Safety principles of SIMIS interlocking systems

J. Kiefer\(^1\), H. Newi\(^1\) & M. Steingräber\(^2\)

\(^1\)SIEMENS Transportation Systems, Signalling and Control Systems
Main Line, Braunschweig, Germany.

Abstract

In Europe the safety level for railway applications required by the passenger is very high due to high transportation volume as well as for the low levels of risk acceptance. As railway accidents have serious or disastrous consequences, SIEMENS Transportation Systems makes “safety” the most important issue for our everyday business. Additionally, we are aware of the high level of social responsibility associated with development, manufacturing and marketing of safe systems for railway signalling.

In the paper, SIEMENS’s approach for the management of safety is shown focussing the overall philosophy as well as the procedural and technical aspects. Looking at a SIMIS\(^\text{®}\)-interlocking, the safety strategy is explained leading to the advantages of Siemens-systems: highest safety standards, very high availability, and scalability in station size or control distance.

1 Safety policy of SIEMENS Transportation

Railway accidents have serious or disastrous consequences due to technical insufficiency, safety is a necessary feature for all signalling equipment. SIEMENS as a manufacturer of Signalling Equipment is therefore aware of the high level of social responsibility associated with development, manufacturing and marketing of safe systems for railway signalling.

Increasing demands on guided transport systems involve increased requirements on reliability, availability, maintainability, and safety (RAMS) of these systems.

Therefore, SIEMENS states its engagement in the field of "RAMS Policy" in company policies and regulations [2].
We have widely acknowledged that, to meet the RAMS requirements, appropriate activities must be included in the life cycle of systems and their components. These activities have to be managed to be efficient and cost effective. The achievement of RAMS requirements has to be demonstrated and documented.

It is the target of Transportation Systems Group to be one of the most competitive companies in the field of transportation systems. Our aim is to provide systems, products and services of appropriate quality that offer maximum benefit to our customers world-wide. RAMS is an integral part of quality, therefore, RAMS policy is based on our quality policy.

Reliability, availability, maintainability and safety play an important role in ensuring the specified performance, which justifies the special attention paid to RAMS aspects throughout the project.

Our main RAMS objectives are as follows:

- to comply with agreed and implied customer RAMS requirements
- to monitor and optimise the processes in order to achieve maximum benefits for our customer and, at the same time, economic efficiency
- to comply with statutory requirements, guidelines, standards and acknowledged rules of technology and environmental protection affecting our products
- to consider RAMS requirements as an important part of design targets and all other phases of a project.
- to design, manufacture operate and maintain reliable and safe products in a cost effective manner.
- to effectively incorporate subcontractors and suppliers with regard to RAMS.

We work towards achieving our RAMS objectives

- in all stages of the value-added process applying the greatest care and specialist knowledge
- at all levels of the organisation, whereby the executive personnel exercise their process and leadership responsibilities and continuously improve the process

by assessing achievement of the RAMS objectives in audits and reviews and following with corrective actions, if necessary.

2 Project safety management process

Safety and availability of systems have always been of utmost importance to SIEMENS Transportation. The underlying technical principles are based on more than 100 years of tradition. Efforts were made to use fail-safe components for the construction of safety systems to a wide extent (bottom-up-principle).

The efforts towards a single European market as well as the results in the harmonisation of the requirements and the methods for railway signalling have led to an extension of this method with a more systematic top-down-approach. It deduces the requirements for components and subsystems from the overall system requirements.
For new products, SIEMENS Transportation applies a risk-based approach based on the CENELEC standards [3], [4], [5]. This allows optimal tailoring of product features to the customers requirements and the railway applications. Products already developed according to other standards (e.g. Mű8004) are integrated if requirements are equivalent. Therefore, the technical safety measures and appropriate verification and validation activities, the business processes, and culture play an important role in the creation of the product feature ‘Safety’. Safety of SIEMENS Transportation products is proven by the safety case, including

- Report of Quality Management according to ISO 9001;
- Report of Safety Management;

SIEMENS Transportation aims to obtain application-independent approvals (certificates) based on international standards from acknowledged approval authorities. Many of the product approvals come from EBA (German Railway Central Office). These approvals for subsystems are potent to be used in specific system applications for the evidence of the overall system safety.

2.1 RAMS Engineering

The RAMS lifecycle and management activities are fully integrated into the engineering process lifecycle:

After the nomination of a RAMS Manager a Safety Plan and a RAMS Programme is generated. Usually, these documents are agreed and endorsed by the customer and the responsible railway safety authority. As a next, step the Hazard and Risk Analysis and the RAM Analysis are carried out. The purpose is to identify critical functions and their RAMS requirements. When the system architecture has been developed, safety integrity and RAM requirements for components of the architecture can be apportioned. Safety management activities, hazards identified, decisions made, and solutions adopted are recorded or referenced in a Safety Log. The adequacy and efficiency of the RAMS management is checked by regular audits. A strategy for satisfying the safety requirements is developed and documented in a safety case concept. The necessary evidence for the fulfilment of the RAMS requirements is prepared during the design and implementation phase, in particular by safety validation activities. The evidence is integrated in the Safety case. The achieved RAM performance is documented by RAM Demonstration. The safety case is reviewed by an independent safety assessor agreed by the customer and the responsible railway safety authority.

2.2 Safety Validation

Siemens Transportation maintains a Safety Validation Department consisting of an Independent Safety Validator and an allocated team of accredited Validators.

This department is independent from the design activities within the project and is qualified to check hardware and software in safety related systems.
The **Independent Safety Validator** is responsible for

- validating the demonstration of safety for hardware modules (= technical safety report) and providing a validation report
- validating the functional correctness for software modules (= technical safety report) and providing a validation report
- validating of subsystem and system design.

### 2.3 Independent safety assessment

Details of safety assessment are planned and agreed with the railway authority as part of the project Safety Plan.

SIEMENS Transportation is licensed to design and develop applications for railway signalling by the German railway authority EBA. As part of this license, experts from the Safety Validation Department are accredited as independent safety assessors on particular projects in agreement with the railway authority.

Our internal standard "Assessment of Safety Cases in Co-operation with the German Railways Central Office" describes tasks and responsibilities of the Safety Validation Department of SIEMENS Transportation and defines the methods and procedures used for the assessment of safety cases under the direction of this Safety Assessment Department. In most cases, system approval is based on this Independent Assessment.

A general overview of the process is given in Figure 1. It is based on a Siemens guideline [1] conform to CENELEC standards under agreement with the EBA. This process needs to be tailored for a particular project and will be part of the projects Safety Plan.

### 3 The SIEMENS Interlocking System SIMIS W

The electronic interlocking SIMIS-W is a geographical interlocking. The system design allows to realise a complex interlocking out of individual functional modules for the different signalling elements. Due to the fact that these modules are equivalent to elements in the railway environment, interlockings can be scaled from very small solutions up to large central stations with more than 1000 outside elements.

#### 3.1 Functional structure of SIMIS W

Figure 2 shows the overall architecture of the SIMIS W-interlocking including the man-machine-interface. The central processing units IIC/OMC and ACC are implemented using a redundant and vital computer system (2 out of 3 architecture). The individual channels use the same software and the results are hardware voted. A redundant bus-system is used for the data transmission among all components and covers the whole control area. The bus system is vital sending coded data on both data lines. In case of disruption of one data line, a vital transmission is still available using double-length telegrams.
Figure 1: Assessment and approval process including documents
SIMIS W uses the following functional layers:

- Man machine interface functions including the following units:
  - man-machine interface (MMI)
  - service and diagnosis (S&D)
  - communication interface (COMIN) to overhead units (e.g. traffic management system)
- Central interlocking functions including the following units:
  - overhead management component (OMC)
  - interlocking and interface component (IIC)
  - video display unit (BAI)
- Logical functions and control including the following units:
  - area control computer (ACC)
  - element control computer
- Physical layer including the following units:
  - interface units
  - cabling
  - field elements (e.g.: points, signal, track vacancy detection)

The first two functions are located in a central building whereby the others are implemented on a decentralised and vital hardware.

### 3.2 SIMIS 2-out-of-3 system as the ECC version

For the ACC function, the 2-out-of-3 version of the ECC (element control computer) is used as the fail-safe computer in the SIMIS-W.

The three computer channels are accommodated in an ECC computer rack which can be extended if necessary (see Figure 3). On the left-hand side in the
ECC computer rack, there are five slots on the computer core (3 CPU modules) and there are also the communication modules. The other slots are for element interface modules.

![ECC fail-safe microcomputer system](image)

**Figure 3: ECC fail-safe microcomputer system**

### 4 SIEMENS safety principles of SIMIS Interlocking Systems

The safety philosophy of the division Transportation Systems in SIEMENS is based on 150 years of experience in design and manufacturing of signalling systems for the railways.

The elementary principles on which this technology is based have proven themselves over the years and are now regarded as accepted principles.

In the last 25 years, more and more use has been made of electronic components.

All these components must meet the following requirements:
• A potentially hazardous (single) fault must be avoided by overdimensioning or redundancy of the mechanical and electrical elements.
• Avoidable (single) faults must not be permitted to have an endangering effect.
• Electronic circuits must have two channels and monitor each other.
• It is only permissible for the results of processing to have an effect on the signalling and safety process if the results of both processing channels agree with each other.
• The processing channels must be independent of each other. The electrical isolation of the channels must be permanent.
• The first fault must be detected and a safe reaction brought about within the failure detection time $\Delta t$.
• The failure detection time $\Delta t$ must be kept so short that it does not have to be assumed that a further fault will occur which, in conjunction with the first fault, can become hazardous.
• It must be impossible for further faults to prevent a fail-safe reaction.

Additionally, SIMIS computers have the following features:
• In fault free condition: Correct functionality
• In fault conditions: Change to safe state - remaining

In the following sections, it will be demonstrated how the principles laid down above are complied with in the SIMIS system.

### 4.1 Faults of short circuit and disconnection

Disconnection or short circuit of wires that are adjacent to each other are taken into consideration. It is prevented by design that a hazardous failure effect occurs, due to a signalling failure. For example, a green signal to a train due to a wiring failure is prevented by design (e.g. by failure detection).

For SIMIS, this means:

| Command circuits (wires) that influence the operating process (e.g. train movement) are always fail-safe. |
| Wires that have different output to field elements are isolated to each other that an influence is not probable under fault conditions. This is applied to input connections and isolations within the system for failure detection purposes (2 channels). |

### 4.2 Faults in the electronic

The effect of a fault in an electronic device is not predictable - especially of complex integrated circuits. For this reason it is always necessary to check the output of the electronic. For SIMIS, this means:

| The computing process must be checked by an additional, independent checking system. The checking system must be able to shut down the faulty system via a second, independent channel. |
To realise these requirements, SIMIS has a two channel architecture (2-out-of-2), shown in Figure 4.

To switch on the lamp both channel must have the same output and the checking devices must be fault free. For this reason the checking system is also a 2-out-of-2 system.

After a first fault occurred the second failure in the checking device can be hazardous if the first fault was not detected meanwhile and if the fault effect is the same. That means:

A first fault must be detected and effect a safe state of the system before a second failure can occur within a specified failure detection time \( t \). The detection time determines the Safety Integrity Level (SIL) of the system. The system is in a safe state after the detection of a fault and another fault shall never influence the system's retention in the safe state.

The specified failure detection time \( t \) is defined with the mean time between failures (MTBF<sub>CH</sub>) of the computing channels whose simultaneous faults could be hazardous:
in a 2-out-of-2 system

The requirement of a specific failure detection time can only be met by a checking mechanism of all functions of the computing system. For this reason, the SIMIS is implemented with very effective *Online Checking Programs* that run online during the system is in service. That means:

| The checking of all system functions shall be done cyclic within a specified time that is determined by the failure detection time t. |

The hazardous event caused by a second fault is prevented by:
- Either the first fault is repaired
- or a third, independent part of the system supervises the processing computer channels and its function is to retain the system in a safe state.

As a consequence of that:

| The fail-safe behaviour of a two channel system must be implemented with a third, independent part of the system which function is the system's retention in the safe state. This requirement is important to be fulfilled by considering both, hardware and software failures. |

### 4.3 Measures for a high reliable system

The system is made up of two or three mutually independent, clock-synchronised and identically programmed microcomputers of identical structure (Figure 5). Each microcomputer is controlled by a CPU. A comparator is assigned to each CPU, which compares the output data of the microcomputers. The data is transmitted by a data exchange unit to the partner microcomputers. The process data is read back using input boards and passed on to the CPU. Via output boards, the control data is output to the process. Microcomputers and process elements are electrically isolated from one another by optocouplers provided at the inputs and outputs of the related boards.

Due to their identical programming, the subsystems always execute the same functions. Hence, the commands output to the peripherals must be the same for all channels. If this is not the case, the comparators shut down the outputs (safety shutdown), immediately. The SIMIS principle ensures a very short failure detection time.

\[
t = \frac{1}{1000 \cdot MTBF_{CH}}
\]
5 Conclusion

This SIMIS principle and the way it is implemented gives important benefits for the operation of an interlocking system:

- The application process of an interlocking can be implemented in a SIMIS system without integrating any check-functions. - The safety functions are independent form the application specific programs and data.
- The SIMIS does not need programs to synchronise the output of the system. A real time operating system can be used. - The checking and fail safe behaviour of a SIMIS is implemented by hardware and software. For this reason the two channels of a SIMIS computer are synchronised.
- Application specific software implementation or update is possible without any cancellations of service. - The SIMIS core provides safety by being independent of the application software.
- SIMIS interlockings are efficiently scalable from small to very large schemes due to its centralised and decentralised architecture, integrated core safety functions and high level of safety.
References

[1] Siemens AG, "Work Guideline, Assessment of Safety Cases in Co-operation with the German Railways Central Office", 16.4.98