the corporate level (PTO, police forces, agencies, private security) to the field level**.

For more information
Mirella Cassani mirella.cassani@kitesolutions.it

Newsletter **Issue 3**

MODSafe

Modular Urban Transport Safety and Security Analysis

ANY OTHER BUSINESS

SECUR-ED Advisory Groups

The objective of SECUR-ED (SECured URban transportation - European Demonstration) is to enhance public transport security in Europe.

To ensure that the real needs of all stakeholders are taken into account, and to improve the acceptance and applicability of the SECUR-ED proposals developments outside the project, four Advisory Groups composed of non-project partners will be giving feedback and advice to the project. These four Advisory Groups are:

- Public Transport Operators and Authorities
- law Enforcement and First Responders
- Industry
- Ethical and Societal issues

For further information or if you are interested in joining an Advisory Group:
lara.isasa@uitp.org and http://www.secur-ed.eu

MODSafe Final Conference

Do you want to find out what the final results of the MODSafe project are? Then join us in **Cologne** (Germany) on **25-26 June 2012**!

Project partners will highlight the most significant project outcomes regarding Safety, Process and Security aspects and discuss them with the public. All participants will also have access to a guided tour of the KVB Museum and will ride and have dinner within a historical train.

To register and consult a more detailed programme: www.modsafe.eu

The MODSafe team