Safety assessment of Copenhagen driverless automatic mass transit system

Peter Wigger & Ulrich Haspel
TÜV Rheinland Sicherheit und Umweltschutz GmbH
Institute for Software, Electronics, Railroad Technology (ISEB), D - 51101 Cologne, Germany
EMail: Wigger@Tuev-Rheinland.de

Abstract

In 2000, the automatic driverless Metro will commence operation in Copenhagen. The German BOStrab (Regulation for the Construction and Operation of Tramways) was chosen as a basis for the safety approval/assessment of the Metro in conjunction with the European standards for Railway Applications. For the system, a Safety Case has to be assessed. TÜV Rheinland has been assigned the role of the Safety Assessor. Using the PASC approach developed by TÜV Rheinland, safety is a fixed part of the system development from the beginning. An effective course of the project and in-time start of operation can be expected as benefits.

1 Introduction

In autumn 2000, the Copenhagen Metro will commence revenue service. This first Danish metro will be an automatic driverless system, in the first project phase connecting downtown Copenhagen with the university, the new fair area and the developing suburb Ørestad on Amager island. Up to 19 trains - consisting of 3 cars each - will travel with a headway of 90 s between 14 stations on a permanent way of 19 km double track. While the system will be operated in downtown Copenhagen as an underground it will run aboveground and even across bridges and viaducts in the Amager area. In later project phases the system will be extended to the
north-west of Copenhagen and in the south-east to the international airport.

As Denmark had no legal framework for the approval of systems like the Copenhagen Metro, the Danish Government decided to rely on a proven German approval procedure as e.g. performed for the Sky Line, an automatic, driverless mass transit system at Frankfurt Airport (see Frederiksen & Haspel[5]).

In Germany, public tracked mass transit systems fall under the German regulation for the construction and operation of tramways (BOStrab). This regulation does not only apply to conventional tramway systems - as the title may imply - but also to new, unconventional types of tracked transport systems including fully automatic rapid transit systems.

The German BOStrab regulation requires a strongly regimented approval procedure under the supervision of a Technical Supervisory Authority (TSA). The respective Danish Authority (the Railway Inspectorate Jernbanetilsynet, an authority under the Ministry of Transport) asked for safety assessment by an independent Assessor. For the complete system a safety case must be assessed. The safety assessment of the Copenhagen Metro including a special assessment procedure which is supported by computerised tools for planning and monitoring of the assessment process will be described in the following.

2 Safety Assessment of the Copenhagen Metro

TÜV Rheinland with their competence and experience in the certification of complex, safety relevant systems for railway applications was chosen after the tender phase to play the role of the independent Safety Assessor in the Copenhagen Metro project.

The safety assessment of the Copenhagen Metro covers all relevant sub-systems like Permanent Way, Power Supply and Traction Power, Radio and Telecommunication, Control Centre, Stations, Station Doors, Rolling Stock and Civil Works. Special attention is paid on the Automatic Train Protection (ATP) system being part of the Automatic Train Control (ATC) sub-system, the electronic heart of the Metro responsible for control and safety of the automatic driverless system.

TÜV Rheinland has subcontracted Det Norske Veritas Danmark for local support in Copenhagen and safety assessment in the area of civil works.
2.1 Basis for Safety Assessment

The assessment of the Copenhagen Metro system is performed based on the German BOSTrab [1]. The European Union already stated some years ago that the use of BOSTrab does not hinder competition and thus it may be used throughout the countries of the EU.

BOSTrab calls for compliance with the orders of the Technical Supervisory Authority, and with the "generally accepted rules of technology" (GARTs). These rules consist of standards and regulations that represent the opinion of the majority of the experts in the field of public transport technology.

Besides standards like DIN, VDE, UIC, EN, IEC in Germany several of the VDV papers have the status of a GART in the field of public transport technology. The VDV is a German association of companies that operate public short-distance transport systems (tramways, light rail, busses, private railroad systems). Some of the VDV papers even have the status of a directive to BOSTrab and have been acknowledged by the Federal Ministry of Transport.

For the Copenhagen Metro the VDV papers in connection with the new European Standards for Railway Applications prEN50126 [2], prEN50128 [3], and ENV50129 [4] have been assigned to be GARTs for the safety assessment. These standards are supplemented with the American fire standard for rapid transit systems NFPA 130 and Danish national standards. All safety activities as well as the generation of the safety documentation are performed according to these standards.

2.2 Safety Approach

The BOSTrab distinguishes between the Inspection of documents (§ 60), the inspection during manufacturing (§ 61) and the final safety acceptance (§ 62) as the different main steps of the assessment. The overall procedure of the new European Standard prEN50126 [2] is based on the lifecycle model. The lifecycle model distinguishes between different phases starting with the Concept Phase, continuing with the System Definition and Application Conditions, The Risk Analysis, The System Requirements, Apportionment of System Requirements, System Design and Implementation, Manufacturing, Installation, System Validation, System Acceptance, Operation and Maintenance, Performance Monitoring, Modification and Retrofit and finally Decommissioning and Disposal. Each phase contains well defined, phase-related general, RAM (reliability, availability, maintainability) and safety tasks. In order to follow the safety approach of BOSTrab in combination with the lifecycle
Computers in Railways

model of prEN50126, the following Approval / Authority Acceptance Milestones have been defined.

- Overall System Design Approval (OSD)
- Design Approval (DA)
- Engineering Approval (EA)
- Sub-system Acceptance (SA)
- Prototype Installation Acceptance (PIA)
- Installation Acceptance for Sections of the Metro (IAS)
- Design Approval for Series Production (DAS)
- Acceptance of each Series Produced Train (ARS)
- Approval of System Operator Procedures & Organisation (AOP)
- Approval of System Operator Staff Training (AOT)
- Preliminary System Operator Certificate (POC)
- Final System Operator Certificate (OC)

2.3 Project Accompanying Safety Certification (PASC)

The safety assessment of fully automatic transport systems implies several specialities resulting from their characteristics and complexity. In former times, e. g. for conventional interlocking components, the assessment process only started after the development, when the safety documentation had been completed. For the assessment of modern automatic transport systems (like the Copenhagen Metro) with - apart from other features - sophisticated computerised automatic train protection systems, this procedure is no longer suitable, because the time needed for the development (especially for the ATP hard- and software) is too long and the innovation cycle of technology is too short.

The advanced procedure used by TÜV Rheinland for several years and various projects is the Project Accompanying Safety Certification (PASC). Using this procedure, safety experts perform their inspections and assessments concurrently with the development of the system. When following this procedure it is very important to perform efficient project management and to plan the course of the safety assessment process thoroughly. Furthermore it is important to trace the assessment and to keep up with the assessment documentation in order to avoid serious shortcomings or gaps in the system safety case to be assessed, which might shift the date of putting the system into operation. For complex systems like the Copenhagen Metro such topics are even more important as several safety experts and authorities will be involved in the assessment process.
The general procedure of PASC is laid down in a working directive which is part of the QM-System of TÜV Rheinland. In addition, project specific QM instructions and working directive have been compiled for the Metro Project.

2.4 Assessment planning and project management

In order to apply the PASC procedure in an effective way, a detailed Assessment Plan is essential for the assessment of the Metro system. TÜV Rheinland uses a top-down structured, computer-supported assessment plan, which has been adapted to the Metro Project. The upper three of totally four levels contain semi-graphic representations while the bottom level consists of assessment data stored in an MS-ACCESS database programme.

The toolset called TRACY (tracked transport certification database system) has been developed by TÜV Rheinland since the middle of the eighties for supporting the PASC approach on complex, time-critical assessment projects (see Haspel[6]). The actual version is a flexible toolset that can easily be matched to the requirements of the safety assessment of different guided transport systems.

Figure 1 shows a sketch of the four levels of the Assessment Plan for the Copenhagen Metro. While on level 1 the total Metro system is divided into sub-systems, on Level 2 the sub-systems are broken down into main components, and these into component groups and components which are subject to BOStrab assessment. Within level 3 these are subdivided into separate assessment objects. Every single assessment object is marked by the component-number followed by an additional three-digit number, that allows the indication of the according milestone, kind of assessment and the assessment object. This assessment number represents the link to level 4 - the TRACY databases. These databases do not really represent a hierarchically lower level - the number of assessment objects in level 3 and 4 is the same - but contain detailed data for planning, performing and monitoring of all assessment activities.
Figure 1: Principle representation of the four-level assessment plan for the Metro. The TRACY assessment database program represents level four and contains in addition the documentation database for the management of assessment-related documentation.

In order to incorporate assessments that apply to the overall system (e.g. overall safety acceptance according to BOStrab § 62, Evacuation and Rescue Concept etc.) the "dummy" sub-system "System Comprehensive 1.000" was added in level 1 of the assessment plan. This allows the
breaking down of system safety items to the bottom level in the same way as for "real" sub-systems. In a similar way a block sub-system Comprehensive was added in every sub-system on level 2.

While in former applications the aspect of completeness of the safety assessment was the main goal for using the TRACY tool, for the Metro project aspects of planning and monitoring the assessment process across the many defined assessment and approval milestones, also under aspects of resources and the project schedule are very important. These features were enabled by introducing these milestones into level 3 of the Assessment Plan and by incorporating of more project planning capabilities into TRACY.

During the assessment of the Metro a huge number of assessment-related documents (e.g. plans, descriptions, specifications, analyses, V&V documents, reports, expert opinions) will be produced. These document data (e.g. document type, title, version, author) need to be stored by the Assessor in a way that they can easily be retrieved at any time. For this purpose TRACY contains a documentation database which allows easy storing and retrieval of document data and serves as important part of the assessor's configuration management.

All TRACY databases are based on Microsoft Access and are arranged under one Windows-based user interface, which eases operation and enables data-interrelations between the contents of different databases. The interrelations between schedule information in the assessment databases and the schedule diagrams (based on Microsoft Project) are based on identifiers for dates and milestones. The graphic representations of the assessment plan are created using the program MetaDesign, which eases the interface between the graphic plan and the TRACY databases. This is important, because in the course of the project there are a lot of detail changes in the plan to expect, that would require updating both the graphic an the database plan and would very likely lead to data mismatch if there was no data interface between them.

In the assessment databases, detailed plan information on every assessment activity per milestone can be found, as well as data fields containing results and information concerning the associated reports, which represent the actual assessment status. The division into 3 databases containing different assessment plan data - concerning inspection of documents, during manufacture and safety acceptance - was carried out according to BOStrab §60-62.
Another TRACY database contains relevant interface information about logical/physical interfaces between different assessment objects and system components. This feature provides important information for the assessment of the system and sub-system safety cases. Especially logical interfaces between sub-systems are likely to be "forgotten" by the system developers. E.g. the ATP must not allow trains driving into aboveground stations at a higher speed than allowed for proper operation of the platform obstacle detection system.

Summarising it can be stated that TRACY is a toolset for use during the whole assessment process, i.e. it does not only support the planning process but also support tracing/monitoring of all necessary assessment activities.

2.5 Assessment Results

The results of every inspection, test and safety acceptance will be laid down in a report. These reports also contain an identification of the component/item and the foundations (regulations, standards etc.) of the performed assessment. After the completion of all necessary single assessments of a sub-system (for all sub-sub-systems or components), for each sub-system of the Metro defined in the initial assessment plan a sub-system-comprehensive assessment report - based on the assessment of the sub-system safety cases - will be created that not only sums up the results of the single assessment activities but also judges the suitability of the component/assessment object for the Metro from the system safety point of view. Figure 2 depicts the dependencies of the different safety cases.

For the whole system, so-called Safety Trial Runs will have to be performed by the supplier in order to prove that the system is operating properly and safely under real operating conditions. This is especially important for the ATP system. The Assessor will have to perform several tasks concerning the Safety Trial Runs. On completion of the trials he will issue a report on the results of the complete safety trial period.

For each milestone of the assessment plan that needs to be accepted by the Technical Supervisory Authority (TSA) the Assessor will prepare a report showing the degree of fulfilment of the BOStrab requirements by that milestone. Finally, the Assessor will create a comprehensive report on the fulfilment of the BOStrab requirements and - after the safety acceptance on the overall system has been performed - will issue a statement on the operational safety of the overall Metro system and will rec-
ommend approval by the TSA. After the TSA has issued the preliminary permit for operation the system may be put into revenue service.

For all the aforementioned steps of assessment and creation of reports, TRACY serves as a valuable aid to the Assessor. This is not only because it gives an overview on the assessment status on the different assessment/approval milestones whenever needed, but also provides the Assessor in an easy and convenient way with needed data, e.g. lists of assessed documents and created inspection reports that can easily be retrieved from the databases and inserted into e.g. comprehensive assessment reports.
3 Conclusion

By using the Project Accompanying Safety Certification (PASC) procedure combined with the described Assessment Plan and the TRACY Assessment Databases for the Safety Assessment of complex automatic Mass Transit Systems like the Copenhagen Metro, the assessment activities are synchronised with the system development process. Time- and cost intensive design changes are avoided and system safety is a fixed part of the system development from the beginning. An effective course of the project and in-time start of operation can be expected as benefits.

References


