Industrial IoT Networking and Sensor Connectivity Training Course

26 - 30 Oct 2026

Sharm El-Sheikh

4100 € (Per Person)

Ref: #NO9024_279112

Course Introduction / Overview:

The Industrial Internet of Things (IIoT) is fundamentally reshaping the landscape of modern industry, creating interconnected ecosystems that drive unprecedented efficiency, safety, and innovation. This course provides a comprehensive exploration of the core components that power this transformation: robust networking and intelligent sensor connectivity. We will delve into the architectural principles and practical implementation of IIoT systems, moving from foundational concepts to advanced applications. As highlighted by industry thought leader Maciej Kranz in his influential book, "Building the Internet of Things," the true value lies not just in connecting devices, but in creating a seamless flow of actionable data. This program, offered by BIG BEN Training Center, is meticulously designed to bridge the critical gap between operational technology (OT) and information technology (IT), equipping participants with the skills to design, deploy, and manage secure and scalable industrial networks. Participants will gain a deep understanding of sensor technologies, communication protocols, edge computing, and data security, empowering them to lead Industry 4.0 initiatives within their organizations and turn the promise of smart manufacturing into a tangible reality.

Target Audience / This training course is suitable for:

- Automation Engineers.
- Control Systems Engineers.
- IT and OT Professionals.
- Network Architects and Administrators.
- Instrumentation and Control Technicians.
- Plant Managers and Operations Supervisors.
- Systems Integrators.
- Industrial Data Scientists.
- Product Development Engineers.
- Technical Project Managers.

Target Sectors and Industries:

- Manufacturing and Industrial Production.
- Energy, Utilities, and Power Generation.
- Oil and Gas Exploration and Refining.
- Transportation and Logistics.
- Automotive and Aerospace.
- Pharmaceuticals and Chemical Processing.
- Mining and Metals.
- Agriculture and Smart Farming.
- Government agencies and public sector infrastructure management.

Target Organizations Departments:

- Operations and Production.
- Engineering and Technical Services.
- Information Technology (IT).
- Maintenance and Reliability.
- Research and Development (R&D).
- Health, Safety, and Environment (HSE).
- Quality Assurance and Control.
- Supply Chain and Logistics.
- Capital Projects and Infrastructure.

Course Offerings:

By the end of this course, the participants will have able to:

- Design a robust IIoT network architecture tailored to specific industrial environments.
- Select and deploy the appropriate sensors and actuators for various industrial applications.
- Implement and troubleshoot key industrial communication protocols like Modbus, Profinet, and OPC UA.
- Configure wireless connectivity solutions including LoRaWAN, NB-IoT, and 5G for industrial use cases.
- Develop a comprehensive cybersecurity strategy to protect IIoT assets from threats.
- Integrate edge and fog computing principles to optimize data processing and response times.
- Manage the lifecycle of IIoT devices, from provisioning to decommissioning.
- Analyze sensor data to support predictive maintenance and operational efficiency initiatives.
- Evaluate the role of cloud platforms in IIoT data aggregation and analytics.
- Develop a strategic roadmap for implementing Industry 4.0 solutions.

Course Methodology:

The training methodology at BIG BEN Training Center is centered on creating a dynamic and immersive learning experience that bridges theory with practical application. This course employs a blended approach, combining expert-led instruction with interactive workshops, real-world case study analysis, and collaborative group projects. We believe that adult learning is most effective when participants are actively engaged in solving problems they face in their professional roles. Therefore, sessions are designed to be highly participatory, encouraging open discussion, knowledge sharing, and peer-to-peer learning. Participants will work through simulated scenarios of designing and securing an IIoT network for a model factory, allowing them to apply concepts in a risk-free environment. Our instructors facilitate these activities, providing personalized feedback and guiding participants to connect theoretical knowledge with tangible operational outcomes. The curriculum is structured to build skills progressively, ensuring a solid foundation before moving to more complex topics, culminating in a final project that integrates all the key competencies learned throughout the five days.

Course Agenda (Course Units):

Unit One: Foundations of Industrial IoT and Sensor Technologies

- Introduction to Industry 4.0 and the Industrial Internet of Things (IIoT).
- The IIoT Reference Architecture and Key Components.
- Understanding the OT vs. IT Convergence.
- Principles of Industrial Sensors and Transducers.
- Types of Sensors: Temperature, Pressure, Proximity, Vibration, and Vision.
- Sensor Calibration, Accuracy, and Data Acquisition Fundamentals.
- Introduction to Actuators and Control Systems in an IIoT Context.

Unit Two: Wired and Wireless Industrial Networking Protocols

- The OSI Model in an Industrial Context.
- Wired Communication Standards: Industrial Ethernet, Profinet, and EtherNet/IP.
- Legacy Fieldbus Protocols: Modbus, Profibus, and Foundation Fieldbus.
- Fundamentals of Wireless Communication for IIoT.
- Short-Range Wireless Technologies: Wi-Fi, Bluetooth, and Zigbee.
- Low-Power Wide-Area Networks (LPWAN): LoRaWAN and NB-IoT.
- Protocol Gateways and Data Translation in Heterogeneous Networks.

Unit Three: IIoT Messaging Protocols and Edge Computing

- Application Layer Protocols for IIoT: MQTT and CoAP.
- Understanding the Publish/Subscribe Model vs. Request/Response.
- Implementing MQTT Brokers and Clients for Industrial Data.
- The Role of Edge and Fog Computing in IIoT Architectures.
- Benefits of Processing Data at the Edge: Latency, Bandwidth, and Security.
- Designing and Deploying Edge Computing Solutions.
- Introduction to Time-Sensitive Networking (TSN) for Critical Control.

Unit Four: IIoT Data Integration and Cybersecurity

- Integrating IIoT with SCADA, MES, and ERP Systems.
- OPC UA (Unified Architecture) for Secure and Standardized Data Exchange.
- Connecting Industrial Assets to Cloud Platforms (e.g., AWS IoT, Azure IoT).
- The IIoT Cybersecurity Landscape: Threats and Vulnerabilities.
- Securing the IIoT Ecosystem: Device, Network, and Application Layers.
- Implementing Network Segmentation and Access Control Policies.
- Encryption, Authentication, and Secure Device Provisioning.

Unit Five: IIoT Applications, Analytics, and Future Trends

- Practical IIoT Use Cases: Predictive Maintenance and Asset Tracking.
- Condition Monitoring and Overall Equipment Effectiveness (OEE).
- Building Digital Twins for Industrial Processes.
- Fundamentals of Analyzing and Visualizing Sensor Data.
- The Role of Artificial Intelligence and Machine Learning in IIoT.
- Managing the IIoT Project Lifecycle: From Pilot to Full-Scale Deployment.
- The Future of Industrial Connectivity and the Smart Factory.

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

As IIoT systems become more integrated with critical infrastructure, how do we balance the drive for operational efficiency with the escalating risks of cybersecurity threats and data privacy concerns?

What unique qualities does this course offer compared to other courses?

This course distinguishes itself by offering a holistic, end-to-end perspective on industrial connectivity, meticulously bridging the often-siloed domains of Operational Technology (OT) and Information Technology (IT). Unlike programs that focus narrowly on a single protocol or technology, our curriculum provides a comprehensive understanding of the entire IIoT stack, from the physical sensor layer to cloud-based analytics. We emphasize a vendor-agnostic approach, teaching foundational principles and architectural patterns that can be applied across diverse industrial environments and equipment. A key differentiator is our profound focus on cybersecurity as an integral component of network design, not as an afterthought. Participants learn to build security into their IIoT systems from the ground up. Furthermore, the course content moves beyond mere theory by immersing participants in practical, problem-solving scenarios that mirror real-world industrial challenges. This focus on applied knowledge ensures that attendees leave not just with information, but with the strategic competence to design, deploy, and manage secure, scalable, and value-driven IIoT solutions that directly impact their organization's bottom line.

Course Introduction / Overview:

The Industrial Internet of Things (IIoT) is fundamentally reshaping the landscape of modern industry, creating interconnected ecosystems that drive unprecedented efficiency, safety, and innovation. This course provides a comprehensive exploration of the core components that power this transformation: robust networking and intelligent sensor connectivity. We will delve into the architectural principles and practical implementation of IIoT systems, moving from foundational concepts to advanced applications. As highlighted by industry thought leader Maciej Kranz in his influential book, "Building the Internet of Things," the true value lies not just in connecting devices, but in creating a seamless flow of actionable data. This program, offered by BIG BEN Training Center, is meticulously designed to bridge the critical gap between operational technology (OT) and information technology (IT), equipping participants with the skills to design, deploy, and manage secure and scalable industrial networks. Participants will gain a deep understanding of sensor technologies, communication protocols, edge computing, and data security, empowering them to lead Industry 4.0 initiatives within their organizations and turn the promise of smart manufacturing into a tangible reality.

Target Audience / This training course is suitable for:

- Automation Engineers.
- Control Systems Engineers.
- IT and OT Professionals.
- Network Architects and Administrators.
- Instrumentation and Control Technicians.
- Plant Managers and Operations Supervisors.
- Systems Integrators.
- Industrial Data Scientists.
- Product Development Engineers.
- Technical Project Managers.

Target Sectors and Industries:

- Manufacturing and Industrial Production.
- Energy, Utilities, and Power Generation.
- Oil and Gas Exploration and Refining.
- Transportation and Logistics.
- Automotive and Aerospace.
- Pharmaceuticals and Chemical Processing.
- Mining and Metals.
- Agriculture and Smart Farming.
- Government agencies and public sector infrastructure management.

Target Organizations Departments:

- Operations and Production.
- Engineering and Technical Services.
- Information Technology (IT).
- Maintenance and Reliability.
- Research and Development (R&D).
- Health, Safety, and Environment (HSE).
- Quality Assurance and Control.
- Supply Chain and Logistics.
- Capital Projects and Infrastructure.

Course Offerings:

By the end of this course, the participants will have able to:

- Design a robust IIoT network architecture tailored to specific industrial environments.
- Select and deploy the appropriate sensors and actuators for various industrial applications.
- Implement and troubleshoot key industrial communication protocols like Modbus, Profinet, and OPC UA.
- Configure wireless connectivity solutions including LoRaWAN, NB-IoT, and 5G for industrial use cases.
- Develop a comprehensive cybersecurity strategy to protect IIoT assets from threats.
- Integrate edge and fog computing principles to optimize data processing and response times.
- Manage the lifecycle of IIoT devices, from provisioning to decommissioning.
- Analyze sensor data to support predictive maintenance and operational efficiency initiatives.
- Evaluate the role of cloud platforms in IIoT data aggregation and analytics.
- Develop a strategic roadmap for implementing Industry 4.0 solutions.

Course Methodology:

The training methodology at BIG BEN Training Center is centered on creating a dynamic and immersive learning experience that bridges theory with practical application. This course employs a blended approach, combining expert-led instruction with interactive workshops, real-world case study analysis, and collaborative group projects. We believe that adult learning is most effective when participants are actively engaged in solving problems they face in their professional roles. Therefore, sessions are designed to be highly participatory, encouraging open discussion, knowledge sharing, and peer-to-peer learning. Participants will work through simulated scenarios of designing and securing an IIoT network for a model factory, allowing them to apply concepts in a risk-free environment. Our instructors facilitate these activities, providing personalized feedback and guiding participants to connect theoretical knowledge with tangible operational outcomes. The curriculum is structured to build skills progressively, ensuring a solid foundation before moving to more complex topics, culminating in a final project that integrates all the key competencies learned throughout the five days.

Course Agenda (Course Units):

Unit One: Foundations of Industrial IoT and Sensor Technologies

- Introduction to Industry 4.0 and the Industrial Internet of Things (IIoT).
- The IIoT Reference Architecture and Key Components.
- Understanding the OT vs. IT Convergence.
- Principles of Industrial Sensors and Transducers.
- Types of Sensors: Temperature, Pressure, Proximity, Vibration, and Vision.
- Sensor Calibration, Accuracy, and Data Acquisition Fundamentals.
- Introduction to Actuators and Control Systems in an IIoT Context.

Unit Two: Wired and Wireless Industrial Networking Protocols

- The OSI Model in an Industrial Context.
- Wired Communication Standards: Industrial Ethernet, Profinet, and EtherNet/IP.
- Legacy Fieldbus Protocols: Modbus, Profibus, and Foundation Fieldbus.
- Fundamentals of Wireless Communication for IIoT.
- Short-Range Wireless Technologies: Wi-Fi, Bluetooth, and Zigbee.
- Low-Power Wide-Area Networks (LPWAN): LoRaWAN and NB-IoT.
- Protocol Gateways and Data Translation in Heterogeneous Networks.

Unit Three: IIoT Messaging Protocols and Edge Computing

- Application Layer Protocols for IIoT: MQTT and CoAP.
- Understanding the Publish/Subscribe Model vs. Request/Response.
- Implementing MQTT Brokers and Clients for Industrial Data.
- The Role of Edge and Fog Computing in IIoT Architectures.
- Benefits of Processing Data at the Edge: Latency, Bandwidth, and Security.
- Designing and Deploying Edge Computing Solutions.
- Introduction to Time-Sensitive Networking (TSN) for Critical Control.

Unit Four: IIoT Data Integration and Cybersecurity

- Integrating IIoT with SCADA, MES, and ERP Systems.
- OPC UA (Unified Architecture) for Secure and Standardized Data Exchange.
- Connecting Industrial Assets to Cloud Platforms (e.g., AWS IoT, Azure IoT).
- The IIoT Cybersecurity Landscape: Threats and Vulnerabilities.
- Securing the IIoT Ecosystem: Device, Network, and Application Layers.
- Implementing Network Segmentation and Access Control Policies.
- Encryption, Authentication, and Secure Device Provisioning.

Unit Five: IIoT Applications, Analytics, and Future Trends

- Practical IIoT Use Cases: Predictive Maintenance and Asset Tracking.
- Condition Monitoring and Overall Equipment Effectiveness (OEE).
- Building Digital Twins for Industrial Processes.
- Fundamentals of Analyzing and Visualizing Sensor Data.
- The Role of Artificial Intelligence and Machine Learning in IIoT.
- Managing the IIoT Project Lifecycle: From Pilot to Full-Scale Deployment.
- The Future of Industrial Connectivity and the Smart Factory.

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

As IIoT systems become more integrated with critical infrastructure, how do we balance the drive for operational efficiency with the escalating risks of cybersecurity threats and data privacy concerns?

What unique qualities does this course offer compared to other courses?

This course distinguishes itself by offering a holistic, end-to-end perspective on industrial connectivity, meticulously bridging the often-siloed domains of Operational Technology (OT) and Information Technology (IT). Unlike programs that focus narrowly on a single protocol or technology, our curriculum provides a comprehensive understanding of the entire IIoT stack, from the physical sensor layer to cloud-based analytics. We emphasize a vendor-agnostic approach, teaching foundational principles and architectural patterns that can be applied across diverse industrial environments and equipment. A key differentiator is our profound focus on cybersecurity as an integral component of network design, not as an afterthought. Participants learn to build security into their IIoT systems from the ground up. Furthermore, the course content moves beyond mere theory by immersing participants in practical, problem-solving scenarios that mirror real-world industrial challenges. This focus on applied knowledge ensures that attendees leave not just with information, but with the strategic competence to design, deploy, and manage secure, scalable, and value-driven IIoT solutions that directly impact their organization's bottom line.