CENELEC TS 50701 - Rail Cyber Security

This course is based upon the new railway cybersecurity-specific CENELEC standards, 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.**

BLENDED LEARNING/ONLINE PROGRAM | 5 Self-Paced Modules + 3 Live Interactive Sessions

12 February - 22 March 2024 | 12 August - 20 September 2024

Online Program

REGISTER NOW
www.informaconnect.com/academy

Course Information

Key Learning Objectives

- 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 TS70101 and how it can improve cybersecurity across the entire railway

Who Will Benefit

This blended CENELEC 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.

Course Information

About the Course

'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 CENELEC 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 CENELEC standards, 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.

Meet Your Course Director

Howard Parkinson

Howard is a chartered engineer with over 20 years of experience in the international railway industry, more recently as an independent consultant, researcher and trainer. He has experience in signaling, rolling stock, infrastructure and railway systems projects at a senior level and has just finished an assignment in Australia working on systems integration for automatic train protection.

His project positions at senior levels have included systems assurance manager, senior project manager, lead safety assessor, and head of systems engineering and safety. He has had experience in metro, tram and heavy rail (conventional and high speed).

Howard has expertise in systems engineering, compliance, safety /notified body assessment, safety and reliability engineering, the latest safety standards, European interoperability and UK legislation.

His current research interests include safety engineering in the railway, accident investigation and systems engineering. Howard has been deployed internationally in countries including: Australia, Korea, Germany, The Netherlands, UK, Croatia, Saudi Arabia, Canada and China. In addition to his consulting and research work, Howard designs, develops and delivers training to industry in the areas of engineering, safety and risk management.

Howard holds a doctorate from the department of mechanical and aeronautical engineering at the University of Manchester and a postgraduate certificate in education. He is a registered chartered engineer in the United Kingdom, a fellow of the Institution of Mechanical Engineers (FIMechE), and a member of the Institution of Railway Signal Engineers (MIRSE) including the Australasian branch.

Course Outline

MODULE 1

Introduction to Cyber Security in Railway Systems

- Setting the scene
- Threat landscape in the railway domain
- Safety and security
- Terminology
- Railway cybersecurity challenges
- Risk factors

MODULE 2

Cyber Security Incidents, including:

- Lodz Tram Cyber Attack
- Stuxnet Cyber Attack
- San Francisco Municipal Transportation Authority Ware Attack
- Deutsche Bahn Ransomware Attack

MODULE 3

Cyber Security Standards and Schemes, including:

- IEC 62443 Series and ISO27001

MODULE 4

TS50701 and the Railway system

- Introduction
- Railway asset model
- Railway physical architecture model
- High-level railway zone model

MODULE 5

Cybersecurity within a railway application lifecycle

- Railway application and product lifecycles

- Activities, synchronisation and deliverables
- Cybersecurity context and cybersecurity management plan
- Relationship between cybersecurity and essential functions
- Cybersecurity assurance process

MODULE 6

System definition and initial risk assessment

- Identification of the system under consideration
- Initial risk assessment
- Partitioning of the SuC
- Output and documentation

MODULE 7

Detailed risk assessment

- General aspects
- Establishment of cybersecurity requirements
- General guidance on risk assessment including setting security levels (SL)

MODULE 8

Cybersecurity requirements

- Objectives
- System security requirements
- Apportionment of cybersecurity requirements

MODULE 9

Cybersecurity assurance and system acceptance for operation

- Overview
- Cybersecurity case

- Cybersecurity verification
- Cybersecurity validation
- Cybersecurity system acceptance

MODULE 10

Operational, maintenance and disposal requirements

- Vulnerability management
- Security patch management

MODULE 11

TS50701 Appendices and Guidance (Informative)

MODULE 12

Conclusions and Test

February – March 2024		
Live Interactive Session:	**22 February**	**18:00 AEDT** (22 February - 07:00 GMT)
Live Interactive Session:	**7 March**	**18:00 AEDT** (7 March - 07:00 GMT)
Live Interactive Session:	**21 March**	**18:00 AEDT** (21 March - 07:00 GMT)

August – September 2024		
Live Interactive Session:	**22 August**	**17:00 AEST** (22 August - 07:00 GMT)
Live Interactive Session:	**5 September**	**17:00 AEST** (5 September - 07:00 GMT)
Live Interactive Session:	**19 September**	**17:00 AEST** (19 September - 07:00 GMT)

CENELEC TS 50701 - Rail Cyber Security

Easy Ways to Register

www.informaconnect.com/academy   +61 (02) 9080 4399   training@informa.com.au

CENELEC TS 50701 - Rail Cyber Security

Course Code	Location/ Format	Course Dates	Standard Price	
P24GR07ON	Online Program	12 February - 22 March 2024	$2,695.00 + $269.50 GST	$2,964.50
P24GR07ON02	Online Program	12 August - 20 September 2024	$2,695.00 + $269.50 GST	$2,964.50

Great Savings:
When you book **4 or more** participants! **Call us** today on **+61 (2) 9080 4399** or email **training@informa.com.au** to take advantage of the discount offer.

Terms, Privacy Policy & Updating Your Details: Please visit us at **www.informaconnect.com/terms-and-policies** for terms and conditions and privacy policy.
Database amendments can be sent to **database@informa.com.au** or call **+61 (2) 9080 4399.**

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.

ON-SITE & CUSTOMISED TRAINING

Informa Connect Academy has a long-standing track record of delivering very successful customised learning solutions achieving real and measurable value for our clients through our senior training consultants. If you have 8+ interested people, an on-site course can be the ideal solution – giving you the opportunity to customise our course content to your specific training needs, as well as attracting significant savings compared to public course costs.

WHY CHOOSE ON-SITE WITH INFORMA CONNECT ACADEMY?

1. **Custom design –** Together, we will identify the best blended learning solution for your culture, your people and your training objectives.

2. **Quality assured –** We design market-leading training programs, concepts and methodologies, with a 400+ course portfolio. Our rigorously selected 900+ instructor faculty are recognised experts in their field. Quality of their content and delivery methods is assured through continuous monitoring and evolution.

3. **On-site training** is a cost effective way to train your people and achieve your defined outcomes.

Speak with **Sushil Kunwar** on **+61 (2) 9080 4370** to discuss your customised learning solution, or email **inhouse@informa.com.au**