COURSE OVERVIEW DM0122
Advanced Physical Security Management & Related Systems

Course Title
Advanced Physical Security Management & Related Systems

Course Date/Venue
Session 1: August 10-14, 2025/Tamra Meeting Room, Al Bandar Rotana Creek, Dubai, UAE
Session 2: September 21-25, 2025/Tamra Meeting Room, Al Bandar Rotana Creek, Dubai, UAE

Course Reference
DM0122

Course Duration/Credits
Five days/3.0 CEUs/30 PDHs

Course Description

This practical and highly-interactive course includes real-life case studies and exercises where participants will be engaged in a series of interactive small groups and class workshops.

This course is designed to provide participants with a detailed and up-to-date overview of Advanced Physical Security Management & Related Systems. It covers the principles of physical security in high-risk industries and security risk assessment process; the threat-vulnerability-consequence analysis and role of physical security in enterprise risk management; the security architecture design and planning, critical infrastructure protection (CIP) and latest physical security technologies; and the physical security policies and procedures and security risk assessment tools.

Further, the course will also discuss the perimeter intrusion detection systems (PIDS), advanced CCTV and video analytics; the access control system design and management and integration of physical security information management (PSIM); the command and control room operations and security incident detection; the response technologies, intrusion detection and anti-sabotage measures; and the visitor and contractor security management, vehicle access management and anti-vehicle measures.

During this interactive course, participants will learn the security response planning and drills, insider threat detection and mitigation; the crisis management and business continuity planning; the smart security infrastructure for oil and gas, cyber-physical security convergence and drones, robots and autonomous surveillance; the digital twins and augmented reality in security, security system integration projects and security technology lifecycle management; the security audits and compliance, security incident investigation and reporting and emergency communication systems; and the workforce and contractor security awareness, KPIs and performance metrics in security and the future trends in physical security.

Course Objectives

Upon the successful completion of this course, each participant will be able to:-

- Apply and gain an advanced knowledge on physical security management and related systems
- Discuss the principles of physical security in high-risk industries including the security risk assessment process, threat-vulnerability-consequence analysis and role of physical security in enterprise risk management
- Illustrate security architecture design and planning, critical infrastructure protection (CIP) and latest physical security technologies
- Carryout physical security policies and procedures and security risk assessment tools
- Recognize perimeter intrusion detection systems (PIDS), advanced CCTV and video analytics
- Apply access control system design and management and integrate physical security information management (PSIM)
- Employ command and control room operations, security incident detection, response technologies, intrusion detection and anti-sabotage measures
- Carryout visitor and contractor security management, vehicle access management and anti-vehicle measures
- Conduct security response planning and drills, insider threat detection and mitigation, crisis management and business continuity planning
- Discuss smart security infrastructure for oil and gas, cyber-physical security convergence and drones, robots and autonomous surveillance
- Explain digital twins and augmented reality in security, security system integration projects and security technology lifecycle management
- Apply security audits and compliance, security incident investigation and reporting and emergency communication systems
- Carryout workforce and contractor security awareness, KPIs and performance metrics in security as well as discuss the future trends in physical security

Exclusive Smart Training Kit - H-STK®

*Participants of this course will receive the exclusive "Haward Smart Training Kit" (**H-STK®**). The **H-STK®** consists of a comprehensive set of technical content which includes **electronic version** of the course materials conveniently saved in a **Tablet PC**.*

Who Should Attend

This course provides an overview of all significant aspects and considerations of advanced physical security management and related systems for security managers and supervisors, it and security systems professionals, risk and compliance officers, project managers in security installations, security consultants and auditors and emergency response and crisis management teams.

Course Certificate(s)

Internationally recognized certificates will be issued to all participants of the course who completed a minimum of 80% of the total tuition hours.

Certificate Accreditations

Haward's certificates are accredited by the following international accreditation organizations: -

- British Accreditation Council (BAC)

  Haward Technology is accredited by the **British Accreditation Council** for **Independent Further and Higher Education** as an **International Centre**. Haward's certificates are internationally recognized and accredited by the British Accreditation Council (BAC). BAC is the British accrediting body responsible for setting standards within independent further and higher education sector in the UK and overseas. As a BAC-accredited international centre, Haward Technology meets all of the international higher education criteria and standards set by BAC.

- The International Accreditors for Continuing Education and Training (IACET - USA)

  Haward Technology is an Authorized Training Provider by the International Accreditors for Continuing Education and Training (IACET), 2201 Cooperative Way, Suite 600, Herndon, VA 20171, USA. In obtaining this authority, Haward Technology has demonstrated that it complies with the **ANSI/IACET 2018-1 Standard** which is widely recognized as the standard of good practice internationally. As a result of our Authorized Provider membership status, Haward Technology is authorized to offer IACET CEUs for its programs that qualify under the **ANSI/IACET 2018-1 Standard**.

  Haward Technology's courses meet the professional certification and continuing education requirements for participants seeking **Continuing Education Units** (CEUs) in accordance with the rules & regulations of the International Accreditors for Continuing Education & Training (IACET). IACET is an international authority that evaluates programs according to strict, research-based criteria and guidelines. The CEU is an internationally accepted uniform unit of measurement in qualified courses of continuing education.

  Haward Technology Middle East will award **3.0 CEUs** (Continuing Education Units) or **30 PDHs** (Professional Development Hours) for participants who completed the total tuition hours of this program. One CEU is equivalent to ten Professional Development Hours (PDHs) or ten contact hours of the participation in and completion of Haward Technology programs. A permanent record of a participant's involvement and awarding of CEU will be maintained by Haward Technology. Haward Technology will provide a copy of the participant's CEU and PDH Transcript of Records upon request.

Course Instructor(s)

This course will be conducted by the following instructor(s). However, we have the right to change the course instructor(s) prior to the course date and inform participants accordingly:

General Ahmed Mady is a **Senior Security Consultant** and an **Expert** in **Intelligence**, **Strategic Planning**, **Terrorism**, **Security Management**, **Security Risk Assessment**, **Operating Access Control System**, **Security Operations Management** and **HSE Management** with over **30 years** of practical experience. He has consistently exemplified great skills in **Strategic Security** Management, **Security Risk** Management, **Security Threat** Identification, **Risk Analysis Evaluation** & Management, **Security Systems**, **Security Inteligence**, **Security Operations** Management, **Investigssation & Security Surveying**, **Security Crisis** Management, **Corporate Security Planning**, **Strategic Analysis**, Strategy Selection & Implementation, **Security Policies & Procedures**, **Logistics Management**, **Systems Analysis & Design**, **Organization Procedure Evaluation & Auditing**, **Contracting & Systems Construction** and Maximo Managing Work & Foundation. Curently, he is the **Chief Information Directorate** of the **Ministry of Civil Aviation**.

During his service, he had been tasked as the **Chief Engineering Analyst**, **On-Scene Commander** (**OSC**) **& Incident Commander** (**IC**) in the **Air Force** and was responsible for a team of engineers supporting all engineering studies, modifications, aging studies and maintenance analysis. Being a **Board Member** of the **Aviation Information Technology Center**, he holds control of the overall strategies and procedures for the ministry, contracting for major IT projects, supervising all IS activities in the aviation sector and ensuring quality and success of delivery. He had likewise served as the **Commander** of the **Air Force** and had worked closely with the **Logistics Computer Center** wherein he gave out direction on **Operational & Tactical Logistics Planning** and **Strategic Military Logistics** to numerous high ranking officials, and at the same time **commanding flying Air Force maintenance squadron logistics field activities**. General Ahmed retired in the service as a **Major General**.

Earlier in his career, General Ahmed had occupied several challenging roles with several large Logistics companies as their **General Manager**, **Maintenance Engineer**, **Systems Analyst**, **Training Branch Chief**, **Systems & Communication Engineer**, **Computer Programmer** and **Logistic Instructor**. Further, he has travelled all over Europe, Asia and the Americas joining numerous conferences and workshops with the **Ministry of Foreign Affairs** and international companies such as **IBM**, **System Science Corporation** (**SSC**) and **International Air Transport Association** (**IATA**).

General Ahmed has a **Bachelor** degree in **Mechanical Engineering**. Further, he has gained **Diplomas** on **Civil Aviation Engineering**, **Islamic Studies** and **Information Systems & Technology**. Moreover, he is a **Certified Assessor** by **City & Guilds Level 4 Certificate** in **Leading the Internal Quality Assurance of Assessment Processes & Practice** and **Level 3 Certificate in Assessing Vocational Achievement** under the **TAQA Qualification** (**Training**, **Assessment & Quality Assurance**), a **Certified Internal Verifier Level 2 & 3 NVQ Processing Operations: Hydrocarbons** by **the British City & Guilds**, a **Certified Internal Verifier/Trainer/Assessor by the British Institute of Leadership & Management** (**ILM**) and a **Certified Instructor/Trainer.**

Training Methodology

All our Courses are including **Hands-on Practical Sessions** using equipment, State-of-the-Art Simulators, Drawings, Case Studies, Videos and Exercises. The courses include the following training methodologies as a percentage of the total tuition hours:-

30% Lectures
20% Practical Workshops & Work Presentations
30% Hands-on Practical Exercises & Case Studies
20% Simulators (Hardware & Software) & Videos

In an unlikely event, the course instructor may modify the above training methodology before or during the course for technical reasons.

Course Fee

US$ 5,500 per Delegate + **VAT**. This rate includes H-STK® (Haward Smart Training Kit), buffet lunch, coffee/tea on arrival, morning & afternoon of each day.

Accommodation

Accommodation is not included in the course fees. However, any accommodation required can be arranged at the time of booking.

Course Program

The following program is planned for this course. However, the course instructor(s) may modify this program before or during the workshop for technical reasons with no prior notice to participants. Nevertheless, the course objectives will always be met:

Day 1

0730 – 0800	*Registration & Coffee*
0800 – 0815	*Welcome & Introduction*
0815 – 0830	***PRE-TEST***
0830 – 0930	***Introduction to Physical Security Risk Management*** *Principles of Physical Security in High-Risk Industries • Security Risk Assessment Process • Threat-Vulnerability-Consequence Analysis • Role of Physical Security in Enterprise Risk Management*
0930 – 0945	*Break*
0945 – 1030	***Security Architecture Design & Planning*** *Layered Defense (Concentric Rings of Protection) • Zones of Control and Access • Integration of People, Procedures, and Technologies • Design Considerations for Oil & Gas Facilities*
1030 – 1130	***Critical Infrastructure Protection (CIP)*** *Identifying Critical Assets and Vulnerabilities • Regulatory Frameworks and Global Standards (e.g., NIST, DHS, ISA/IEC 62443) • Protective Strategies for Pipelines, Refineries, and Terminals • Risk Scenarios: Sabotage, Insider Threat, Terrorism*
1130 – 1215	***Latest Physical Security Technologies Overview*** *AI-Based Video Analytics and Surveillance • Biometric Access Control Systems • Intrusion Detection and Perimeter Security Systems • Smart Barriers and Anti-Ram Vehicle Protection*

1215 – 1230	*Break*
1230 – 1330	***Physical Security Policies & Procedures*** *Creating and Maintaining Security SOPs • Site-Specific and Asset-Specific Security Postures • Integration with Cybersecurity and Operational Procedures • Physical Security Incident Reporting Protocols*
1330 – 1420	***Security Risk Assessment Tools*** *Security Threat and Risk Assessment (STRA) Methodology • Security Gap Analysis Tools • Risk Mitigation Matrix and Prioritization • Use of GIS-Based Risk Mapping Tools*
1420 – 1430	***Recap*** *Using this Course Overview, the Instructor(s) will Brief Participants about the Topics that were Discussed Today and Advise Them of the Topics to be Discussed Tomorrow*
1430	*Lunch & End of Day One*

Day 2

0730 – 0830	***Perimeter Intrusion Detection Systems (PIDS)*** *Sensor Technologies: Microwave, Fiber Optics, IR Beams • Fence Detection and Vibration Systems • Real-Time Alarm Response Integration • Performance Evaluation and False Alarm Reduction*
0830 – 0930	***Advanced CCTV & Video Analytics*** *AI-Driven Behavior Analytics (e.g., Loitering, Object Detection) • License Plate Recognition (LPR) Systems • Drone-Based Video Surveillance • Central Monitoring and Analytics Dashboards*
0930 – 0945	*Break*
0945 – 1100	***Access Control System Design & Management*** *Card-Based and Biometric Access Systems • Multi-Factor Authentication (MFA) in Secured Zones • Visitor Management Integration • Access Rights Hierarchy and Audit Trails*
1100 – 1215	***Integration of Physical Security Information Management (PSIM)*** *Overview of PSIM Platforms • Integrating Multiple Subsystems: CCTV, Alarms, Fire, Access Control • Incident Handling and Dispatch Coordination • Real-Time Data Fusion and Decision Support*
1215 – 1230	*Break*
1230 – 1330	***Command & Control Room Operations*** *Roles and Layout of Modern Security Control Centers • SCADA, BMS, and PSIM Coordination • Monitoring Protocols and Escalation Paths • Training Operators on Decision-Making During Critical Events*
1330 – 1420	***Security Incident Detection & Response Technologies*** *AI-Based Anomaly Detection • Sensor Fusion for Early Warning • Automated Lockdown Protocols • Mobile Response Systems for Field Officers*
1420 – 1430	***Recap*** *Using this Course Overview, the Instructor(s) will Brief Participants about the Topics that were Discussed Today and Advise Them of the Topics to be Discussed Tomorrow*
1430	*Lunch & End of Day Two*

Day 3

0730 – 0830	***Intrusion Detection & Anti-Sabotage Measures*** *Asset Hardening Techniques • Dual-Redundant Surveillance for Critical Zones • Environmental Sensors (Gas Leaks, Vibrations) • Case Study: Sabotage Attempt Mitigation in a Refinery*
0830 – 0930	***Visitor and Contractor Security Management*** *Contractor Vetting and Onboarding • Smart Badge Systems with Geofencing • Escort Policies and Surveillance • Integrating Visitor Logs with PSIM*
0930 – 0945	*Break*
0945 – 1100	***Vehicle Access Management & Anti-Vehicle Measures*** *RFID Vehicle Access Control • Under Vehicle Surveillance System (UVSS) • Anti-Ram and Crash-Rated Barriers • Automatic Number Plate Recognition (ANPR) Systems*
1100 – 1215	***Security Response Planning & Drills*** *Security Drill Design and Execution • Table-Top vs Full-Scale Simulations • Post-Drill Debriefing and Action Plans • Metrics for Measuring Drill Success*
1215 – 1230	*Break*
1230 – 1330	***Insider Threat Detection & Mitigation*** *Early Warning Indicators and Red Flag Behaviors • Data and Access Monitoring for Suspicious Activity • Behavioral Analytics and Profiling Tools • Collaborating with HR and IT Security Teams*
1330 – 1420	***Crisis Management & Business Continuity Planning*** *Crisis Response Frameworks • Coordination with Emergency Responders • Maintaining Security During Shutdowns/Evacuations • Recovery and Continuity Plans for Secured Assets*
1420 – 1430	***Recap*** *Using this Course Overview, the Instructor(s) will Brief Participants about the Topics that were Discussed Today and Advise Them of the Topics to be Discussed Tomorrow*
1430	*Lunch & End of Day Three*

Day 4

0730 – 0830	***Smart Security Infrastructure for Oil & Gas*** *Converged IT/OT Security Environments • IIoT Devices for Field-Level Security • Role of SCADA in Physical Security Alerts • AI-Enabled Security Dashboards*
0830 – 0930	***Cyber-Physical Security Convergence*** *Understanding Physical-Cyber Interface Risks • Tampering of Surveillance and Access Systems • Bridging Cybersecurity Policies with Physical Controls • SOC-NOC-PSIM Integration Strategies*
0930 – 0945	*Break*
0945 – 1100	***Drones, Robots & Autonomous Surveillance*** *UAV Patrols for Remote Pipelines • AI-Based Robotic Surveillance • Integration with Real-Time Alert Systems • Regulatory and Privacy Considerations*
1100 – 1215	***Digital Twins & Augmented Reality in Security*** *Creating Digital Models of Facilities • Using AR/VR for Training and Simulations • Virtual Patrol Planning and Zone Modeling • Predictive Threat Simulation*

1215 – 1230	*Break*
1230 – 1330	***Security System Integration Projects*** *Scoping and Planning Integration Projects • Selecting Open Architecture Systems • Vendor Management and Commissioning • Acceptance Testing and System Handover*
1330 – 1420	***Security Technology Lifecycle Management*** *Planning for Obsolescence and Upgrades • System Maintenance and Patch Management • Audit and Compliance of Physical Security Tech • ROI Analysis of Security Investments*
1420 – 1430	***Recap*** *Using this Course Overview, the Instructor(s) will Brief Participants about the Topics that were Discussed Today and Advise Them of the Topics to be Discussed Tomorrow*
1430	*Lunch & End of Day Four*

Day 5

0730 – 0830	***Security Audits & Compliance*** *Types of Physical Security Audits • Oil & Gas Security Compliance Frameworks • Checklists and Audit Trail Documentation • Remediation Action Planning*
0830 – 0930	***Security Incident Investigation & Reporting*** *Evidence Collection and Chain of Custody • CCTV and Access Log Analysis • Interviewing and Documenting Witness Statements • Writing Security Investigation Reports*
0930 – 0945	*Break*
0945 – 1100	***Emergency Communication Systems*** *Mass Notification Systems (MNS) • Intercom and PA System Integration • Mobile Alerts and Geo-Fenced Messaging • Integration with Emergency Response Teams*
1100 – 1230	***Workforce & Contractor Security Awareness*** *Induction and Awareness Programs • Building a Security-Conscious Culture • Role-Based Security Responsibilities • Using E-Learning and Simulation Tools*
1230 – 1245	*Break*
1245 – 1300	***KPIs & Performance Metrics in Security*** *Defining Security KPIs and Metrics • Incident Response Time Benchmarks • Threat Resolution Rate Tracking • Monthly and Quarterly Security Reporting*
1300 - 1245	***Future Trends in Physical Security*** *Predictive Security Using AI and Machine Learning • Blockchain for Access Control and Identity • Integration with ESG and Sustainability Goals • Emerging Threats and Countermeasure Strategies*
1345 – 1400	***Course Conclusion*** *Using this Course Overview, the Instructor(s) will Brief Participants about the Course Topics that were Covered During the Course*
1400 – 1415	***POST-TEST***
1415 – 1430	*Presentation of Course Certificates*
1430	*Lunch & End of Course*

Practical Sessions

This practical and highly-interactive course includes real-life case studies and exercises:-

Course Coordinator

Mari Nakintu, Tel: +971 2 30 91 714, Email: mari1@haward.org