Advanced Security Integration for Smart Buildings Training Course



21 - 25 Dec 2026

Kuala Lumpur

5200 € (Per Person)

Ref: #SM3241_132693

Course Introduction / Overview:

This course provides a comprehensive exploration of integrating advanced security technologies within smart facilities and buildings. In an era where operational technology (OT) and information technology (IT) are converging, creating a seamless and resilient security posture is paramount. This program delves into the complex ecosystem of smart building technologies, from IoT sensors and building automation systems (BAS) to sophisticated video surveillance and access control. Participants will learn to navigate the unique challenges posed by cyber-physical systems, addressing both physical threats and digital vulnerabilities. Drawing on principles discussed by experts like Joseph A. Sinopoli in the field of intelligent buildings, the curriculum emphasizes a holistic approach to security design and management. We will explore concepts similar to those in texts like "The Design of Smart and Intelligent Environments," focusing on creating secure, efficient, and responsive infrastructures. BIG BEN Training Center has designed this course to equip professionals with the strategic foresight and technical knowledge to design, implement, and manage state-of-the-art integrated security solutions, transforming facilities into truly smart and secure environments. This training moves beyond theory to provide actionable strategies for mitigating risks and leveraging technology for proactive threat detection and response.

Target Audience / This training course is suitable for:

- Facilities Managers and Directors.
- Security Managers and Consultants.
- IT Directors and Network Administrators.
- Building Engineers and Automation Specialists.
- System Integrators and Security Solution Providers.
- Corporate Real Estate and Asset Managers.
- Risk and Compliance Officers.
- Project Managers overseeing building construction or retrofitting.

Target Sectors and Industries:

- Commercial and Corporate Real Estate.
- Healthcare and Hospital Facilities.
- Educational Campuses and Institutions.
- Government, Municipal, and Public Sector Buildings.
- Critical Infrastructure and Utilities.
- Hospitality and Entertainment Venues.
- Data Centers and Technology Hubs.
- Manufacturing and Industrial Plants.

Target Organizations Departments:

- Facilities Management and Operations.
- Corporate Security and Loss Prevention.
- Information Technology (IT) and Cybersecurity.
- Engineering and Maintenance.
- Risk Management and Compliance.
- Capital Projects and Construction.
- Physical Security Operations.
- Strategic Planning and Development.

Course Offerings:

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

- Design a holistic security strategy that integrates physical and cybersecurity measures for smart facilities.
- Evaluate and select appropriate security technologies, including access control, video surveillance, and intrusion detection systems.
- Understand the principles of system interoperability and integration platforms like PSIM.
- Identify and mitigate cybersecurity risks associated with Building Management Systems (BMS) and IoT devices.
- Develop robust incident response plans tailored to the unique environment of a smart building.
- Manage the convergence of IT and OT security protocols and teams effectively.
- Ensure security system designs comply with relevant industry standards and data privacy regulations.
- Analyze security data to identify trends, predict threats, and improve operational efficiency.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be immersive, practical, and highly interactive, ensuring participants can apply learned concepts directly to their professional roles. This course utilizes a blended approach that combines expert-led instruction with hands-on learning experiences. Mornings will feature detailed presentations on core concepts, frameworks, and emerging technologies in smart facility security. Afternoons are dedicated to practical application through collaborative workshops, where participants will work in teams to solve real-world security integration challenges. We will analyze detailed case studies of both successful security implementations and notable security breaches in smart buildings to extract valuable lessons. Group discussions and brainstorming sessions are integral, fostering a shared learning environment where professionals can exchange insights and experiences. The course culminates in a capstone project where teams design a comprehensive integrated security plan for a model smart facility, which they will present for peer and instructor feedback. This emphasis on active participation and practical problem-solving ensures a deep and lasting understanding of the material.

Course Agenda (Course Units):

Unit One: Foundations of Smart Facility Security

- Introduction to Smart Buildings and Facilities.
- The Convergence of Physical Security and Cybersecurity.
- Understanding the Smart Building Technology Ecosystem (IoT, BMS, IIoT).
- Key Security Principles for Cyber-Physical Systems.
- The Modern Threat Landscape for Smart Infrastructure.
- Regulatory and Compliance Frameworks Overview.
- Defining a Holistic Security Strategy.

Unit Two: Core Physical Security Technologies

- Advanced Access Control Systems (Biometrics, Mobile Credentials, Cloud-Based ACaaS).
- Modern Video Surveillance and Management Systems (VMS).
- The Role of AI and Video Analytics in Threat Detection.
- Intrusion Detection and Perimeter Protection Technologies.
- Integrating Fire and Life Safety Systems.
- Emergency Communication and Mass Notification Systems.
- Evaluating and Selecting Security Hardware and Software.

Unit Three: Integration Strategies and Platforms

- Principles of System Interoperability and Open Standards (e.g., ONVIF).
- Physical Security Information Management (PSIM) Platforms.
- Application Programming Interfaces (APIs) for Security Integration.
- Centralizing Operations in a Security Operations Center (SOC).
- Data Management and Storage Strategies for Security Systems.
- Integrating Legacy Systems with Modern Technology.
- Project Management for Security Integration Projects.

Unit Four: Cybersecurity for OT and Building Systems

- Fundamentals of Operational Technology (OT) Security.
- Securing Building Management Systems (BMS) and HVAC Controls.
- Network Segmentation and Architecture for Smart Buildings.
- Vulnerability Management for IoT and Connected Devices.
- Secure Remote Access Protocols and Policies.
- Developing a Patch Management Strategy for Embedded Systems.
- Incident Response for OT and Industrial Control Systems (ICS).

Unit Five: Advanced Security Management and Future Trends

- Conducting Comprehensive Risk and Threat Assessments.
- Developing and Testing an Integrated Incident Response Plan.
- Data Privacy Considerations in Surveillance and Monitoring.
- The Role of Artificial Intelligence and Machine Learning in Predictive Security.
- Utilizing Drones and Robotics for Facility Security.
- Building a Security-Aware Culture Among Facility Staff.
- The Future of Smart Building Security and Resilience.

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 smart facilities become more autonomous, where does the responsibility for a security breach lie—with the technology provider, the facility manager, or the end-user?

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

This course distinguishes itself by focusing intensely on the critical convergence of physical security and cybersecurity, a nexus often overlooked in traditional training programs. While other courses may treat these as separate disciplines, our curriculum is built on the principle that in a smart facility, they are inextricably linked. We provide a vendor-neutral perspective, teaching enduring principles of integration, risk assessment, and strategic design rather than focusing on specific product features that quickly become outdated. The curriculum is uniquely structured to address the security of Operational Technology (OT) and Building Management Systems (BMS), a highly specialized area that is a primary vulnerability in modern infrastructure. Participants engage in practical, scenario-based workshops that simulate real-world integration challenges, moving beyond theoretical knowledge to build tangible problem-solving skills. Furthermore, the course is forward-looking, dedicating significant time to emerging technologies like AI-driven predictive analytics and the ethical implications of advanced surveillance, preparing professionals not just for today's challenges but for the future of facility security.