Safety Critical Software in the Rail Industry

Focus on: The Manager ☑ The Specialist ☑ Spotlight Programme ☑ Hands-on Skills ☐

Course Overview

The course has been updated to reflect the publication of the new standard **EN50716:2023 Railway Applications** — Requirements for software development.

It provides software developers, engineers, testers, managers and others involved in safety-related projects with a detailed understanding of the fundamentals of safety critical software development and testing.

The opening module provides background to software lifecycle, the standards and their application in the railway drawing upon best practice. The next modules introduce a number of incidents where software failures resulted in incidents. The succeeding modules go into depth regarding the content, aims and requirements for developing software for the railway in accordance with EN50716 for all SIL levels.

Course Objectives		This Course is Ideal For:	
1	Demonstrate a sound understanding of the principles and language of safety critical software	✓	Railway Business Leaders and Managers
2	Appreciate software risk in the context of railway design and safety management	✓	Railway Inspectors and Legislators
3	Describe how software design and the software safety lifecycle interact and influence each other	✓	Railway Safety Assessors
4	Appreciate how current best practices in software safety standards and, in particular, the latest EN50716:2023	✓	Safety Professionals and Planners
5	Understand the need for a risk-based system engineering lifecycle approach to enable built-in safety, value and performance	✓	IT Professionals and Resilience Specialists
6	Understand how to review case studies to understand the potential for things to go wrong on the railway	✓	Railway Engineers
7	Understand the complexity of railway accidents involving software failures		

Course Content

Day	Theme	Coverage
1	Introduction to EN50716	Overview of EN50716 and its scope. Software safety route map – Relationship between generic system development and application development. Key definitions relevant to software safety. Alignment of EN50716 with other railway standards (e.g., EN50126, EN50129).

Safety Critical Software in the Rail Industry

Focus on: The Manager ☑ The Specialist ☑ Spotlight Programme ☑ Hands-on Skills ☐

		Activity: Desktop study to map key activities from EN50716 to a given example project
2	Case Studies of Software Failures	Case studies of accidents related to software failures. Analysis of lessons learned from past mistakes. Detailed review of a specific case study caused by software errors and inadequate safety management. Risk mitigation strategies derived from historical failures. **Activity**: Group discussion to identify safety failures in a provided case and propose mitigations.
3	Software Safety Integrity Level (SIL), Software. Requirements, Architecture, and Design	Process for assigning SIL using EN50126 principles. Competence and responsibilities of personnel carrying out software safety activities. Levels of independence required for various SIL levels in software design and verification/validation. Strategies for maintaining compliance across SIL levels. **Activity**: Exercise to assess and assign SIL for a mock railway system. Required properties for software requirement specifications. Techniques and methods for software architecture based on SIL. Software design and implementation techniques/methods in relation to SIL. Common pitfalls in software requirement and design phases. **Activity**: Develop a simplified software requirement specification for a safety-critical system.
4	Development and Testing Techniques. Integration, Validation, and Maintenance	Techniques for building safety-critical software (Annex B of the standard). Certification requirements for tools used in software development and testing. Software verification/testing techniques and methods based on SIL. Best practices for iterative testing and feedback loops. **Activity**: Compare tools and techniques for safety-critical software compliance. Integration of software with hardware in safety-critical systems. Software validation techniques/methods based on SIL Reporting requirements for software assessment and SW Quality Assurance. Considerations for software maintenance and lifecycle updates. **Activity**: Review a sample software assessment report for compliance with EN50716.
5	Documentation and Emerging Practices	Documentation and traceability requirements for safety-critical systems. Comparison of Agile vs. Waterfall methodologies in safety-critical software development. Process/workflow optimization for EN50716 compliance. Incorporating security measures against cyberthreats in software systems. **Activity**: Desktop study using the

		latest AI tool by Digital Transit to ensure software safety-critical documents comply with EN50716

Course Assessment	Certification
Participants will be assessed on:	Upon successful completion of the course, participants will receive a **Certificate of Successful Completion**, along with a **Transcript of Marks** showing the performance by grade in each element of assessment and overall.
Participation in sessions	
Completion of exercises & case studies	
Performance in assessments	

Course Instructor

This speaker is a Member of the Institution of Railway Signal Engineers (MIRSE), He holds a doctorate in Mechanical and Aeronautical Engineering and undertakes consultancy and research. He delivers specialised training in engineering, safety, risk management, interoperability, and railway legislation.
With over 30 years of international experience, he has held senior roles in signalling, rolling stock, infrastructure, and railway systems, including Systems Assurance Manager and Head of Systems Engineering and Safety. His expertise spans metro, tram, and heavy rail, with a focus on safety, compliance, and reliability.