

COURSE AGENDA

Cyber-Physical Systems (CPS)

A professional training programme focused on connected physical-digital systems, intelligent infrastructure, operational efficiency and secure technology integration

15 Hours Duration	eLearning Primary format	English Language
-----------------------------	------------------------------------	----------------------------

Primary format	eLearning course delivered through the digital learning platform
Available on request	Live trainer-led online delivery or in-house classroom training
Contact us	Request a tailored quote for your organisation

About Us

This course is delivered by a team with strong expertise in cybersecurity, digital resilience, emerging technologies and secure digital transformation. Our work is grounded in internationally recognised standards, European regulatory requirements and practical experience supporting organisations operating in complex, regulated and technology-driven environments.

INFOSEC CENTER holds ISO/IEC 27001 certification for information security management and, reflecting a structured and responsible approach to cybersecurity, data protection, governance and AI-enabled technologies. The organisation is also recognised as an **EASA-approved** training provider for specialised aviation cybersecurity training, aligned with European aviation safety and information security requirements.

Our innovation capacity has been recognised through the **Impact Stars distinction** at the **Deloitte Technology Fast 50**, awarded for the innovation delivered by our Machine Learning platform. This reflects our commitment to practical, high-impact technology solutions that combine advanced digital capabilities with real business and societal value.

We are actively connected to European digital innovation networks, including the **European DIGITAL SME Alliance** and the **BSC AI Factory Incubation Program**, contributing to secure, competitive and responsible digital transformation across Europe.

Our broader innovation platform, **FACTORY X.0**, supports the secure transformation of industrial and digital ecosystems by integrating cybersecurity, automation, artificial intelligence, industrial digitalisation and advanced technology adoption, with a focus on resilience, compliance and sustainable innovation.

We support organisations in understanding cyber risk, strengthening digital infrastructure, improving governance, preparing for regulatory compliance and building a stronger security culture across aviation, industry, education, public services and digital business.

Why This Course Matters

Cyber-Physical Systems are a key component of modern digital transformation. They connect the physical world with digital systems, enabling organisations to monitor, control and optimise devices, equipment, infrastructure and operational processes in real time. Through sensors, actuators, embedded systems, communication networks, data platforms and intelligent control mechanisms, CPS technologies allow physical operations to become more responsive, measurable and efficient.

Cyber-Physical Systems can support automation, reduce errors, improve productivity, enable real-time monitoring, strengthen quality control and support faster, data-driven decision-making. In industrial, logistics, healthcare, infrastructure, mobility and service environments, CPS can help organisations improve operational visibility and respond more effectively to complex business conditions.

At the same time, the integration of CPS requires careful planning. These systems depend on the secure interaction between physical devices, software, networks, data flows and control mechanisms. Poorly designed or poorly secured CPS environments can introduce operational disruption, safety risks, data exposure, interoperability issues and cybersecurity vulnerabilities.

This course addresses those challenges directly. It is designed for learners who want to understand what Cyber-Physical Systems are, how their components interact, which technologies support them, how they can be integrated into SME operations and how they should be managed and secured throughout their lifecycle.

Participants will leave this course equipped to:

- Understand the definition, characteristics and core principles of Cyber-Physical Systems
- Identify the main components of CPS, including sensors, actuators, embedded systems, control systems and communication networks
- Explain how physical and digital components interact to create intelligent operational capabilities

- Understand the role of IoT, cloud computing, big data, artificial intelligence, machine learning and real-time systems in CPS environments
- Evaluate CPS applications in SME operations, including automation, monitoring, control and data-driven decision-making
- Plan the integration of CPS technologies based on operational needs, resources, costs, scalability and technical maturity
- Understand the main cybersecurity, risk management, monitoring and governance requirements for CPS environments

Course Overview

Course Title	Cyber-Physical Systems (CPS)
Total Duration	15 Hours
Primary Delivery Format	eLearning course delivered through the digital learning platform
Optional Delivery Formats	Available on request as live trainer-led online delivery or in-house classroom training
Target Audience	Professionals seeking to understand, evaluate, integrate and manage Cyber-Physical Systems in organisational, industrial or business contexts
Prerequisites	No prior CPS engineering experience required; basic digital literacy and general understanding of operational or business processes are recommended
Language	English

Planning & Delivery Options

The standard version of this programme is structured as an eLearning course, allowing participants to progress through the agenda in a flexible and accessible format. This option is suitable for organisations that need scalable delivery, consistent learning materials and clear assessment through the digital platform.

At the client's request, the same course agenda can also be delivered with a live trainer, either online or in an in-house classroom format. These options are recommended when the organisation wants direct interaction with the trainer, applied discussions based on internal workflows or a more guided learning experience.

For organisational enrolment, adapted delivery or group implementation, please request a tailored quote.

Learning Approach

The learning approach is built on four pillars:

01 Conceptual Clarity

Each module introduces Cyber-Physical Systems in a clear and structured way before moving into technical components, integration strategies and management considerations. Learners build a solid understanding of CPS terminology, architecture, physical-digital interaction, automation, feedback, interconnectivity and real-time control.

02 Applied Learning

Case studies, scenario-based exercises and practical examples connect CPS concepts to real organisational needs. Learners explore how CPS can improve operational efficiency, productivity, quality, monitoring, decision-making and process control in small and medium-sized enterprises.

03 Security & Governance Integration

Cybersecurity, compliance, interoperability, risk management, access control, data protection and operational resilience are embedded throughout the course. CPS is presented as a connected operational environment that must be designed, implemented and monitored with strong attention to safety, security and governance.

04 Progressive Assessment

Each module includes a knowledge check through the eLearning platform. A final comprehensive assessment consolidates learning across all modules and supports the validation of knowledge gained throughout the programme.

Detailed Course Agenda

Module 01 Introduction to Cyber-Physical Systems

Learning Objectives

- Develop a clear understanding of what Cyber-Physical Systems are and how they connect physical processes with digital control, monitoring and data-driven decision-making.
- Understand the fundamental characteristics of CPS, including integration between physical components, computational systems, communication networks and control mechanisms.
- Identify the essential components of a CPS, including sensors, actuators, embedded systems, controllers, software platforms and communication infrastructure.
- Understand how physical and cyber components interact within a CPS to achieve desired operational functionality.
- Understand the relevance of CPS for enterprises, particularly in relation to efficiency, quality improvement, operational visibility and productivity.

- Examine the importance of regulations and standards in CPS environments, especially for ensuring system security, interoperability, reliability and safe integration.
- Recognise why CPS adoption requires alignment between operational needs, technical capabilities, security requirements and organisational objectives.

Tools & Methodology

eLearning modules, optional live trainer-led sessions.

Assessment: Knowledge test via the eLearning platform.

Module 02 Key Technologies and Components of Cyber-Physical Systems

Learning Objectives

- Understand the role of the Internet of Things in CPS environments and how connected devices collect, transmit and support the monitoring of physical systems.
- Discuss the benefits of cloud infrastructure for implementing, managing and expanding CPS capabilities.
- Identify the importance of big data and data analytics in CPS, especially when large volumes of operational data are generated by sensors, machines and connected devices.
- Discuss practical applications of machine learning and artificial intelligence in CPS environments, including predictive maintenance, process optimisation and adaptive control.
- Explore the hardware and software components used in embedded systems for CPS implementation.
- Identify communication networks, protocols and standards used in CPS for data transmission between components and devices, including NFC, ZigBee, 5G and MQTT.

- Explore real-time systems and understand how they support fast processing and response to events or changes in the physical environment.

Tools & Methodology

eLearning modules, optional live trainer-led sessions, case studies.

Assessment: Knowledge test via the eLearning platform.

Module 03 Integrating CPS into Operations

Learning Objectives

- Explore how Cyber-Physical Systems can generate significant improvements in operations, including efficiency, quality, productivity, process visibility and operational control.
- Analyse how CPS can help organisations reduce operational errors, improve workflow coordination and increase responsiveness to changes in the business or production environment.
- Learn how to develop a customised CPS integration strategy based on available resources, budget, operational priorities and technical capabilities.
- Evaluate cost, scalability, interoperability, technical maturity and implementation complexity when selecting CPS technologies.
- Understand how to plan and manage CPS implementation, including infrastructure readiness, staff training, process adaptation and change management.
- Develop a framework for monitoring and evaluating CPS performance after implementation.

Tools & Methodology

eLearning modules, optional live trainer-led sessions, case studies.

Assessment: Knowledge test via the eLearning platform.

Module 04 CPS Management, Monitoring and Performance Control

Learning Objectives

- Understand how Cyber-Physical Systems should be managed throughout their operational lifecycle, from implementation to monitoring, maintenance and optimisation.
- Understand how real-time monitoring supports faster detection of operational anomalies, performance degradation, equipment issues or process inefficiencies.
- Explore methods for controlling CPS performance and ensuring that systems remain aligned with operational requirements and business objectives.
- Identify the importance of maintenance, calibration, software updates and system validation in CPS environments.
- Understand how CPS data can be used to support continuous improvement, process optimisation and evidence-based decision-making.
- Examine how CPS management should address interoperability, system dependencies, vendor coordination, infrastructure limitations and operational continuity.
- Understand the importance of documenting CPS architecture, system behaviour, maintenance activities, changes and incidents.

Tools & Methodology

eLearning modules, optional live trainer-led sessions, case studies.

Assessment: Knowledge test via the eLearning platform.

Module 05 CPS Security and Risk Management

Learning Objectives

- Identify and evaluate risks specific to Cyber-Physical Systems, including cybersecurity threats, operational disruption, data compromise, unauthorised access, unsafe system behaviour and communication failures.

- Understand how vulnerabilities in digital components can affect physical systems, equipment, operational processes and business continuity.
- Learn how to implement risk management measures for CPS environments, including risk identification, risk assessment, mitigation planning and ongoing monitoring.
- Understand the importance of CPS security policies and how they support consistent protection of systems, networks, data and operational processes.
- Define security procedures for CPS environments and understand how they should be applied across devices, networks, software, users and operational workflows.
- Explore the role of encryption, authentication, authorisation and access control in protecting CPS data and system functions.
- Examine the relationship between CPS security, operational safety, business continuity and organisational resilience.
- Understand why CPS security must be integrated from the design phase and maintained throughout the full system lifecycle.

Tools & Methodology

eLearning modules, optional live trainer-led sessions, case studies.

Assessment: Knowledge test via the eLearning platform.

Module 06 Course Closing & Consolidation

Learning Objectives

- Consolidate understanding across all previous modules through a structured review of CPS concepts, components, technologies, integration strategies, management requirements and security principles.
- Revisit the most important technical and business themes covered throughout the programme.
- Prepare for the final assessment by reviewing key definitions, practical applications and decision-making criteria related to CPS adoption and implementation.

Tools & Methodology

Final online assessment, optional trainer review session, individual feedback where applicable.

Assessment & Certification

Assessment in this course is continuous, formative and cumulative. Rather than relying on a single high-stakes examination, the programme uses a layered approach that supports learning throughout and ensures that the final certification reflects a genuine command of the material.

Assessment Type	Description
Module Knowledge Checks	Each module is followed by a knowledge test delivered through the eLearning platform. These tests reinforce learning at the point of completion and allow learners to identify any gaps before progressing.
Final Assessment	A comprehensive online test covering all modules is completed at the end of the course. This assessment evaluates the learner's overall understanding and ability to apply key concepts across the programme.
Trainer Feedback	When trainer-led delivery is requested, live session interactions and final assessment performance can be reviewed by the course trainer, who provides structured feedback to support ongoing professional development.
Certificate of Completion	Participants who successfully complete the course and final assessment may receive a certificate of completion issued by INFOSEC CENTER, confirming participation and successful completion of the training programme.

Closing Note

The organisations that benefit most from CPS are those that approach implementation with a clear understanding of their operational needs, technical constraints, security requirements and long-term business objectives. CPS adoption requires more than deploying sensors or software. It requires planning, integration, governance, monitoring and continuous improvement.

This course has been designed with that understanding at its core. It aims to prepare learners not only to understand CPS concepts and technologies, but also to evaluate their organisational relevance, support implementation planning and recognise the security and management requirements involved.

By combining conceptual clarity, applied examples, technical awareness and governance considerations, the programme helps learners build a practical and responsible perspective on Cyber-Physical Systems. The knowledge developed here is relevant across sectors where physical processes, connected devices, data and digital control increasingly interact.

We hope this programme supports your development as a confident, capable and responsible professional in the field of connected physical-digital systems. The perspective you build here will help you contribute meaningfully to operational transformation while maintaining the security awareness, technical judgement and governance mindset that modern organisations require.

We wish you a productive and insightful learning experience.

Primary format: eLearning course

Live trainer-led and in-house delivery available on request

Request a quote: contact@edkore.com