Railway Operational Technology Cybersecurity

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

Course Overview

The first part of this comprehensive training course focuses on the emerging railway-specific cybersecurity standard **IEC 63452** (based on TS 50701), alongside established best practices from operational and information technology cybersecurity frameworks such as **IEC 62443** and **ISO/IEC 27001**. Delegates will be introduced to foundational cybersecurity concepts, enabling them to assess risks, apply countermeasures, strengthen defences, and reduce system vulnerabilities. Practical guidance is provided on managing cybersecurity risks throughout the lifecycle of railway assets and systems.

Together, these standards provide the necessary structure for integrating safety and cybersecurity into complex railway systems, ensuring compliance, assurance, and resilience in the face of evolving threats.

The course content is mapped to recognised industry competencies, evidence frameworks for railway safety roles, and relevant international and national standards.

Course Objectives		This Course is Ideal For:	
1	**Comprehend** the critical landscape of cybersecurity within railway systems**,** including the unique challenges and the importance of integrating cybersecurity throughout the railway application lifecycle.	✓	Railway Business Leaders and Managers
2	**Analyse and apply** key international and railway-specific cybersecurity standards and frameworks**,** specifically **IEC 63452, IEC 62443, and ISO/IEC 27001,** to identify risks and implement effective countermeasures in operational and information technology environments.	✓	Railway Inspectors and Legislators
3	**Conduct detailed risk assessments** and **define cybersecurity requirements** for railway assets and systems, including considerations for legacy infrastructure and the development of secure new devices.	✓	Railway Safety Assessors and Cybersecurity Professionals
4	**Integrate cybersecurity requirements within the railway safety (RAMS) framework** to ensure holistic system compliance, assurance, and resilience.	✓	Railway Engineers

Railway Operational Technology Cybersecurity

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

Course Content

Day	Theme	Coverage
1	Core Concepts and Real-World Applications	• Introduction to Cybersecurity in Railway Systems • Cyber Security Incidents • Cyber Security Standards and Schemes • Cybersecurity within a Railway Application Lifecycle
2	Advanced Implementation and Case Studies	• Case study: Comprehensive Security Programme - Overview of establishing a full-scale cybersecurity program. • Case Study: Rolling Stock Case Study for Legacy Vehicles: Challenges and solutions in securing legacy railway vehicles.
3	Risk Assessment, Zone Model and Requirements	• Detailed Risk Assessment and Cybersecurity Requirements • Cybersecurity Assurance and System Acceptance • Legacy Systems and Secure Design
4	Applications	• Case Study: Using Current Standards to Develop Signalling Systems (e.g., ERTMS) - Applying standards (IEC63452) to enhance signalling systems' security. • Case Study: Developing Secure Devices - Best practices in the design and development of secure railway devices
5	Useful tools, Assessment and Wash-Up.	• Use of AI tools for Assessing Cybersecurity Standards Compliance • Conclusions and Assessment

Course Assessment

Participants will be assessed on:

Participation in sessions

Completion of exercises & case studies

Performance in assessments

Certification

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.

Course Instructor

This speaker is a Chartered Engineer and 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. The speaker also sits on the IEC committee for the railway OT Cybersecurity standard.