• Application of generic product and generic application approvals as base for specific applications
• Application of cross acceptance to the extent possible

26.5 Independent Safety Assessment throughout the Life Cycle

The independent safety assessment is based on the application of the life cycle/V-model approach of the railway application standards, applicable for both the railway sector and urban guided transport sector.

Figure 26.1 shows the typical involvement of the independent safety assessor in relation to the life cycle phases. At the discretion of the operator and/or the safety authority, the independent safety assessor can be involved in all life cycle approach phases.

26.5.1 Intermediate Assessment and Approval Milestones

The more complex the system the more detailed has the assessment and approval process to be planned. The life cycle model (also in conjunction with other standards/regulations)* may form the basis to define an acceptance/authority approval process based on authority approval milestones derived from the life cycle approach.

In order to allow for a project accompanying safety approval and continuous evaluation, whether all relevant safety activities and the corresponding submittals are in place, it is recommended to introduce interim safety approval milestones after certain life cycle approach phases.

* Other (project-specific) specific standards, rules, and regulations may apply in addition, for example, the new standard EN 50657 for software on Rolling Stock.
The following project milestones/safety approval milestones as shown in Figure 26.2 are recommended. They should be matched with respective supplier’s project planning. The final definition of milestones is topic of mutually agreement between the actors affected, namely, the operator and the supplier as well as the independent safety assessor and the safety authority.

Intermediate approval milestones can be applied as go-ahead gates, allowing the supplier to enter the next stage only after the respective intermediate approval milestone has been achieved to the satisfaction of the independent safety assessor and the safety authority. This avoids, for example, the start of detailed design (based on potentially incomplete, inconsistent, or invalid requirements) prior to having achieved acceptance of the functional and safety requirements.

### 26.5.2 Handling of Subsystems

In case the life cycle approach is applied to a total railway system/urban guided transport scheme that includes the integration of various subsystems such as rolling stock, permanent way, signaling and communication, and stations the handling of subsystem requires a further refinement. This also covers renewal/modernization projects where new subsystems such as signaling or rolling stock are integrated into existing total railway or urban guided transport systems, also affecting operational aspects in case of change in the grade of automation.

Therefore, for complex systems, it is highly recommended to refine the general life cycle approach model in order to address overall system aspects as well as subsystem specific issues. Some of the equipment being used could also be developed as part of the project, but this activity would also have its own V life cycle approach that would integrate with the V life cycle approach of the overall project. This situation is illustrated in Figure 26.3.

This means, in practice, that the design and development processes as well as the related independent safety assessment for the individual subsystems run in parallel.
The subsystems are developed, manufactured, tested, and assessed in the factory (according to the respective subsystem life cycle approach) before finally being integrated into the overall railway/urban guided transport system.

The handling of subsystems depends on whether the subsystems are part of an overall railway/urban guided transport system process or whether they are considered stand alone, for example, a signaling/train control system in case of a signaling system renewal project or in the case of buying new rolling stock for an existing railway/urban guided transport system.

In the first case (subsystem part of a [new] overall system), the subsystem may run its own life cycle as an “underlying life cycle approach”; this should apply at least for the signaling/train control subsystem. In the second case (stand-alone subsystem), the
subsystem may run its own life cycle approach as a “stand-alone life cycle approach”; this should apply at least for the signaling/train control subsystem. In both cases, basically, the same life cycle process applies as described for the overall railway/urban guided transport system, of course, limited and focused on the sub-system boundaries.

### 26.5.3 Life Cycle Approach Phase-Related Roles and Responsibilities

Figure 26.4 shows the life cycle approach phase-related roles and responsibilities and related interfaces, in particular, the involvement of an independent safety assessor and the safety authority.

**FIGURE 26.4**
Life cycle approach-related roles, responsibilities, and interfaces.
26.5.4 Integration of Subsystems into System Safety Case

Overall, the system life cycle approach phases 1–5 provide the input and requirements for the individual subsystems, whereas each subsystem itself (once having completed the subsystem design and development process) comes with potential application conditions and operation and maintenance requirements to be observed on system level forming the input for life cycle approach phases 8–10.

On this basis, the overall life cycle approach (as well as the independent safety assessment process) can focus on a clear and precise set of safety documentation and, afterward, on thorough checks that the defined targets have been achieved. Figure 26.5 shows the principle hierarchy of safety documentation, following a top–down approach at the beginning of the project (life cycle approach phases 1–5) and a final bottom–up approach for the collection of the subsystem safety evidence (life cycle approach phases 8–10) and forming an integrated system level safety case.

26.5.5 Supplier’s V&V and Related Assessment Activities

V&V applies on both the railway system/urban guided transport system level (ref. EN 50126 [1]) and subsystems, at least for the signaling and train control subsystem (ref. EN 50128 [2] and EN 50129 [3]). This means that validation and safety acceptance applies first for the signaling and train control subsystem for the sole subsystem functions and second for the whole system with respect to functional integration and interfaces including operational aspects. Figure 26.6 shows the main actors for the system validation and safety acceptance phase (life cycle phase 9).

FIGURE 26.5
Principle hierarchy of documentation.
26.6 Conclusion and Benefits of Independent Safety Assessment

Considering the development in the railway and urban guided transport sector (see also MODSafe)* during the last decade, the following can be concluded:

- Systems become more and more complex and software driven, requiring adequate safety means.
- Due to increasing complexity, traditional methods of proof become more problematic.
- Trends in standardization show increasing requirements on independent safety assessment.
- Involvement of independent safety assessment becomes increasingly important.
- Approval authorities more frequently require the involvement of an independent safety assessor.
- Authorities, operators, and even suppliers may not be able to ensure full scale qualification.

* MODSafe—Modular urban transport safety and security analysis—is one of the latest projects in the European Transport sector under the Seventh Framework Programme (FP7) for Research and Technological Development of the European Union, performed from 2008 to 2012. The purpose of the MODSafe project was the development of a safety analysis and model reference for future urban guided transport projects. Even if the rail safety landscape in urban guided transport is highly diversified, the sector will benefit from some kind of harmonization. TÜV Rheinland was the project coordinator on behalf of the European Commission and furthermore responsible for the life cycle work package—both in the person of Peter Wigger, the author of the chapter at hand. The raw material for the chapter at hand has been taken from the MODSafe deliverables, respectively, from TÜV Rheinland in-house sources. Refer to http://www.modsafe.eu for details.
In conclusion, the application of independent safety assessment is recommended since it comes along with the following benefits for the project and involved actors:

- Independence of the assessor ensures opinions being free from project constraints.
- Independent safety assessor qualification and competence ensures views on the relevant aspects.
- There is a reduction of project risk due to competent third-party opinion.
- Independent safety assessor may contribute with lessons learnt from previous projects.
- Involvement of different independent safety assessor team members ensures a variety of views.
- Positive assessment report (and authority approval) result in marketing and sales benefits.
- Positive assessment report (and authority approval) may allow to reduce liability insurance.
- The cross-acceptance approach will significantly reduce project risks.
- Assessor organizations may be accredited as inspection bodies, ensuring criteria compliance.
- Assessor organizations may be accredited as certification bodies, ensuring criteria compliance.
- Operators are given increased confidence independent from potential supplier constraints.
- Responsible safety authorities can limit their resources and activities to the legal responsibility.
- Participation of an independent safety assessor is a win–win situation for all parties involved.

References

27

Application of the Interface and Functional Failure Mode Effects and Criticality Analysis (IFF-MECA) for RAM and Safety Assessment of Rail Electrification

Qamar Mahboob

CONTENTS
27.1 Introduction and Background ......................................................................................... 487
27.2 IFF-MECA ...................................................................................................................... 488
27.3 System under Analysis .................................................................................................... 490
27.4 IFF-MECA Application ................................................................................................... 493
27.5 Conclusion and Outlook .................................................................................................. 500
References.............................................................................................................................500

27.1 Introduction and Background

Railway-related standards require from the railway suppliers and operators to demonstrate the reliability, availability, and maintainability (RAM) and safety in projects (EN 50126 [CEN 1999]). Reliability, availability, maintainability, and safety (RAMS) studies should (a) give answers to the questions associated to the failures in interfaces (INs), functions, and components/subsystems (SSs); (b) consider system and SS level hazards; and (c) show the evaluation of the results in reference to the contracts and standards compliances. Existing methods have limitations in the combined handling of three areas mentioned earlier. Existing RAMS analysis methods (such as failure modes and effects analysis [FMEA], hazard log management, IN hazard analysis, fault tree analysis [FTA]) mainly take into account the system evaluation by considering the subsystem and component level failures of a system (Zio 2007; Aven 2012; Braband 2001; Jahanian and Mahboob 2016). For example, one big limitation of the classical FMEA is that it does not consider the combination of component failures in a system. A single component is considered at a time, and it is assumed that other components in the system are working correctly (IEC 60812, 2006-01 [IEC 2006]). In usual engineering systems, there can be more than one failing component at a time. Additionally, existing analysis approaches only consider portion of system failures. For additional readings on the FMEA, we refer to the study by Carlson (2017) and references therein.

The new approach presented herein is called interface and function failure mode effects and criticality analysis (IFF-MECA) and provides a framework to handle the system properties, functions, INs, components, and combination of all these together with external events. In the modern engineering systems, there is considerable amount of no identified defects caused by neglecting INs, properties, and function-related failures in the systems.
The structure of the study explodes in case the system under analysis is large and complex, which is usual in modern engineering systems (Mahboob 2016). The complexity in systems arises due to the microprocessors, computers, and inter- and intradependencies in the system and its INs. Demonstrating acceptable safety of a technology requires combined, careful, and precise handling of the information on complex and large systems such as rail electrification systems (Chen et al. 2007; Mahboob 2014). In order to demonstrate acceptable safety of a technology, considerations on INs and functions of one system with other systems are important; because RAMS-related requirements can be exported and or imported to other systems. Usually, system development is based on historical experiences, and system correctly performs its intended functions. However, a wrong method or system model for the purpose of RAMS analysis can lead to over- or underestimation of the system RAMS (Mahboob et al. 2012). Consequently, complications toward, e.g., demonstrating acceptable safety and high related costs can occur. Classical methods have following main limitations:

- Mainly limited to the component level considerations (such as FMEA/failure mode, effects and criticality analysis)
- Functions and INs (also required for safety integrity level [SIL] quantification) are not dealt with
- No combinations of failures and no handling of dependence
- SIL-related issues are not dealt with
- Bottom-up approaches, but contractual requirements require top–down demonstrations
- Limitations toward demonstration of “functional tendering documents”
- Extra delivery of functions leading to expensive customer solutions
- Transparency and visualization problems leading to long time of acceptance

This chapter will present the application of the IFF-MECA to a large and complex rail electrification system as an example of any engineering application. The new methodology offers a simple, flexible, and concise visualization of the assessment and demonstration. It offers top–down analysis with focus on system functions and INs. One of the major advantages of the IFF-MECA is that the realization of function, which is usually dependent on hardware, and the incorporation of software can be done at the early stages of the product design and development. In other words, this approach offers flexibility to replace function realization via hardware to software and vice versa. Additionally, IFF-MECA supports decision makers even with limited knowledge in the area of RAMS to understand and then handle the related requirements and constraints adequately.

### 27.2 IFF-MECA

The IFF-MECA provides a framework to handle the system functions, INs, components, and combination of all these together with external events. This approach is presented by Mahboob et al. (2016, 2017) where the application of the IFF-MECA is presented for a