Advanced Physical Security System Design and Integration Training Course



21 - 25 Dec 2026

Kuala Lumpur

5200 € (Per Person)

Ref: #SM2299_132207

Course Introduction / Overview:

This course provides a comprehensive exploration of the principles and practices required for designing and implementing effective physical security systems. In an era of evolving threats, a siloed approach to security is no longer viable. This program focuses on a holistic, integrated methodology, ensuring that disparate systems like access control, video surveillance, and intrusion detection work in concert to create a robust, layered security posture. We delve into the entire security system lifecycle, from initial threat vulnerability assessment and risk analysis to system design, procurement, project management, and final commissioning. Drawing on established frameworks and contemporary best practices, participants will learn to develop security master plans that are both resilient and adaptable. As highlighted by security expert Mary Lynn Garcia in her seminal work, "The Design and Evaluation of Physical Protection Systems", the effectiveness of any security program hinges on a systematic design process. BIG BEN Training Center has structured this course to equip professionals with the strategic thinking and technical knowledge needed to protect critical assets, manage complex security projects, and navigate the convergence of physical and cybersecurity. This is not just a technical course; it is a strategic masterclass in modern asset protection.

Target Audience / This training course is suitable for:

- Security Managers and Directors.
- Corporate Security Professionals.
- Facility Managers and Directors.
- IT Professionals involved in security system networking.
- Security System Designers and Engineers.
- Law Enforcement and Government Security Officials.
- Security Consultants and Integrators.
- Project Managers overseeing security installations.
- Risk Management and Compliance Officers.

Target Sectors and Industries:

- Banking and Financial Services.
- Critical Infrastructure and Utilities (Energy, Water, Transportation).
- Government, Defense, and Homeland Security Agencies.
- Healthcare and Pharmaceutical Facilities.
- Telecommunications and Data Centers.
- Commercial and Corporate Real Estate.
- Education and University Campuses.
- Retail and Logistics.
- Hospitality and Large-Scale Entertainment Venues.

Target Organizations Departments:

- Corporate Security and Asset Protection.
- Facilities Management and Operations.
- Information Technology and Network Security.
- Risk Management and Compliance.
- Project Management Office (PMO).
- Health, Safety, and Environment (HSE).
- Engineering and Maintenance.
- Legal and Corporate Governance.

Course Offerings:

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

- Conduct a comprehensive physical security risk and vulnerability assessment.
- Apply Crime Prevention Through Environmental Design (CPTED) principles.
- Design integrated access control, video surveillance, and intrusion detection systems.
- Develop detailed security system specifications and documentation for procurement.
- Manage the lifecycle of a security project from conception to commissioning.
- Evaluate and select appropriate security technologies for specific environments.
- Understand the fundamentals of physical and cybersecurity convergence.
- Create a strategic security master plan for an organization.
- Oversee the testing and commissioning process for new security systems.
- Develop effective security system maintenance and upgrade strategies.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be highly interactive, practical, and engaging, moving beyond theoretical lectures to foster real-world problem-solving skills. This course employs a blended learning approach that includes expert-led presentations, in-depth group discussions, and collaborative workshops. A significant portion of the training is dedicated to hands-on exercises, where participants will work with realistic case studies to conduct risk assessments, sketch out system designs, and develop project implementation plans. These practical sessions are designed to simulate the challenges faced by security professionals, allowing for the direct application of learned concepts in a controlled environment. We will analyze real-world security system failures and successes to draw valuable lessons. Participants will receive continuous feedback from the instructor and their peers, creating a dynamic learning environment that encourages critical thinking and the sharing of diverse experiences. The goal is to ensure that every participant leaves not just with knowledge, but with the confidence and competence to apply security design and integration best practices within their own organization.

Course Agenda (Course Units):

Unit One: Foundations of Physical Security and Risk Assessment

- Introduction to physical security principles and concepts.
- Understanding the layered security approach (deter, detect, delay, respond).
- Conducting comprehensive threat, vulnerability, and risk assessments (TVRA).
- Introduction to Crime Prevention Through Environmental Design (CPTED).
- Site surveys and information gathering techniques.
- Developing a security basis of design document.
- Legal and regulatory compliance in physical security.

Unit Two: Access Control and Intrusion Detection Systems

- Fundamentals of electronic access control systems (EACS).
- Exploring credential technologies from cards to biometrics.
- Designing door hardware and locking solutions.
- Intrusion Detection Systems (IDS) sensors and technologies.
- Perimeter intrusion detection systems (PIDS) design.
- Alarm monitoring and response protocols.
- Integrating access control with HR and IT systems.

Unit Three: Video Surveillance Systems and Analytics

- Core components of modern CCTV and video surveillance systems.
- Camera selection criteria, lens types, and placement strategies.
- Understanding video management systems (VMS) and network video recorders (NVR).
- Principles of lighting for effective surveillance.
- Introduction to video analytics and artificial intelligence (AI) in surveillance.
- Storage, retention, and bandwidth calculations for video systems.
- Privacy considerations and ethical use of video surveillance.

Unit Four: Physical Security System Integration and Project Management

- The concept of Physical Security Information Management (PSIM).
- Integrating access control, video, and intrusion detection systems.
- The convergence of physical security and cybersecurity.
- Securing the network for physical security devices.
- Developing security system specifications and scope of work.
- The security procurement process and vendor selection.
- Managing security installation projects from start to finish.

Unit Five: System Commissioning, Maintenance, and Future Trends

- The factory and site acceptance testing (FAT/SAT) process.
- Commissioning and final handover of security systems.
- Developing system documentation and as-built drawings.
- Creating a proactive security system maintenance plan.
- Troubleshooting common security system issues.
- The impact of IoT, cloud computing, and drones on physical security.
- Developing a long-term security technology roadmap.

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 physical and cybersecurity continue to converge, how should organizations adapt their security design philosophies to address threats that exploit the intersection of both domains?

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

This course distinguishes itself by moving beyond a product-focused or single-system approach to embrace a holistic and strategic methodology for physical security. While many courses concentrate on the technical specifications of individual components, our curriculum emphasizes the art and science of integration, ensuring participants understand how to make disparate systems function as a single, cohesive security ecosystem. We focus on the entire security lifecycle, from the foundational philosophy of risk assessment and security master planning to the practical realities of project management, commissioning, and long-term maintenance. The program is built on a foundation of vendor-neutral principles, empowering participants to design and specify systems based on operational requirements rather than brand loyalty. Furthermore, a significant focus is placed on the critical convergence of physical and cybersecurity, a topic often overlooked but essential in today's threat landscape. By blending established security doctrines with forward-looking concepts like IoT security and AI-driven analytics, this course provides a uniquely comprehensive and strategic perspective, preparing professionals not just for today's challenges, but for the future of asset protection.