**Smart Infrastructure Engineering Training Programme Proposal**

**Evolving Sustainability and Security for a Net Zero Future**

**March 2025**

# Contents

[1. Smart Infrastructure Engineering Training Programme Overview 1](#_Toc192538073)

[2. Programme Structure 2](#_Toc192538074)

[3. Programme Audience and Delivery 3](#_Toc192538078)

[4. Overview of Foundation Modules 4](#_Toc192538086)

[4.1 Foundation Module Summaries 4](#_Toc192538087)

[4.2 Assessment of Foundation Modules 5](#_Toc192538089)

[5. Overview of Advanced Cyber-Physical Security and Resilience Modules 6](#_Toc192538090)

[5.1 Advanced Module Summaries 4](#_Toc192538087)

[5.2 Assessment of Advanced Modules 7](#_Toc192538092)

# Smart Infrastructure Engineering Training Programme Overview

**Introduction**

The transition to net zero and the digitalisation of critical infrastructure require a skilled workforce capable of designing, implementing, and securing smart, connected, and sustainable systems.

The Smart Infrastructure Engineering Training Pathway is designed to equip professionals with the technical knowledge and interdisciplinary competencies needed to develop resilient and sustainable infrastructure systems. This programme supports the UK’s infrastructure transformation agenda by addressing the growing demand for digital, data, and cyber capabilities across sectors such as utilities, transport, and construction.

The pathway will:

* Close the skills gap by reskilling and upskilling professionals in smart systems, cyber-physical security, and net zero-aligned engineering.
* Support national growth and innovation through a digitally and sustainability-literate workforce.
* Provide clear career progression, from core digital infrastructure skills to advanced specialisms.

The training programme comprises 11 foundation modules designed to equip learners with core knowledge in digital infrastructure, data intelligence, secure systems, and environmental sustainability. In addition, a specialist Cyber-Physical Security and Resilience pathway is available, featuring 6 advanced modules that build on the foundation. This pathway focuses on advanced OT security, real-time threat detection, incident response, and resilience planning to protect critical infrastructure systems from evolving cyber and environmental threats.

While the Cyber-Physical Security and Resilience pathway is the first advanced specialisation, further pathways will be developed in the future, including:

* Net Zero and Sustainability – Focusing on low-carbon infrastructure solutions and renewable integration.
* Smart Building and Built Environment Automation – Addressing building control systems, digital twins, and IoT-enabled infrastructure.

These specialisations will enable learners to pursue in-depth expertise in emerging fields that are critical to the future of smart, sustainable infrastructure.

# Programme Structure

1. **Foundation Modules**

Foundation Modules – Digital, Data, Secure Systems and Sustainable and Environmental Systems.

All learners will complete the following foundation modules, developing baseline knowledge in digital infrastructure, data-driven systems, secure integration and environmental sustainability:

**Digital Foundations:**

* Module 1: Foundations of Smart Infrastructure and Net Zero
* Module 2: Smart Infrastructure Systems and IoT
* Module 3: Telecommunications and Networking for Infrastructure

**Data and Intelligence:**

* Module 4: Data Analysis for Smart Infrastructure
* Module 5: AI and Machine Learning in Infrastructure

**Secure and Integrated Systems:**

* Module 6: Cybersecurity for Smart Infrastructure
* Module 7: Software and Hardware Integration for Smart Infrastructure

**Sustainable and Environmental Systems:**

* Module 9: Energy Systems Principles
* Module 10: Renewable Energy Technologies
* Module 11: Environmental Data Collection

1. Advanced Cyber-Physical Security and Resilience Modules

Learners seeking specialist skills in securing critical infrastructure systems can progress beyond the foundation modules into this advanced pathway:

* Module A1: ICS, SCADA Security, and Operational Technology (OT) Protocols
* Module A2: OT/IoT Network Architecture and Segmentation
* Module A3: Incident Response, Monitoring, and Forensics for OT/IoT
* Module A4: Resilience Planning, Disaster Recovery, and Climate Adaptation
* Module A5: OT Threat Intelligence and Vulnerability Management
* Module A6: Safety-Critical Systems and Regulatory Compliance for OT

# Programme Audience and Delivery

**Target Audience and Industry Applications**

This training pathway is designed for engineers, IT professionals, urban planners, data analysts, sustainability specialists, and cybersecurity experts across:

* Critical National Infrastructure (CNI) – Utilities, transport, energy, manufacturing.
* Public Sector and Government – Local Authorities, National Agencies.
* Construction and Smart Buildings – Urban development, Built Environment Automation.
* Health and Education – Smart hospitals, energy-efficient campuses.
* Cybersecurity and Data Centres – OT/IoT security in critical systems.

**Delivery Model**

This programme will be delivered using a blended learning approach, combining theoretical knowledge and practical skills:

* Online Learning: Self-paced digital modules with interactive content.
* Hands-on Labs & Simulations: Application of real-world tools and smart infrastructure technologies.
* Industry Case Studies: Learning from UK and international best practices.
* Mentoring & Career Pathways: Guidance from industry experts and professional networks.

**Proposed Certification or Micro-Credentials**

Participants will receive modular credentials, enabling stackable qualifications:

* Smart Infrastructure Foundations Certification – Completion of Core Modules 1–11.
* Advanced Cyber Resilience Specialist – Completion of Core + Advanced Pathway (A1–A4).

**Programme Impact This pathway will strengthen the workforce’s capability to deliver secure, smart, and net zero-aligned infrastructure by:**

* Filling digital and cyber skills gaps in infrastructure sectors.
* Enabling sustainable infrastructure design and operations.
* Driving efficiency, resilience, and long-term competitiveness.
* Creating clear career progression pathways.

# Overview of Foundation Modules

**4.1 Foundation** Module summaries

Detailed module specifications, including an overview and learning outcomes for each foundation module, are provided in Appendix 1.

1. **Foundations of Smart Infrastructure and Net Zero**

* Understanding net zero and smart infrastructure goals: How digital and smart infrastructure supports decarbonisation and sustainability.
* Key components and system integration: Introduction to smart systems, renewable energy, and energy-efficient infrastructure.
* Policy and regulatory context: Overview of climate policies and regulations driving smart infrastructure development.

1. **Smart Infrastructure Systems and IoT**
   * Understanding smart infrastructure components: sensors, data analytics, AI, and IoT.
   * Practical applications in roads, bridges, utilities, and smart cities.
   * Case studies on real-world infrastructure innovations.
2. **Telecommunications and Networking for Infrastructure**
   * Fundamentals of networking: IP addressing, routers, switches.
   * Wireless and wired communication technologies (5G, fibre optics, LoRaWAN, LPWA).
   * Network resilience and infrastructure connectivity.
3. **Data Analysis for Smart Infrastructure**
   * Data handling, statistical methods, and predictive analysis.
   * Visualisation techniques using industry-standard tools.
   * Real-world applications in infrastructure planning and maintenance.
4. **AI and Machine Learning in Infrastructure**
   * Predictive maintenance and automation using AI.
   * Machine learning applications in smart infrastructure.
   * Ethical and practical considerations in AI adoption.
5. **Cybersecurity for Smart Infrastructure**
   * Cyber threats in Operational Technology (OT) and Information Technology (IT).
   * Securing smart infrastructure systems and IoT networks.
   * Compliance with cybersecurity standards.
6. **Software and Hardware Integration for Smart Infrastructure**
   * Sensor and control system integration.
   * Embedded systems and cloud-based infrastructure solutions.
   * Hardware-software troubleshooting and optimisation.
7. **Cloud Computing for Smart Infrastructure**
   * Cloud services (AWS, Azure, Google Cloud) for data management.
   * Scalability, security, and cloud-based infrastructure monitoring.
   * Implementing smart infrastructure solutions using cloud platforms.
8. **Energy Systems Principles**
   * The role of smart grids, distributed energy, and efficient energy systems in smart infrastructure.
   * Energy efficiency practices: Techniques for reducing energy consumption and improving system performance.
   * Integration of renewable and smart systems: How energy systems interface with digital infrastructure to support net zero.
9. **Renewable Energy Technologies**
   * Overview of solar, wind, hydro, and other renewable energy sources.
   * Challenges and solutions for integrating renewables into smart infrastructure.
   * Real-world examples of renewable energy deployment in infrastructure projects.
10. **Environmental Data Collection**
    * Cloud services (AWS, Azure, Google Cloud) for data management.
    * Scalability, security, and cloud-based infrastructure monitoring.
    * Implementing smart infrastructure solutions using cloud platforms.

**4.2** Assessment of Foundation Modules

To ensure that learners achieve the desired foundational knowledge and practical skills, a combination of formative and summative assessments will be employed.

*Formative assessments* will include regular quizzes to provide ongoing feedback on learners' understanding of fundamental concepts, helping to identify areas that may require additional focus. Laboratory hands-on experiments and simulations will be conducted to assess the practical application of theoretical knowledge, to enhance skill development.

*Summative assessments* will include multiple choice tests, including sections with short-answer questions and problem-solving exercises to evaluate learners' comprehension of the course material.

# Overview of Advanced Cyber-Physical Security and Resilience Modules

**5.1 Advanced** Module summaries

Detailed module specifications, including an overview and learning outcomes for each advanced module, are provided in Appendix 2.

**Module A1: Industrial Control Systems (ICS) , SCADA Security, and OT Protocols**

* ICS, SCADA, DCS, PLCs: Core components and vulnerabilities.
* OT-Specific Protocols: Modbus, DNP3, BACnet, and security considerations.
* Practical OT security case studies and risk assessments.

**Module A2: OT/IoT Network Architecture and Segmentation**

* OT/IT Segmentation: Reducing lateral movement risks.
* Designing resilient OT networks.
* Best practices for zoning and perimeter defence.

**Module A3: Incident Response, Monitoring, and Forensics for OT/IoT**

* Real-time monitoring: Recognising OT/IoT anomalies.
* Incident containment & response playbooks.
* OT-Specific Forensics: Collecting and analysing artefacts in industrial settings.
* Basic automation using Python/PowerShell for analysis and incident support.

**Module A4: Incident Response, Monitoring, and Forensics for OT/IoT**

* Resilience planning for OT systems (cyber recovery + physical threats).
* Business continuity and disaster recovery planning for smart infrastructure.
* Climate resilience and system adaptation (flooding, extreme weather, power disruptions).

**Module A5: OT Threat Intelligence and Vulnerability Management**

* Understanding emerging OT/IoT threats and attack techniques.
* Assessing and managing OT vulnerabilities.
* Operationalising threat intelligence feeds for OT environments.
* Vendor patching and risk-based mitigation strategies.

**Module A6: OT Threat Intelligence and Vulnerability Management**

* Safety-critical infrastructure risks in OT environments.
* Linking safety and security in OT system design.
* Regulatory compliance: Health & Safety Executive (HSE), IEC 61508 (Functional Safety), and other safety/security regulations.

**5.2** Assessment of Advanced Modules

To ensure that learners achieve the desired advanced competencies, a combination of formative and summative assessments will be employed.

*Formative assessments* will include regular quizzes as well as case study analyses to examine real-world scenarios, and engage in group discussions, to develop analytical skills and apply theoretical knowledge to practical situations.

*Summative assessments* will include extended multiple-choice tests, including sections with short and long answer questions, and problem-solving exercises.

Appendix 1 - Smart Infrastructure Engineering – Foundation Module

**Module 1: Foundations of Smart Infrastructure and Net Zero**

**Overview**:

This module provides a foundational understanding of the relationship between smart infrastructure and achieving net zero goals. It introduces learners to the core principles of decarbonisation, sustainability and how digital technologies support the transition to low-carbon infrastructure systems. Learners will explore the key components of smart infrastructure, including the integration of renewable energy, energy efficiency, and the convergence of digital and physical infrastructure. The module also examines the UK and international policy landscape driving net zero commitments and the regulatory frameworks shaping the development of sustainable infrastructure.

**Learning Outcomes:**

By the end of this module, learners will be able to:

1. Explain the concept of net zero and the role smart infrastructure plays in achieving decarbonisation and sustainability.
2. Identify the key components of smart infrastructure and their role in enhancing energy efficiency and renewable energy integration.
3. Describe how digital and physical systems converge to optimise the performance of infrastructure networks.
4. Analyse the impact of UK and international climate policies, including net zero targets and sustainability regulations, on infrastructure development.
5. Evaluate how policy, regulation, and sustainability drivers influence decision-making in smart infrastructure projects.

**Module 2: Smart Infrastructure Systems and IoT**

**Overview:**  
This module provides foundational knowledge on smart infrastructure systems, focusing on how sensors, IoT, AI, and machine learning are integrated into modern infrastructure such as roads, bridges, and utilities. Participants will explore real-world applications and case studies.

**Learning Outcomes:**

By the end of this module, learners will be able to:

1. Explain the role of IoT and smart systems in infrastructure management.
2. Identify the types of sensors used in smart infrastructure and their applications.
3. Describe the data flow in IoT-enabled infrastructure, from collection to analysis.
4. Discuss real-world applications of smart infrastructure, such as traffic monitoring and energy efficiency.
5. Evaluate the benefits and challenges of implementing smart infrastructure solutions.

**Module 3: Telecommunications and Networking**

**Overview:**  
This module introduces the fundamentals of networking, telecommunications, and communication protocols relevant to smart infrastructure. Topics include IP networking, routers, switches, and emerging technologies such as 5G, fibre optics, and LoRaWAN.

**Learning Outcomes:**

By the end of this module, learners will be able to:

1. Explain the basic concepts of networking, including IP addressing, routers, and switches.
2. Describe the role of telecommunications in smart infrastructure systems.
3. Compare different wireless and wired communication technologies (5G, fibre optic, LoRaWAN, LPWA).
4. Analyse the importance of latency, bandwidth, and reliability in smart infrastructure networks.
5. Apply networking principles to design basic communication systems for smart infrastructure projects.

**Module 4: Data Analysis for Smart Infrastructure**

**Overview:**  
This module introduces data analysis techniques essential for managing smart infrastructure systems. It covers data collection, cleaning, statistical analysis, and visualisation using common tools.

**Learning Outcomes:**

By the end of this module, learners will be able to:

1. Explain the importance of data in smart infrastructure decision-making.
2. Use basic data handling techniques (data cleaning, formatting, and transformation).
3. Apply simple statistical methods to analyse infrastructure data.
4. Use visualisation tools to present infrastructure data insights.
5. Interpret real-world smart infrastructure datasets to drive decision-making.

**Module 5: AI and Machine Learning Concepts for Smart Infrastructure**

**Overview:**  
This module introduces AI and machine learning principles and their applications in predictive maintenance, data analysis, and automation in infrastructure systems.

**Learning Outcomes:**

By the end of this module, learners will be able to:

1. Define AI and machine learning and their relevance to smart infrastructure.
2. Explain how predictive analytics enhances infrastructure management.
3. Identify key AI-driven applications in smart infrastructure (e.g., automated monitoring, fault detection).
4. Understand the basics of training and deploying simple machine learning models.
5. Assess the ethical and practical implications of AI in infrastructure.

**Module 6: Cybersecurity Principles for Smart Infrastructure**

**Overview:**  
This module introduces cybersecurity best practices for IT and OT (Operational Technology) environments to protect infrastructure systems from cyber threats.

**Learning Outcomes:**

By the end of this module, learners will be able to:

1. Explain the fundamental principles of cybersecurity for IT and OT systems.
2. Identify common cyber threats in smart infrastructure and their potential impact.
3. Describe best practices for securing IoT devices and infrastructure networks.
4. Understand cybersecurity frameworks and compliance requirements.
5. Implement basic cybersecurity measures to protect infrastructure systems.

**Module 7: Software and Hardware Integration for Smart Infrastructure**

**Overview:**  
This module covers the integration of software and hardware components in smart infrastructure systems, including sensors, control systems, and data platforms.

**Learning Outcomes:**

By the end of this module, learners will be able to:

1. Understand the role of sensors and control systems in smart infrastructure.
2. Describe the interaction between hardware (e.g., embedded systems, IoT devices) and software (e.g., cloud platforms, AI models).
3. Integrate sensors with data processing systems to collect and analyse data.
4. Troubleshoot common hardware-software integration challenges.
5. Design a basic smart infrastructure solution combining hardware and software elements.

**Module 8: Cloud Computing for Smart Infrastructure**

**Overview:**  
This module explores cloud computing fundamentals, with a focus on cloud platforms like AWS, Azure, and Google Cloud for data storage, computation, and infrastructure management.

**Learning Outcomes:**

By the end of this module, learners will be able to:

1. Explain cloud computing concepts and their applications in smart infrastructure.
2. Compare major cloud service providers and their offerings for infrastructure management.
3. Demonstrate how to use cloud platforms for data storage and processing.
4. Understand cloud security and compliance considerations.
5. Deploy a cloud-based solution for monitoring and analysing smart infrastructure data.

**Module 9: Energy Systems Principles**

**Overview:**  
This module introduces the fundamentals of energy systems, focusing on the transition to smart grids, energy efficiency, and the integration of distributed and renewable energy sources. Learners will explore how energy systems underpin smart infrastructure and support net zero ambitions.

**Learning Outcomes:**

By the end of this module, learners will be able to:

1. Explain the role of energy systems in supporting smart infrastructure and achieving net zero goals.
2. Understand the operation and characteristics of smart grids and distributed energy systems.
3. Evaluate energy efficiency techniques and their application in infrastructure projects.

**Module 10: Renewable Energy Technologies**

**Overview:**  
This module provides an overview of key renewable energy technologies (solar, wind, hydro, etc.) and their integration into smart infrastructure systems. It examines how renewable energy contributes to reducing carbon emissions and supports sustainable infrastructure.

**Learning Outcomes:**

By the end of this module, learners will be able to:

1. Identify and describe common renewable energy technologies and their applications.
2. Assess the benefits and challenges of integrating renewable energy into infrastructure systems.
3. Analyse case studies of renewable energy implementation within smart infrastructure projects.

**Module 9: Environmental Data Collection**

**Overview:**  
This module focuses on techniques for collecting and analysing environmental data to support sustainable infrastructure management. Learners will explore the role of data in monitoring environmental performance, emissions, and resource usage.

**Learning Outcomes:**

By the end of this module, learners will be able to:

1. Describe methods for environmental data collection, including sensor systems and IoT applications.
2. Apply basic data analysis techniques to interpret environmental performance data.
3. Use environmental data to inform decision-making in infrastructure planning and management.

Appendix 2 - Smart Infrastructure Engineering – Advanced Modules

**Module A1: ICS, SCADA Security, and OT Protocols**

**Overview:**

This module provides an in-depth understanding of industrial control systems (ICS), SCADA, DCS, and PLCs, focusing on their security vulnerabilities and the OT-specific protocols that underpin critical infrastructure operations. Learners will explore the unique challenges of securing OT environments and gain practical knowledge of protocols such as Modbus, DNP3, and BACnet.

**Learning Outcomes:**

By the end of this module, learners will be able to:

1. Explain the architecture and operational role of ICS, SCADA, DCS, and PLC systems.
2. Identify vulnerabilities specific to industrial control systems.
3. Understand and evaluate OT-specific protocols, including Modbus, DNP3, and BACnet.
4. Conduct risk assessments for industrial environments.
5. Apply security measures to reduce risk in OT environments.

**Module A2: OT/IoT Network Architecture and Segmentation**

**Overview:**

This module focuses on the design and implementation of secure OT and IoT network architectures to protect infrastructure systems. Learners will explore network segmentation techniques, perimeter security, and best practices for reducing the risk of lateral movement within cyber-physical systems.

**Learning Outcomes:**

By the end of this module, learners will be able to:

1. Design secure OT/IoT network architectures aligned with industry best practices.
2. Implement network segmentation to isolate critical infrastructure systems.
3. Evaluate the effectiveness of perimeter defence and zoning strategies.
4. Identify and mitigate common network vulnerabilities in OT/IoT environments.
5. Integrate secure network design into wider infrastructure security planning.

**Module A3: Incident Response, Monitoring, and Forensics for OT/IoT**

**Overview:**

This module develops learners' capability to monitor OT/IoT systems in real-time, detect security incidents, and respond effectively. It also covers forensic investigation techniques specific to industrial systems, alongside the application of scripting and automation tools for security operations.

**Learning Outcomes:**

By the end of this module, learners will be able to:

1. Implement real-time monitoring solutions for OT/IoT systems.
2. Detect and analyse security anomalies within industrial environments.
3. Develop and execute incident response plans tailored to critical infrastructure.
4. Conduct forensic investigations in OT/IoT settings.
5. Use scripting (e.g., Python, PowerShell) to automate security analysis and response.

**Module A4: Resilience Planning, Disaster Recovery, and Climate Adaptation**

**Overview:**

This module equips learners with the knowledge and tools to strengthen the resilience of smart infrastructure systems against cyberattacks, operational failures, and climate-related disruptions. It covers business continuity planning, disaster recovery, and adaptive strategies for climate resilience.

**Learning Outcomes:**

By the end of this module, learners will be able to:

1. Conduct resilience and risk assessments for critical infrastructure systems.
2. Develop and implement business continuity and disaster recovery plans.
3. Design resilient infrastructure solutions accounting for both cyber and physical threats.
4. Evaluate the impact of climate change on critical systems and adapt accordingly.
5. Integrate resilience principles into infrastructure operations and security management.

**Module A5: OT Threat Intelligence and Vulnerability Management**

**Overview:**

This module introduces learners to the evolving landscape of OT threats and vulnerabilities. It focuses on gathering and interpreting threat intelligence, identifying vulnerabilities, and implementing proactive patch management and mitigation strategies in industrial environments.

**Learning Outcomes:**

By the end of this module, learners will be able to:

1. Interpret OT-specific threat intelligence and apply it to infrastructure protection.
2. Identify vulnerabilities in OT/IoT systems using industry tools.
3. Evaluate the impact of emerging threats on critical infrastructure.
4. Implement vulnerability management processes, including patching and risk-based prioritisation.
5. Develop proactive mitigation strategies to reduce OT security risks.

**Module A6: Safety-Critical Systems and Regulatory Compliance for OT**

**Overview:**

This module addresses the intersection of safety and security in OT environments, focusing on safety-critical systems and regulatory compliance. Learners will explore functional safety standards, the consequences of system failures, and the need to align cybersecurity with safety requirements.

**Learning Outcomes:**

By the end of this module, learners will be able to:

1. Explain the importance of safety-critical systems in OT environments.
2. Assess the relationship between operational safety and cybersecurity.
3. Apply key safety standards such as IEC 61508 and other sector-specific regulations.
4. Evaluate the consequences of system failures in safety-critical operations.
5. Integrate safety and security practices into the design and management of OT systems.