Informa Connect
Academy

CENELEC IEC63452 and TS50701 - Rail Cyber Security

BLENDED LEARNING/ONLINE COURSE | 12 Self-Paced Modules + 3 Live Interactive Sessions

This course is based upon the new railway cybersecurity-specific IEC63452 and TS50701, and best practices from other OT and IT Cybersecurity standards such as **ISO-27001, IEC 62443** and the **Australian Standard® AS 7770 Rail Cyber Security.**

Click here to visit website

Course Overview

'If it is not secure, it is unlikely to be safe':
UK Department for Transport

The railway sector is facing a new challenge: the Network Information Security (NIS) regulations. According to a 2020 survey by the European Union Agency for Cybersecurity (ENISA), only 33% of rail operators of essential services (OES) have fully implemented defensive measures against cyber attacks, as recommended by NIS regulations. This places their software under serious risk, not to mention their lack of compliance with the new regulations.

When security breaches occur, the ripple effect throughout an organisation can be vast, with consequences that are both financial and personal. There may also be implications concerning system safety and resilience.

This IEC63452 and TS50701 Rail Cyber Security training is an introduction to the major themes of cybersecurity and will start you on a journey to the creation of a secure rail operation. After taking this course, you will be able to communicate effectively, make informed trade-offs, assess risk, improve defences, and reduce vulnerabilities in your systems.

This program is based upon the new railway cybersecurity-specific IEC63452 and TS50701 and best practices from other OT and IT Cybersecurity benchmarks such as ISO27001, IEC 624423 and the Australian Standard® AS 7770 Rail Cyber Security.

Our experts will answer questions and provide advice throughout the course via interactive live online sessions and the learning management system.

Key Benefits

- What is Cybersecurity? Putting it into the context of railway and transportation
- Identify threats and vulnerabilities (such as cybersecurity, safety and availability)
- Develop mitigation actions for threats and vulnerabilities and recovery from potential consequences
- Cybersecurity: What standards are available for dealing with threats
- An understanding of IEC63452 and TS50701 and how it can improve cybersecurity across the entire railway

Who Should Participate

This blended IEC63452 and TS50701 rail cyber security online course is for railway business leaders, managers, railway inspectors, railway legislators, safety professionals, planners, information technology (IT) professionals, resilience specialists and railway engineers tasked with making decisions that could impact the cyber resilience of technical and organisational systems.

The course is focused more towards railway Operational technology (OT), although it also covers IT issues, particularly their security risks and strategies from ISO-27001. No prior knowledge of cybersecurity is required for this course.

March – April 2025

Live Interactive Session:	27 March	18:00 AEDT (27 March - 07:00am GMT)
Live Interactive Session:	10 April	17:00 AEST (10 April - 07:00am GMT)
Live Interactive Session:	20 April	17:00 AEST (20 April - 07:00am GMT)

August – September 2025

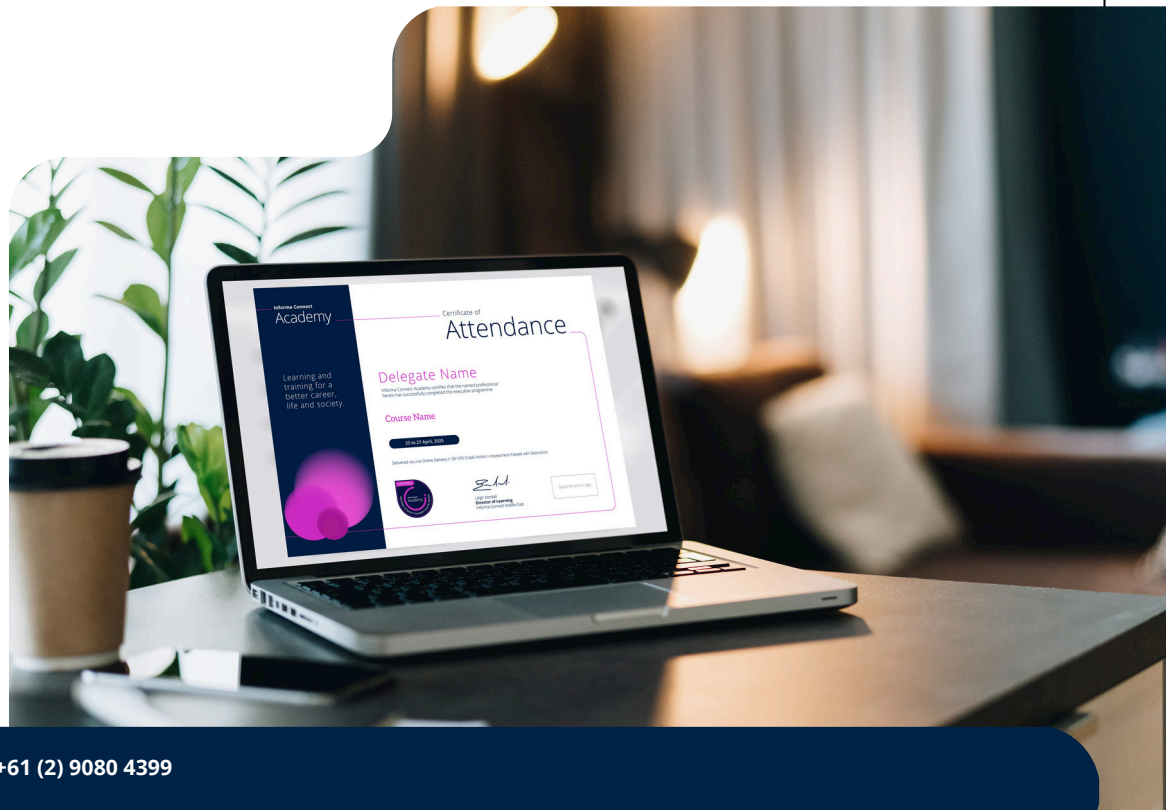
Live Interactive Session:	21 August	17:00 AEST (21 August - 07:00am GMT)
Live Interactive Session:	4 September	17:00 AEST (4 September - 07:00am GMT)
Live Interactive Session:	18 September	17:00 AEST (18 September - 07:00am GMT)

Course Requirements and Certificates

Delegates must meet two criteria to be eligible for an Informa Connect Academy Certificate of Completion:

- **Satisfactory attendance** - Delegates must attend all sessions of the course. Assessments will be ongoing and based on in-class participation and activities.

If delegates have not attended all sessions, the certificate will clearly state the number of hours attended. In-person delegates will receive a printed certificate and virtual delegates will receive a digital certificate.



Course Outline

Informa Connect Academy

Module 1: Introduction to Cybersecurity in Rail

- Meet the presenters and discover the course objectives
- Explore TS50701, IEC63452, and their importance to rail cybersecurity
- Gain insights into cybersecurity principles and the IT/OT divide
- Understand the unique challenges and threats facing the rail industry

ACTIVE LEARNING

Quiz: Identifying personal expectations of the course and foundational knowledge through an interactive quiz

Module 2: Threat Landscape and Incident Examples

- Discover key cybersecurity statistics and attack trends in rail
- Learn from real-world incidents like WannaCry and the Lodz Tram hack
- Explore vulnerabilities in rail systems and potential future threats
- See how proactive measures can mitigate risks

ACTIVE LEARNING

Activity - Assess a simulated attack scenario and identify how it happened

Module 3: Standards, Guidance, and Compliance

- Get an introduction to key standards like IEC62443 and ISO27000
- Understand how legislation such as NIS2 impacts rail cybersecurity
- Explore practical guidance tools like Cyber Essentials and NIST frameworks
- Learn how to apply standards to real-world scenarios

ACTIVE LEARNING

Activity - Match rail cybersecurity scenarios to relevant standards

Module 4: Railway System Cybersecurity Modelling

- Explore the taxonomy and classification of railway systems
- Learn how to create railway zone models and assess criticality levels
- Understand the importance of IT/OT separation and IoT considerations
- Develop communication matrices for effective cybersecurity planning

ACTIVE LEARNING

Activity - Identify and build the features of high-level zone models for a railway system

Module 5: Overall Security Management

- Discover how to develop a robust OT cybersecurity programme
- Learn best practices for supply chain and inventory management
- Explore strategies for security awareness and training
- Understand architecture constraints in managing cybersecurity

ACTIVE LEARNING

Activity - An exercise to understand the key high-level features cybersecurity management plan

Module 6: Cybersecurity Across the Lifecycle

- Understand cybersecurity integration at every lifecycle stage
- Explore interfaces between design, safety, and security processes
- See how concepts from previous modules apply to lifecycle management
- Gain insight into validation, maintenance, and decommissioning

ACTIVE LEARNING

Activity - Map cybersecurity actions to lifecycle stages

Module 7a & 7b: Risk Assessment

- Learn how to identify Systems under Consideration (SuC) and their threats
- Explore threat and vulnerability identification methods
- Understand principles of risk acceptance and countermeasure implementation
- Evaluate risks and determine appropriate security levels

ACTIVE LEARNING

Activity - Complete a simplified detailed risk assessment for a rail cybersecurity case study

Module 8: Cybersecurity Requirements

- Discover how to specify and allocate cybersecurity requirements
- Learn strategies for conflict resolution and compensating countermeasures
- Explore the role of SecRACs in system and subsystem requirements
- Address shared cybersecurity needs across interconnected systems

ACTIVE LEARNING

Activity - Draft cybersecurity requirements for a railway subsystem

Module 9: Assurance

- Gain insight into verification, validation, and cybersecurity case creation
- Learn best practices for integration and handover processes
- Understand the role of independent cybersecurity assessors
- See how assurance activities ensure system compliance

ACTIVE LEARNING

Activity - Work through an example process of verification of a cybersecurity system

Module 10: Operation, Maintenance, and Disposal

- Learn how to manage incidents and vulnerabilities effectively
- Explore strategies for security monitoring and patch management
- Understand best practices for remote access and maintenance
- Discover how to address cybersecurity during decommissioning

ACTIVE LEARNING

Activity - Respond to a simulated cybersecurity incident in an interactive scenario

Module 11: Legacy Systems and Role Competence

- Identify risks and implement countermeasures for legacy systems
- Learn the basics of zoning, defence-in-depth, and risk analysis
- Explore the European Cyber Skills Framework and role definitions
- Discover best practices for training and asset inventory management

ACTIVE LEARNING

Activity - Develop a risk mitigation plan for a legacy railway system, identifying what is and is not possible to achieve

Module 12: Good Practices and Conclusion

- Review key lessons from the course and future applications
- Learn about secure coding practices and memory-safe languages
- Explore tools like CyRail for enhancing rail cybersecurity
- Discover best practices for managing cyber risks in rail

ACTIVE LEARNING

Quiz: A final multiple-choice quiz to test your knowledge and share your insights

Howard Parkinson

Dr Howard Parkinson is a Chartered Engineer contributing to global standards in railway safety, software and systems engineering. With over 20 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.

A Fellow of the Institution of Mechanical Engineers (FIMechE) and a member of the Institution of Railway Signal Engineers (MIRSE), Howard holds a doctorate in Mechanical and Aeronautical Engineering from the University of Manchester. Alongside consultancy and research, he delivers specialised training in engineering, safety, risk management, European interoperability, and railway legislation.

Dan Basher

Dan Basher is an accomplished railway software and safety professional based in Lancaster, with expertise in systems and compliance. He has played a pivotal role in the collaboration between the University of Huddersfield and Digital Transit Limited, contributing to the development of RAPORS—an innovative tool designed to support regulatory compliance in rail safety critical software development.

With a global outlook, Dan delivers training programmes on Safety Critical Software, OT cybersecurity, focusing on key standards such as EN50716. His work is dedicated to strengthening safety and cybersecurity practices worldwide, while fostering resilience and growth within the railway sector.

CENELEC IEC63452 and TS50701 - Rail Cyber Security

BOOK NOW

Click Here for Schedules and Pricing

+61 (2) 9080 4399
training@informa.com.au

Run This Course In-Company

+61 (2) 9080 4370
Inhouse@informa.com.au

ABOUT INFORMA CONNECT ACADEMY

Informa Connect Academy

Informa Connect Academy is a premier provider of global education and training solutions that caters to a diverse range of professionals, industries, and educational partners. We are dedicated to promoting lifelong learning and are committed to offering learners expert guidance, training, and resources to help them stay competitive in a rapidly changing world.

Our comprehensive range of courses and programmes are tailored to meet the needs of all professionals, from aspiring specialists to seasoned experts. We partner with elite academic organisations and industry leaders with unmatched expertise in their respective fields to deliver an exceptional learning experience.

ABOUT TIMINGS, PRICING AND DOCUMENTATION

Course fees include documentation, luncheon and refreshments for in-person learners. Delegates who attend all sessions and successfully complete the assessment, will receive a Informa Certificate and any applicable partner certificates. A hard copy will be provided to in-person learners and a soft-copy will be provided to virtual learners.

AVOID VISA DELAYS – BOOK NOW

Delegates requiring visas should contact the hotel they wish to stay at directly, as soon as possible.

To avoid delays, please ensure you apply for your visa several weeks before your intended travel date. Visa processing times can vary.

REGISTRATION, PAYMENTS AND CANCELLATION

All registrations are subject to our terms and conditions which are available at https://informaconnect.com/delegate-terms-and-conditions**.** Please read them as they include important information. By submitting your registration, you agree to be bound by the terms and conditions in full. All registrations are subject to acceptance by Informa Connect which will be confirmed to you in writing.

A confirmation letter and invoice will be sent upon receipt of your registration. Please note that full payment must be received prior to the course. Only those delegates whose fees have been paid in full will be admitted to the course.

For full cancellation details, please visit https://informaconnect.com/delegate-terms-and-conditions. All cancellations must be sent by email to training@informa.com.au marked for the attention of Customer Services Cancellation. Due to unforeseen circumstances, Informa Connect reserves the right to cancel the course, change the programme, alter the venue, speaker or topics. For full details, please visit www.informaconnect.com/academy.

View our upcoming
Rail Courses

Informa Connect
Academy

If you have any questions about the course or applying, please contact us on:

www.informaconnect.com/academy

training@informa.com.au

+61 (2) 9080 4399