資歷架構
Qualifications Framework

Security Services Industry

SCS-based training package

Basic Premises Security Systems Design course (Level 2)

Feb 2021

FOREWORD

“Training Packages are SCS-based, with learning and assessment materials derived from the selected UoC(s) which correspond with the job role and function. The performance requirements in the UoC(s) are applied in the learning outcome of the Training Package, and the learning and assessment materials correspond with the learning outcome. The contents are developed for the specific learner profile, mode of learning and assessment method, which can be used as reference in module designs.

This Training Package outlines the essential elements for a module, using UoC 107693L2 “Conduct basic design and recommendation of a security system for a client’s site” which correspond with designated job role and function “Basic Security System Design” in the Security Services industry and offering for reference the contents of learning, assessment guidelines, as well as supporting and reference materials. It exemplifies the design of module structure, and comes with suggestions on teaching, learning and assessment materials. Assessment materials include sample tasks or activities, methods and contexts of assessment, outcome standards and performance rubric that are appropriate to the contents of learning.

This Training Package is not meant to be a complete learning programme by itself. Enterprises and education and training providers who wish to use it as a blueprint for module development should adjust the relevant teaching, learning and assessment contents for any variations in learning objectives, target learners, entry requirements such as academic level and experience, etc. In addition, users are advised to check and adopt the latest update of the references to ensure their currency, validity and accuracy when using it. For any learning programme developed by drawing reference to this Training Package to become QF-recognised, it must successfully pass the quality-assurance process of the Hong Kong Council for Accreditation of Academic and Vocational Qualifications or the self-accrediting institutions.”

List of Content

Overview

Introduction

This Training Package is based on UoC 107693L2 and is intended as the teaching plan for the “Basic Premises Security Systems Design Course” for those engaged in designing basic premises security systems or interested in providing such services. Please refer to Appendix 1 and Appendix 2 for details of UoC 107693L2 and mapping of the course outline against the functional areas.

The “Basic Premises Security Systems Design Course” aims at teaching basic practical knowledge and skills for the design of premises security systems. Learners will learn about how to design standards compliant and effective basic security systems (including: intrusion detection alarm systems, video recording or CCTV recording systems and access control systems) for small and medium-sized or non-high-risk premises (including: residential units, retail shops, and offices, etc.).

This Training Package is compiled with the intent to guide training institutions on how to systematically develop the teaching plan for the “Basic Premises Security Systems Design Course”. After reading through this Training Package, training institutions should get a good understanding of the teaching and learning requirements, conditions, and contents of UoC 107693L2, thereby reducing the cost of course development and ensuring the course quality.

Syllabus and Instructions for Use

The “Basic Premises Security Systems Design Course” is consisted of 10 topics, which correspond to the knowledge and skills covered in UoC 107693L2. The course outline includes:

1. Relevant laws and license requirements
2. Principles of physical security, functions of security systems and security standards
3. Understanding the client’s security needs
4. Conducting security risk assessment for the client’s site
5. The basic configuration and application of an intrusion detection alarm system
6. The basic configuration and application of a video recording or CCTV surveillance system
7. The basic configuration and application of an access control system
8. Designing basic premises security systems
9. Knowledge and skills associated with designing basic premises security systems
10. Practical exercises about designing basic premises security systems

This Training Package is divided into three sections:

The first section provides general instructions covering topics such as:

- Aims
- Syllabus
- Teaching Objectives
- Intended Learning Outcomes
- Trainees
- Qualification of Trainers
- Teaching Mode
- Assessment Mode
- Course Development and Management
- Appendices:
  - Appendix 1：UoC 107693L2
  - Appendix 2：Mapping of Course Outline against Functional Areas

The second section outlines the teaching and assessment guidelines for each of the 10 topics of the “Basic Premises Security Systems Design Course”, including:

- Teaching Guidelines
  - Intended Learning Outcomes
  - Contact Hours
  - Self-study Guidelines for Learners
  - Suggested Scope, Contents and Materials
- Assessment Guidelines
  - Assessment Mode
  - Scope of Assessment
  - Marking Rubrics
- List of Training Aids
- References

The third section covers “Self-study Guidelines for Learners” which is a consolidation of the scope of knowledge and skills that the learners must review before certain lessons.

Appendix 1: UoC 107693L2

Specification of Competency Standards for the Security Services Industry
Unit of Competency

Functional Area - "Physical Security & Technological Support"

Title	Conduct basic design and recommendation of a security system for a client's site
Code	107693L2
Range	This unit of competency applies to security personnel responsible for the design and recommendation of security systems and devices of a company holding a Type III security company license for providing relevant security work in Hong Kong. It covers the abilities to provide an initial design and recommendation for an appropriate security system, including relevant devices for a client's site.
Level	2
Credit	3
Competency	Performance Requirements 1. Knowledge about basic design and recommendation of a security system • Understand the client's physical security requirements • Understand the overall objectives of physical security • Understand laws and regulations relevant to security services, which should include but not limited to: ➢ Security and Guarding Services Ordinance, Cap 460 ➢ Occupational Safety & Health Ordinance, Cap 509 and related regulations ➢ Personal Data (Privacy) Ordinance, Cap 486 • Understand duty of care and third-party responsibilities with regard to maintaining safety and security of the premises under protection • Understand the physical environment and safety and security measures in place • Possess the basic skills and techniques for conducting site security reviews and surveys • Possess knowledge in the deployment of security systems to achieve the desired level of physical security • Possess good inter-personal skills for promoting ideas and recommendations 2. Conduct basic design and recommendation of a security system for a

	client's site
	
	Be able to:
	
	• Perform an initial security risk assessment to identify security threats and risks for the client
	• Determine the desired level of physical security based on:
	  ➢ Client's requirements
	  ➢ Client's physical security policy
	  ➢ Findings of security risk assessment after checking the site of the client, etc.
	• Work out an initial security system, with details such as:
	  ➢ The potential security risks identified
	  ➢ The size of the security system required
	  ➢ Whether the system will be monitored on site or off site
	  ➢ Whether the system will be compatible with other security measures on site
	• Suggested spots / locations for:
	  ➢ Installation of security devices such as alarm, CCTV and lighting system, etc.
	  ➢ Laying of wire and cable, etc.
	• Document the findings and recommendations into an initial proposal for the client
	• Discuss with and make recommendations to the client regarding the proposed security system
	• Seek approval from the client, management and other stakeholders about the recommended security system

Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Conduct basic design and recommendation of a security system for the client's site according to requirements and findings of security risk assessment; and • Make appropriate recommendations regarding the security system and relevant devices to be installed at the client's site
Remark	Unit of Competency (UoC) 107693L2 is developed through the joint efforts of relevant stakeholders including SGSIA and the trade. Graduates from programmes UoC107693L2 accredited by the Hong Kong Council for Accreditation of Academic and Vocational Qualifications (HKCAAVQ) will be considered as having received training relevant to basic security system design work when applying for Category D security personnel permit.

Appendix 2: Mapping of Course Outline against Functional Areas

Mapping of Course Outline against Functional Areas

Topic: #	Topic:
Getting Started	
1	Relevant laws and license requirements
2	Principles of physical security, international standards and the functions of security systems
Client Management and Risk Assessment	
3	Understanding the client's security needs
4	Conducting security risk assessment for the client's site
System Design and Recommendations	
5	The basic configuration and application of an intrusion detection alarm system
6	The basic configuration and application of a video recording or CCTV surveillance system
7	The basic configuration and application of an access control system
8	Designing security systems for the client's site
9	Knowledge and skills related to designing security systems
10	Practical exercises about designing security systems

Performance Requirements of UoC 107693L2	Topic: #
Knowledge about basic design and recommendation of a security system:	
• Understand the client's physical security needs	3
• Understand the overall objectives of physical security	2
• Understand laws and regulations relevant to security services, which should include but not limited to: ➢ Security and Guarding Services Ordinance, Cap 460 ➢ Occupational Safety and Health Ordinance, Cap 509 and related regulations ➢ Personal Data (Privacy) Ordinance, Cap 486	1
• Understand duty of care and third-party responsibilities with regard to maintaining safety and security of the premises under protection	1

• Understand the physical environment and safety and security measures in place	4
• Possess the basic skills and techniques for conducting site security reviews and surveys	4
• Possess knowledge in the deployment of security systems to achieve the desired level of physical security	2-10
• Possess good inter-personal skills for promoting ideas and recommendations	3，4，8，9
Conduct basic design and recommendation of a security system for a client's site, be able to:	
• Perform an initial security risk assessment to identify security threats and risks for the client	3，4
• Determine the desired level of physical security based on: ➢ Client's requirements ➢ Client's physical security policy ➢ Findings of security risk assessment after checking the site of the client, etc.	2，3，4
• Work out an initial security system, with details such as: ➢ The potential security risks identified ➢ The size of the security system required ➢ Whether the system will be monitored on site or off site ➢ Whether the system will be compatible with other security measures on site ➢ Suggested spots / locations for: ▪ Installation of security devices such as alarm, CCTV and lighting system, etc. ▪ Laying of wire and cable, etc.	2-10
• Document the findings and recommendations into an initial proposal for the client	9
• Discuss with and make recommendations to the client regarding the proposed security system	9
• Seek the approval of the client, management and other stakeholders about the recommended security system	9
Assessment Criteria	
• Conduct basic design and recommendation of a security system for the client's site according to requirements and findings of security risk assessment; and	
• Make appropriate recommendations regarding the security system and relevant devices to be installed at the client's site	

Section 1: General Instruction

Aims

This Training Package of “Basic Premises Security Systems Design Course” is based on UoC 107693L2 and aims at teaching practical knowledge and skills relating to the design of basic premises security systems in a systematic manner. Upon completion of the course, it is expected that learners will be able to design standards compliant and effective basic security systems and associated devices for small and medium-sized or non-high-risk premises as well as clearly record relevant details in diagrams and texts as instructions for installation.

We therefore recommend that training institutions should adopt this Training Package as their teaching plan for the "Basic Premises Security Systems Design Course", to ensure that learners can learn about the practical knowledge and skills required in a systematic manner and can effectively apply them to the design of basic premises security systems.

Syllabus

This “Basic Premises Security Systems Design Course” is consisted of the following 10 topics:

1. Relevant laws and license requirements
2. Principles of physical security, functions of security systems and security standards
3. Understanding the client’s security needs
4. Conducting security risk assessment for the client’s site
5. The basic configuration and application of an intrusion detection alarm system
6. The basic configuration and application of a video recording or CCTV surveillance system
7. The basic configuration and application of an access control system
8. Designing basic premises security systems
9. Knowledge and skills associated with designing basic premises security systems
10. Practical exercises about designing basic premises security systems

Teaching Objectives

This Training Package is intended for those who are engaged in designing basic premises security systems or interested in providing such services. It teaches them the practical knowledge and skills required for designing standards compliant and effective basic premises security systems for small to medium-sized or non-high-risk premises based on the client’s needs, the site environment and security risks as well as recording such design in diagrams and texts as installation instructions.

Regarding the course structure, learners will firstly be introduced to relevant laws and regulations, principles of physical security, security standards and the functions of security systems in physical security. Thereafter, learners will learn about how to understand the client’s needs and conduct risk assessment, and then the basic configuration and application of various security systems as well as other necessary practical knowledge and skills. Lastly learners will be guided to applying what they have learnt to designing basic security systems for premises of different nature and receive immediate feedback from the Trainer.

Intended Learning Outcomes

Upon completion of the “Basic Premises Security Systems Design Course”, learners should be able to:

- Design standards compliant and effective basic premises security systems based on the client’s needs, site environment and security risks; and
- Clearly record design details of the basic premises security systems in diagrams and texts as installation instructions.

Learners

It is suggested that the target learners should meet the following conditions:

- Are at the age of 18 or above; and
- Are interested in security work in relation to designing basic premises security systems

Qualification of Trainers

It is suggested that the trainers should, as a minimum, possess qualifications as follows:

- Possess qualifications related to “Physical Security and Technological Support” at Qualifications Framework Level 4 (inclusive of “Recognition of Prior Learning”); and
- Possess 6 years or above practical work experience in designing premises security systems; and
- Possess 3 years or above training experience; and
- Being able to read and write in the language to be used as the medium of instruction

Teaching Mode

The teaching mode of “Basic Premises Security Systems Design Course” is mainly consisted of lectures, discussions, and practical exercises. It is hoped that learners will acquire the

necessary knowledge and skills through these activities and gain deep understanding about how to apply them to their daily work.

The recommended ratio of in-person class to self-study hours and the ratio of trainer to trainee for in-person class are listed below:

Teaching Mode:	In-person class
Total Credit Hours:	30 hours
In-person class to Self-study Ratio:	9：1
Contact Hours (minimum):	27 hours
Trainee Self-study Hours:	3 hours
Trainer-to-Trainee Ratio (maximum):	1：30

The recommended number of contact hours for each topic is listed below:

Topics		**Recommended Contact Hours**
1.	Relevant laws and license requirements	1
2.	Principles of physical security, functions of security systems and security standards	2
3.	Understanding the client’s security needs	2
4.	Conducting security risk assessment for the client’s site	2
5.	The basic configuration and application of an intrusion detection alarm system	3
6.	The basic configuration and application of a video recording or CCTV surveillance system	3
7.	The basic configuration and application of an access control system	3
8.	Designing basic premises security systems	3
9.	Knowledge and skills associated with designing basic premises security systems	3
10.	Practical exercises about designing basic premises security systems	4
	Written Examination	1
	Total：	27

Regarding the 3 hours of self-study, it is recommended that learners should use this time to enhance relevant practical knowledge, the scope of which is listed in relevant topics and consolidated in the Self-study Guidelines for Learners.

Assessment Mode

In order to assess whether learners have fully grasped the practical knowledge and skills for designing basic premises security systems and whether the intended learning outcomes have been achieved, it is recommended that each trainee is to be assessed by way of practical exercises and written examination at the end of the course. These should respectively take up 40% and 60% of their total performance.

Details of the practical exercises and their Assessment Mode can be found in the suggestions and materials of the relevant section.

It is recommended that the course-end examination should be in writing and in the form of multiple-choice questions. The scope of examination should cover the topics in the course outline as follows:

Course Outline		Number of Questions
1.	Relevant laws and license requirements	3
2.	Principles of physical security, functions of security systems and security standards	3
3.	Understanding the client’s security needs	3
4.	Conducting security risk assessment for the client’s site	3
5.	The basic configuration and application of an intrusion detection alarm system	4
6.	The basic configuration and application of a video recording or CCTV surveillance system	4
7.	The basic configuration and application of an access control system	4
8.	Designing basic premises security systems	3
9.	Knowledge and skills associated with designing basic premises security systems	3
10.	Practical exercises about designing basic premises security systems	0
	Total:	30

The recommended Assessment Mode of the course-end examination is summarized below:

Assessment Mode：	Written Examination
Content of Examination:	Multiple Choice Questions
Number of Questions	30 (The scope should cover all the topics in the Course Outline and be in the ratio as listed in the above table)
Pass Mark:	Training institutions should set an appropriate pass mark based on the breadth and depth of the questions.

Training institutions should prepare a question bank and ensure that at least 50% of the questions of each examination are different from those of the previous one.

Training institutions should establish necessary examination rules and ensure that learners fully understand and comply with them.

Training institutions should establish a system to ensure that examination results are accurately recorded.

Course Development and Management

Education and training institutions should closely keep track of the training needs of the industry and the guidelines and rules set by relevant regulators (e.g. The Security and Guarding Services Industry Authority) and revise the course content accordingly.

Section 2: Teaching and Assessment Guidelines

Topic: "Relevant Laws and License Requirements"

Teaching Guidelines

Intended Learning Outcomes

Upon completion of this lesson, it is expected that learners will understand the license requirements for engaging in security work about designing premises security systems and the associated laws and regulations.

Contact Hours

It is recommended that the contact hours for this lesson should be not more than 1 hour.

Self-study Guidelines for Learners

It is recommended that learners revise the materials at the websites listed below before the lesson:

Relevant Materials	Website Addresses
• "Security and Guarding Services Ordinance" (Laws of Hong Kong, Cap. 460)	
➢ The Security and Guarding Services Industry Authority is established under the "Security and Guarding Services Ordinance" (Laws of Hong Kong, Cap. 460) to regulate the security industry. What are its key functions?	https://www.sb.gov.hk/eng/links/sgsia/index.html
➢ Definitions of "Security Work" and "Security Device"	https://www.sb.gov.hk/eng/links/sgsia/howto-spp.html
➢ Categories of "Security Work"	
➢ Application Procedures of a Security Personnel Permit	
➢ Which category of "Security Work" does the "design of premises security systems" belong to?	
➢ What are the criteria that one must meet when applying for a security personnel permit for providing services in relation to "installation, maintenance and/or repairing of	https://www.sb.gov.hk/eng/links/sgsia/pdf/GN%20-%20Criteria%20for%20Security%20Personnel%20Permit%20(Eng).pdf

a security device and/or designing (for any particular premises or place) a system incorporating a security device"?	
• "Occupiers Liability Ordinance" (Laws of Hong Kong, Cap. 314)	
➢ Purpose of the "Occupiers Liability Ordinance"	https://www.elegislation.gov.hk/hk/cap314!en-zh-Hant-HK
➢ Definition of an "Occupier"	
➢ What is "common duty of care"?	
• "Occupational Safety and Health Ordinance" (Laws of Hong Kong, Cap. 509)	
➢ The purpose of the "Occupational Safety and Health Ordinance"	https://www.labour.gov.hk/eng/legislat/content4.htm
➢ The roles of the duty holders	
➢ Key provisions of "To prevent fire" and "To provide a safe and healthy work environment" under the Occupational safety and Health Regulation	

Suggested Scope, Contents and Materials

It is recommended that the lesson should focus on the following two areas:

1. Designing premises security systems is one category of "security work" regulated by the "Security and Guarding Services Ordinance" (Laws of Hong Kong, Cap. 460). Security personnel involved in related services must possess a valid Security Personnel Permit.

   It is suggested that the Trainer should guide the learners to discuss:
   - Purpose of the "Security and Guarding Services Ordinance" (Laws of Hong Kong, Cap. 460)
   - Key functions of the Security and Guarding Services Industry Authority
   - Definition of "security work" and "security device"
   - Categories of "security work" and the category that "designing premises security systems" belong to
   - Application procedures of a Security Personnel Permit
   - The criteria for the issuance of relevant Security Personnel Permit

2. When designing premises security systems, the designer owes the common duty of care (to the people using the site). If dangers are caused to the state of the premises or to things done or omitted to be done and resulted in injury or damage to persons or things lawfully on the premises, the designer is liable for such injury or damage in the same way as the occupier of the premises and others.

It is recommended that the Trainer should explain the following to the learners:

- Part 3 of the Occupiers' Liability Ordinance on the extent of occupier’s ordinary duty and the Occupational Safety and Health Ordinance on the roles of employers and occupiers of premises.
- Compare the duty of an “occupier” under the Occupiers Liability Ordinance and the roles of an “employer” under the Occupational Safety and Health Ordinance. Reference may be made to the article “Hong Kong Safety Snapshots: Occupier’s Liability in the Context of Workplace Injuries” published by Herbert Smith Freehills.
- Explain with examples about situations that may easily cause dangers to the state of a premises when designing and making recommendations for basic premises security systems.

Reference Example:

An example is the installation of a lock to a fire exit door against entry from outside by unauthorized persons. This will lead to serious consequences if not carefully managed.

According to Clause B13.2 of the Code of Practice for Fire Safety in Buildings 2011 (October 2015 version) published by the Buildings Department, if it is necessary to secure an exit door against entry from outside, the following conditions must be complied with:

- The locking device should be of the type that is capable of being readily opened from the inside without the use of a key.
- When a push plate, push bar or a single action level handle is installed, it should not be encased.
- A locking device which is electrically operated should be capable of automatic release upon actuation of:
  - An automatic heat or smoke detection system; or
  - The operation of an alarm system; or
  - A central manual override designed and installed to the satisfaction of the Director of Fire Services.
- Upon power failure, the electrical locking device should be released automatically.

- When designing premises security systems, a risk assessment must be carried out to ensure that the design is proportional to risks, comply with relevant safety regulations, and will not cause dangers to the status of the premises. The security

systems and devices are certified to comply with the necessary security standards.

Assessment Guidelines

Assessment Mode

Multiple Choice Questions

Scope of Assessment

Sample Question	Model Answer
Under the Occupational Safety and Health Ordinance, everyone has a role to play in creating a safe and healthy workplace. Which of the following is the role of an occupier? A) Providing and maintaining plant and work systems that do not endanger safety or health B) Ensuring the means of access to and egress from the premises are safe C) Using any equipment or following any laid-down system or work practices D) Providing all necessary information, instruction, training, and supervision for ensuring safety and health E) All the above answers are correct	B

Marking Rubrics

To be able to select the Model Answer

List of Training Aids

No suggestions

References

(Remark: These references are intended for trainers. Their scope may exceed the depth and breadth of relevant topics in the UoC. Training institutions should tailor the materials to suit the needs and abilities of the learners if they decide to adopt them as training materials for the use of the Learners. Copyrights should also be observed. Some of the References may not provide Chinese translation of the materials. Training institutions should translate the materials for the use of the Learners where necessary.)

- "Security and Guarding Services Ordinance" (Laws of Hong Kong, Cap. 460) (must be the latest version); downloadable free of charge from the Hong Kong e-Legislation website (https://www.elegislation.gov.hk/); the latest version at the time of writing this training package was October 2014

- Key functions of the Security and Guarding Services Industry Authority (must be the latest version); downloadable free of charge from the Security and Guarding Services Industry Authority website (https://www.sb.gov.hk/eng/links/sgsia/index.html); the latest version at the time of writing this training package was 19 November 2020

- Relevant information of the Security Personnel Permit (must be the latest version); downloadable free of charge from the Security and Guarding Services Industry Authority website (https://www.sb.gov.hk/eng/links/sgsia/index.html); the latest version at the time of writing this training package was 19 November 2020. Relevant information includes:
  - Definition of "Security Work" and "Security Device" (https://www.sb.gov.hk/eng/links/sgsia/howto-spp.html)
  - Categories of "Security Work" (https://www.sb.gov.hk/eng/links/sgsia/howto-spp.html)
  - How to apply for a Security Personnel Permit (https://www.sb.gov.hk/eng/links/sgsia/howto-spp.html)
  - Criteria for issuing a Security Personnel Permit (https://www.sb.gov.hk/eng/links/sgsia/pdf/GN%20-%20Criteria%20for%20Security%20Personnel%20Permit%20(Eng).pdf)

- "Occupiers Liability Ordinance" (Laws of Hong Kong, Cap. 314) (must be the latest version); downloadable free of charge from the Hong Kong e-Legislation website (https://www.elegislation.gov.hk/); the latest version at the time of writing this training package was September 2018

- Coverage and the Roles of the Duty-holders of the "Occupational Safety and Health Ordinance" (Laws of Hong Kong, Cap. 509); reference may be made to the relevant web page of the Labour Department (https://www.labour.gov.hk/eng/legislat/content4.htm)

- "Hong Kong Safety Snapshots: Occupier's Liability in the Context of Workplace Injuries" (https://hsfnotes.com/asiadisputes/2020/07/16/hong-kong-safety-snapshots-occupiers-liability-in-the-context-of-workplace-injuries/)

- Code of Practice for Fire Safety in Buildings 2011 (October 2015 version) Subsection B3 – Doors in Relation to Exits Clause B13.2 (https://www.bd.gov.hk/doc/en/resources/codes-and-references/code-and-design-manuals/fs2011/partB1.pdf)

Topic: Principles of physical security, functions of security systems and security standards

Teaching Guidelines

Intended Learning Outcomes

Upon completion of this lesson, it is expected that learners will understand the importance of the principles of physical security, functions of security systems and security standards to designing premises security systems.

Contact Hours

It is recommended that the contact hours for this lesson should be not more than 2 hours.

Self-study Guidelines for Learners

Not applicable

Suggested Scope, Contents and Materials

It is recommended that the lesson should focus on the following three areas:

1. Physical security

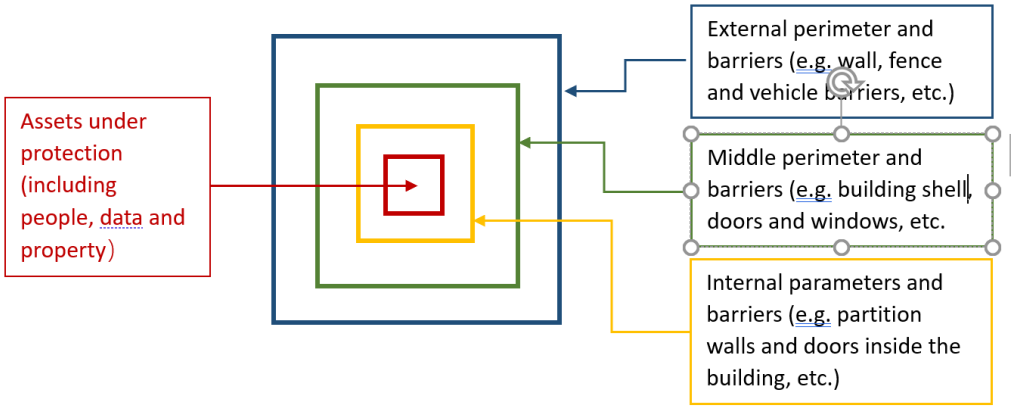
    - Introduce the components of physical security.

    - Explain the following two physical security principles:
        - Protection in Depth / Security in Depth / Defense in Depth
        - Crime Prevention Through Environmental Design “CPTED”

      The Trainer may refer to the reference materials in the next page.

Reference Materials for Trainer:

The Components of Physical Security



They include:

- Perimeters and Barriers: They serve to segregate protected areas into zones; direct people and vehicles to use designated entrances/exits to go in and out of the areas; and delay any unauthorized incoming or outgoing activities. The above diagram depicts a common setup of perimeters/barriers in a building. In Hong Kong, especially in urban areas which space is short, many buildings may only have the middle and internal perimeters and barriers but no external perimeter and barrier.
- Access Control Measures (e.g.: Deploying security personnel or access control systems at key entrances/exits to monitor and control people and vehicles getting in and out of protected areas.)
- Detection Measures (e.g.: Deploying security patrol personnel or installing intrusion detection alarm systems to detect any unauthorized intrusion of protected areas so that security personnel may respond appropriately.)
- Surveillance Measures (e.g.: Using glass walls or installing CCTV surveillance systems to allow monitoring of activities inside protected areas.)

A physical security program should effectively perform the following four functions:

- Deterrence
- Detection
- Delaying
- Response

Protection in Depth / Security in Depth / Defense in Depth serves to provide multiply layers of protection to assets at risk, e.g.: cash kept in a bank may lead to burglary. Banks, therefore, arrange multiple layers of protection for cash storage, including: the building shell, the partitions between the customer lobby and the cash teller area, back office, cashier room, and cash containers such as a safe or

vault inside the cashier room. Furthermore, technological, and other security measures are also deployed to prevent the risk of an occurrence of a burglary. The barriers and containers are designed and built of materials to certain security specifications which may resist break-in and delay the departure of criminals up to give time for the emergency personnel to respond to the event.

Crime Prevention Through Environmental Design "CPTED" originated in the US in the 1960s. It involves the use of environmental design to reduce criminal activities in protected areas, thereby improve community safety. Common CPTED principles include natural surveillance, access control, territorial reinforcement, and space management. In Hong Kong, CPTED principles can be found in many areas for the reduction of crime, e.g.

- The use of glass walls and keeping lights on after hours by retail shops
- The use of glass walls and positioning of customer lobby and teller counters to face the streets outside by banks
- The use of well-lit pedestrian bridges instead of pedestrian underground passages by the government in recent years
- In most properties (particularly residential properties), trees, bushes, lighting, pavements, notices, etc. are commonly used to direct people to exits under control, mark the ownership and accepted activities within the territory.

2. The Functions of Security Systems

It is recommended that the Trainer should guide the learners to discuss the effect of security systems in following four functions:

- Deterrence
- Detection
- Delaying
- Response

Reference Points for Trainer:

- Security systems are one category of the components of physical security. Other categories include barriers inside and outside a building (e.g. fences, walls, doors, and windows); security equipment/hardware (e.g. safe, vault) and security personnel, etc.

- The key functions of security systems are:
  - To reduce the workload of security personnel but they cannot

completely replace their role.
  - To increase the efficiency and effectiveness of the security control room and security personnel in responding to incidents
  - To automatically respond to pre-set events

- Security systems may have the following effects:
  - To create a deterrent effect
    - When an intrusion detection alarm system is activated
    - When cameras are visible
    - When a card reader produces a specific sound in denying entry
  - To detect intrusion in the shortest time possible
    - When sensors are deployed to monitor the external perimeter
    - When a camera is fitted with motion detection function for monitoring
    - When magnetic sensors are fitted for monitoring doors on the external perimeter
  - To deny entry through checking of credentials
    - When two-factor authentication is required for credential checks during non-office hours
    - When anti-tailgating measures are installed at key entrances and exits
  - To delay unauthorised entry using electric locks with physical locking force

3. Security Standards

Explain the following points:

- Security systems and equipment are normally marked with the security standards that they comply with (e.g. door locks that comply with BS3621). Through the security standards, users may understand their security specifications, applications, and methods of installation.

- Security systems and equipment must be tested and certified by the responsible certification body before they can publish the relevant security standards in their product specifications.

- Apart from practical needs, users often adopt security systems as required by insurance companies. Before underwriting an insurance policy, the insurer may require the insured to deploy security measures, systems and installations that are proportional to their security risks.

- Commonly seen security standard labels

Security Standard Labels and the Associated Organizations	Website Address
ISO (International Standards Organization) is a non-governmental organization with a membership of 164 member states, including national standards bodies and major companies in each member state. It is an international standards establishment body that formulates international standards for industry and commerce around the world.	https://www.iso.org/home.html
ASTM (American Society for Testing and Materials) originated from the United States. It is an international standards organization that develops and publishes voluntary consensus technical standards for a wide range of materials, products, systems, and services.	https://www.astm.org/
GB (Guobiao) is the national standard of the People’s Republic of China.	http://www.gbstandards.org/index.asp
ANSI (American National Standards Institute) is the national standard of the United States	https://www.ansi.org/
BSI (British Standards Institution) is the national standard of the United Kingdom	https://www.bsigroup.com/en-GB/
EN (European Standard) is the standard of the European Union	https://www.cencenelec.eu/european-standardization/european-standards/
UL (Underwriter Laboratories) is an independent safety certification company established in the United States	https://www.ul.com/

- Security standards relevant to security systems (refer to “BSI Security Standards” https://shop.bsigroup.com/categories/security-systems)

Assessment Guidelines

Assessment Mode

Multiple Choice Questions

Scope of Assessment

Sample Question	Model Answer
Which of the following is not a component of physical security? A) Security personnel B) Building shell C) Smoke detector D) CCTV system E) Door lock	C

Marking Rubrics

To be able to select the Model Answer

List of Training Aids

No suggestions

References

(Remark: These references are intended for trainers. Their scope may exceed the depth and breadth of relevant topics in the UoC. Training institutions should tailor the materials to suit the needs and abilities of the learners if they decide to adopt them as training materials for the use of the Learners. Copyrights should also be observed. Some of the References may not provide Chinese translation of the materials. Training institutions should translate the materials for the use of the Learners where necessary.)

- ASIS International publication： Facilities Physical Security Measures Guideline (ASIS GDL FPSM-2009)
- ASIS International publication： Protection of Assets - Physical Security
- "Security in Depth" (https://www.protectivesecurity.govt.nz/physical-security/lifecycle/design/apply-good-practices/security-in-depth/)
- What is "Crime Prevention Through Environmental Design"?

(https://designforsecurity.org/crime-prevention-through-environmental-design/)

- BSI Security Standards (https://shop.bsigroup.com/categories/security-systems)

Topic: Understanding the client’s security needs

Teaching Guidelines

Intended Learning Outcomes

Upon completion of this lesson, it is expected that learners will learn about how to understand the client’s physical security needs and the factors to consider.

Contact Hours

It is recommended that the contact hours for this lesson should be not more than 1.5 hours.

Self-study Guidelines for Learners

Not applicable

Suggested Scope, Contents and Materials

It is recommended that the lesson should focus on the following two areas:

1. An effective physical security plan

   Explain the elements of an effective physical security plan:
   - Be proportional to the security risks of the protected site
   - Comply with relevant laws and regulations
   - Integrated with the client's business operations or daily activities
   - Provide the client with total protection

2. Understand the client’s physical security needs

   It is suggested that drawing from personal experience and making use of various types of residential and small and medium-sized industrial and commercial properties, the Trainer should guide the learners to analyse factors to be considered in each of the following areas for each site and discuss where the information can be obtained:

   - Assets to be protected (including people, data and property) and their value
   - The location, surrounding environment, and security risks inherent in the community to which it belongs

- The site environment
- Crimes that occurred in the community and the crime figures
- Crimes that occurred in similar venues at other locations and the crime figures
- The client’s business operations or daily activities and the operating hours
- Site users and visitors (including number, purpose of use and time of use, age, culture, and whether there are pets, etc.)
- The duty of care that the client owes to the site users and visitors
- The layout and existing security measures of the site (including the time required for security personnel or police to respond to an event)
- The client's security policy or security philosophy
- The client's appetite for security risks
- (If insured) understand any security requirements specified by the insurer

(Remark:

- Security risk assessment will be the topic for the next lesson
- Relevant legal liabilities were discussed in the topic “Relevant Laws and License Requirements”)

Assessment Guidelines

Assessment Mode

Multiple Choice Questions

Scope of Assessment

Sample Question	Model Answer
Which of the following is not an asset protected by physical security? A） Safety of people B） Building infrastructure C） Intellectual property D） Computer and equipment E） Cash and property	C

Marking Rubrics

To be able to select the Model Answer

List of Training Aids

- No suggestions

References

(Remark: These references are intended for trainers. Their scope may exceed the depth and breadth of relevant topics in the UoC. Training institutions should tailor the materials to suit the needs and abilities of the learners if they decide to adopt them as training materials for the use of the Learners. Copyrights should also be observed. Some of the References may not provide Chinese translation of the materials. Training institutions should translate the materials for the use of the Learners where necessary.)

- No suggestions

Topic: Conducting security risk assessment for the client’s site

Teaching Guidelines

Intended Learning Outcomes

Upon completion of this lesson, it is expected that learners will understand how to perform a security risk assessment for a site.

Contact Hours

It is recommended that the contact hours for this lesson should be not more than 1.5 hours.

Self-study Guidelines for Learners

Not applicable

Suggested Scope, Contents and Materials

It is recommended that the lesson should focus on the following three areas:

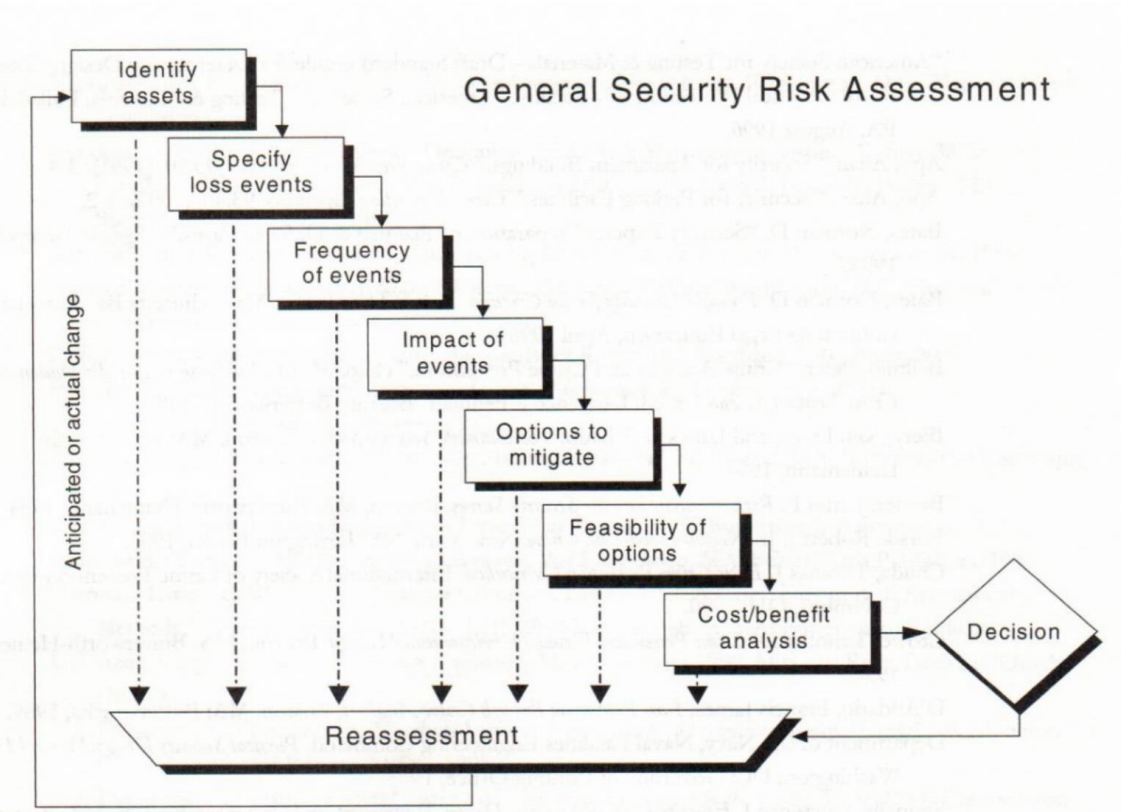
1. The purpose of performing a security risk assessment

   Explain the purpose of performing a security risk assessment.

   Key points:
   - A security risk assessment is a systematic and comprehensive framework for security personnel to analyse all relevant factors of a site, evaluate the security risks and determine a reasonable risk level. Based on the security risk level identified, the strength of countermeasures and the priorities in allocating resources for the countermeasures are then determined.

2. The process for performing a security risk assessment

   Explain the process for performing a security risk assessment.



Process Flow Chart. This flow chart graphically represents this process.

Note 1: The above Process Flow Chart is extracted from the "General Security Assessment Guideline" published by "ASIS International". It is for the reference of the Trainer.

Note 2: Data required in the initial four steps of the Process Flow Chart can be obtained according to the factors for consideration and ways of data collection discussed in the previous topic "Understanding the client's security needs".

3. Data analysis and evaluation of the security risk level of the site

Explain how to perform the following three steps and their inter-relationship:

- Evaluate the frequency of events
- Evaluate the impact or loss caused by the events
- Determine their security risk level

In general, security risk assessment can be performed through qualitative research or quantitative research or a combination of both.

The Trainer should remind learners that when determining the security risk level, the frequency of events and the impact or loss caused by the events must be taken into consideration at the same time by referring to the following formula:

Risk = Frequency x Impact

Regarding Qualitative Research and Analysis, reference may be made to EU Standards EN 50131-1 for Intrusion Detection Alarm Systems, under which alarm systems are classified into 4 grades and applied to premises of different risk levels.

The following is an example to demonstrate how to quantify data obtained for analysis. It is for the reference of the Trainer.

Example:

A burglary occurred in the jewelry shop next to a café. Wondering whether an intrusion detection alarm system should be installed, the café owner appointed a security personnel to conduct a security risk assessment. Relevant data are listed below:

- Located at the ground floor of a commercial and residential building, the café has a floor area of about 500 square feet. There are two exits. The front door is the main exit for people to enter or leave the café. The back door is the emergency exit which is fitted with a push bar and cannot be opened from the outside. When opened on the inside, an alarm bell will sound for 15 minutes.
- The café is divided into the kitchen, washroom, cashier counter and shop floor.
- Apart from the owner and the cashier, there are four other members of staff – two working in the kitchen and two working at the shop floor.
- The operating hours of the café is from 7 am to 6 pm.
- The main door is protected by a roller shutter and both the owner and the chef have the keys for the main door and the roller shutter.
- A CCTV recording system is installed to monitor the cashier counter to deter the cashier from stealing and provide evidence in case of disputes with customers over cash handling.
- At the end of each day, the owner will take the daily revenue away. Hence, there will not be any cash or valuables in the café after hours.
- The café has never experienced any crimes or security events.

Quantitative analysis and evaluation:

Crime	**Frequency (1 - 5；1 being the lowest)**	**Impact or Loss (1 - 5；1 being the lowest)**	**Security Risk = Frequency X Impact/Loss**
Theft	1 (Remark 1)	2 (Remark 2)	2 (Remark 3)

Robbery	1 (Remark 1)	3 (Remark 2)	3 (Remark 3)
Burglary	2 (Remark 1)	1 (Remark 2)	2 (Remark 3)

Notes:

1. Theft, robbery, and burglary have never taken place and there are no valuables in the café to attract criminals. The frequency should be at the lowest score of 1. However, the jewelry shop next door has just been burgled into, indicating the existence of burglars in the community. The frequency may be relatively raised and hence set at the score of 2.
2. Theft or robbery would only take place during business hours. The maximum loss would be the daily revenue. Hence, impact from theft would be 2. Robbery may result in injury to personnel and the score of impact should be relatively higher and set at 3. Burglary occurs outside business hours when there will be no cash and nobody inside. The impact from burglary should therefore be set at the lowest score of 1.
3. The scores for security risk level are therefore theft (2), robbery (3) and burglary (2).

As shown in the above analysis and evaluation, although the frequency of occurrence of burglary is the highest, its risk level is lower than robbery after taking "damage or loss" into consideration.

Regarding whether the owner of the café should install an intrusion detection alarm system, the following should be referred to:

- The café is a small shop. There is no high value property and may only attract inexperienced criminals.
- An intrusion detection alarm system can only be activated outside business hours. However, there will not be any cash or personnel requiring protection. Since the risk level is low, it would not be cost-effective to install an intrusion detection alarm system.
- The security risk level of robbery is comparatively higher. When it happens, staff may activate the alarm through a panic button for assistance. The café is an open environment where customers and personnel could easily see what is happening. The installation of an alarm system would be superfluous and would not be cost-effective.
- Since there is no high value property inside the café, it is unlikely that it would become the target of heavily armed criminals. A more practical approach to reduce the risk of robbery is to train staff to avoid direct confrontations with the robbers.

Assessment Guidelines

Assessment Mode

Multiple Choice Questions

Scope of Assessment

Sample Question	Model Answer
Which of the following is a factor for consideration during a security risk assessment? A） The value of assets B） Security threats C） The mode of operation or living habits of the site users D） Security events E） All of the above	E

Marking Rubrics

To be able to select the Model Answer

List of Training Aids

No suggestions

References

(Remark: These references are intended for trainers. Their scope may exceed the depth and breadth of relevant topics in the UoC. Training institutions should tailor the materials to suit the needs and abilities of the learners if they decide to adopt them as training materials for the use of the Learners. Copyrights should also be observed. Some of the References may not provide Chinese translation of the materials. Training institutions should translate the materials for the use of the Learners where necessary.)

- ASIS International publication： General Security Risk Assessment Guideline

Topic: The basic configuration and application of an intrusion detection alarm system

Teaching Guidelines

Intended Learning Outcomes

Upon completion of this lesson, it is expected that learners will understand the basic configuration and application of an intrusion detection alarm system.

Contact Hours

It is recommended that the contact hours for this lesson should be not more than 3 hours.

Self-study Guidelines for Learners

It is recommended that learners revise the materials at the websites listed below before the lesson:

Relevant Materials	Website Addresses
"Noise Control Ordinance" (Laws of Hong Kong, Cap 400) Section 13A	https://www.elegislation.gov.hk/hk/cap400?xpid=ID_1438403155940_001
The Police Phased Response for Intruder Alarms	https://www.police.gov.hk/ppp_en/04_crime_matters/cpa/iaiu.html

Suggested Scope, Contents and Materials

It is recommended that the lesson should focus on the following four areas:

1. The main functions of an intrusion detection alarm system

   Including:
   - Detect unauthorized intrusion through electronic sensors
   - Report and log alarm events
   - Activate and assist in the process of response (identifying the intrusion location and route)

2. System Components

Key Points:

- Key components of the system and their operational dependency
  - Sensors: detect an intrusion and provide information to the system backend
  - System Backend: raise an alarm through the output devices according to pre-set procedures once an intrusion is detected
  - Output Device: notify security personnel to carry out response actions
  - System Operation Interface: facilitate means for personnel to manage the entire system

- Commonly used sensors, their function, application, and limitation, including:
  - Position Detection Device (e.g.: magnetic door contact)
  - Motion Detector (e.g.: infrared sensors)
  - Vibration Sensor
  - Glass Break Sensor
  - Duress / Panic Alarm

- Output devices, their functions, applications, and limitations, including:
  - Alarm Bell
  - Buzzer
  - Lighting

  (Remark: The requirement of section 13A of Noise Control Ordinance (Laws of Hong Kong, Cap 400) should also be discussed. Under this section, an intrusion detection alarm system installed in any premises is required to be provided with an efficient automatic device which shall cause any audible signal to cease not more than 15 minutes after the activation of the signal.)

- System Backend, including the system panels and the metal enclosures

- Power supply and backup power

- System Operation Interfaces
  - Components include computer software, wall mount keypad, key switch, etc.
  - Functions include managing sensor assignment, arm or disarm, and partition, etc.

3. System Application

Key Points:

- The system and associated devices should be installed according to the specifications of the manufacturer.
  - The security level of the system should be proportional to the security risk level of the site

  - The associated devices of the system (including sensors, controllers and the equipment for connecting the controllers and related devices) should be installed within the protected areas or restricted access areas, or monitored round-the-clock and being able to raise alarms if tampered with.

- Common methods for detecting intrusion to a 3-dimensional space
  - Example:
    - Detect intrusion through the front and back doors using magnetic door contacts
    - Detect intrusion through the walls using volumetric vibration sensors
    - Detect activities of unauthorised intruders inside protected areas using motion detection sensors

    (Remark: When selecting sensors and their installation location, security threats and the surrounding environment should also be taken into consideration.)

- Central Alarm Monitoring Station (CAMS)
  - Main functions:
    - Provides 24-hour alarm monitoring
    - Responds according to pre-set procedures such as viewing live videos, contacting key holders, calling the police, etc.
  - Relationship between an intrusion detection alarm system and CAMS
    - CAMS specified electronic control panels will be installed on site and connected with CAMS through alarm lines
    - Types of alarm lines include dedicated lines, telephone lines and networks, etc.
    - An intrusion detection alarm system achieves its function of transmitting alarm signals to CAMS through the electronic control panels
  - Index of key holders, including CAMS workflow, key holder information, passwords, and duress codes, etc.

- Other means of monitoring
  Examples:
  - The on-site alarm bell generates audible alarms and creates a deterrent effect
  - Alarms can also be received via mobile app

- The Phased Response to Intruder Alarms Policy of the Hong Kong Police

- Common causes of false alarms and their solution:
  - Environment, e.g.
    - Strong wind blowing on a door that causes the magnetic door contacts to mistake it as the door being forced open
    - Passing-by of heavy vehicles that causes the vibration sensors to mistake it as the wall being attacked by an electric drill

- Man-made, e.g.
  - Failure of personnel to leave the area monitored by intrusion detection alarm system through the evacuation route within the specified time limit
- Cables, e.g.
  - Signals are subject to external electronic interferences
- Power supply, e.g.
  - Unstable power supply
- Installation standard, e.g.
  - Sensors not properly secured
- Sensitivity of devices, e.g.
  - Electronic article surveillance (EAS) panel that are too sensitive and trigger the alarm in a shop
- Inappropriate use, e.g.
  - Install infrared sensors in busy areas

4. Relevant international standards

- BS 4737 series – Intruder alarm systems. Specifications for components.
- BS EN 50131 series – Alarm systems. Intrusion and hold-up systems

The following materials are for the reference of the Trainer:

BS4737 is published by the BSI in UK which provides in detail the specifications and installation standards of each component of an intrusion detection alarm system. The latest version was released in 2015, which provides the standard for different types and grades of cables. To ensure the reliability of the design, installation and maintenance of an intrusion detection alarm system, suppliers and installers refer to the specifications and operation guidelines in BS 4737. In recent years, BS 4737 is gradually replaced by BS EN 50131.

A comparison of the two series indicates that BS EN 50131 is better than BS 4737 in that it is more structured, grades the systems, classifies the equipment, and promotes a risk-based approach in deploying an alarm system to protected site.

Under BS EN 50131, intrusion detection alarm systems are classified into four grades:

- Grade 1: Intruders are unlikely to target the premises
  - For residential premises where the installation of an alarm is not required for insurance purposes.
  - It guards against intruders who are more likely to break in and enter through a front or back door
- Grade 2: There is a higher risk of theft due to valuable property being kept on

site
  - For low premises with some cash
  - It guards against intruders who may be experienced thieves who carry tools, have knowledge of intruder alarms and consider entering the property through windows and doors.
- Grade 3: There is a substantial threat from experienced intruders due to high-value contents
  - For premises with high-value contents
  - It guards against seasoned criminals, who are experienced in tampering with intruder alarm systems and carry tools and equipment to overcome them
- Grade 4: The property has a very high risk of being targeted by organized criminals
  - For extremely high-risk premises, such as a bank, jewelry store, or an office that deals with classified information
  - It guards against criminals who may have the knowledge and equipment to prevent detection and may consider all possibilities to breaking and entering the property, including access through the ceiling or floor

Based on BS EN 50131, practitioners have also developed Code of Practice for:

- Assessment of risk
- Technical survey
- System design
- Installation of the system in accordance with the agreed specification
- Installation of equipment in accordance with manufacturers’ recommendations

From a user’s perspective, an alarm system that corresponds to its security risk level and based on BS EN 50131 would meet his needs better and be more cost-effective.

Assessment Guidelines

Assessment Mode

Multiple Choice Questions

Scope of Assessment

Sample Question	Model Answer
Under which of the following conditions should an infrared sensor be deployed? A） Where there is large fluctuation in temperature B） Where there is little fluctuation in temperature C） Where there are people moving about all day D） At an outdoor carpark E） All of the above	B

Marking Rubrics

To be able to select the Model Answer

List of Training Aids

- Intrusion detection alarm system diagrams
- Samples of various sensors

References

(Remark: These references are intended for trainers. Their scope may exceed the depth and breadth of relevant topics in the UoC. Training institutions should tailor the materials to suit the needs and abilities of the learners if they decide to adopt them as training materials for the use of the Learners. Copyrights should also be observed. Some of the References may not provide Chinese translation of the materials. Training institutions should translate the materials for the use of the Learners where necessary.)

- "Intrusion Detection Systems" by David J. Brooks and Michael Coole; Security Science, School of Science, Edith Cowan University, Perth, WA, Australia. (https://www.researchgate.net/publication/334706920_Intrusion_detection_systems)

- ASIS International publication: Facilities Physical Security Measures Guideline ASIS GDL FPSM-2009

- BS4737 (https://shop.bsigroup.com/ProductDetail/?pid=000000000030295318)

- British and European Intruder Alarm Standards (https://www.alertsystems.co.uk/about/industry-standards/bs-en-intruder-alarm/)

- EN50131 Guide – Intruder Alarm Grades Made Simple (https://www.businesswatchgroup.co.uk/en50131-guide-intruder-alarm-grades-made-

simple/)

- “Noise Control Ordinance” (Laws of Hong Kong, Cap. 400) Section 13A （https://www.elegislation.gov.hk/hk/cap400!en?INDEX_CS=N&xpid=ID_1438403155940_001）

- The Police Phase Response for Intruder Alarms Policy https://www.police.gov.hk/ppp_en/04_crime_matters/cpa/iaiu.html#:~:text=THE%20POLICE%20PHASED%20RESPONSE%20FOR,is%20considered%20as%20time%20wasted

Topic: "The basic configuration and application of a video recording or CCTV surveillance system"

Teaching Guidelines

Intended Learning Outcomes

Upon completion of this lesson, it is expected that learners will understand the basic configuration and application of a video recording or CCTV surveillance system.

Contact Hours

It is recommended that the contact hours for this lesson should be not more than 3 hours.

Self-study Guidelines for Learners

It is recommended that learners revise the materials at the websites listed below before the lesson:

Relevant Materials	**Website Addresses**
Guidance on CCTV Surveillance Practices	https://www.pcpd.org.hk/english/publications/files/CCTVpractices_e.pdf
Privacy Guidelines: Monitoring and Personal Data Privacy at Work - in respect of CCTV monitoring	https://www.pcpd.org.hk/english/data_privacy_law/code_of_practices/files/Monitoring_and_Personal_Data_Privacy_At_Work_revis_Eng.pdf

Suggested Scope, Contents and Materials

It is recommended that the lesson should focus on the following four areas:

1. Key functions of a video surveillance system

   Key Points:
   - Create a deterrent effect
   - Keep records of videos
   - Broadcast live videos
   - Support security responses
   - Provide more complete evidence for security events

2. System components, their operational dependency, and their types, functions, applications, and limitations

   Key Points:

   - Cameras: collect videos
     - Explain the differences between CCTV cameras and network cameras
     - CCTV systems
       - Advantages
         - Lower material cost
         - Easy installation
       - Disadvantage
         - Lower resolution
     - Network systems
       - Advantages
         - Higher resolution
         - More flexible design
       - Disadvantages
         - Higher material cost

   - Cables: video transmission
     - CCTV cameras commonly use RG59 cable and BNC connector to directly connect to the recorder
     - IP cameras commonly use CAT5E cable and RJ45 connector to connect to the network switch

   - Recorders and storage devices
     - CCTV recorders are directly connected to CCTV cameras
     - Network recorders are connected to IP cameras through network switches

   - System Operation Interfaces
     - Types of Interfaces
       - Recorder inbuilt interfaces
       - Terminal software interfaces
     - Functions of Interfaces
       - Manage videos
       - Manage recording parameters
       - Video playback (live and recorded)

3. System Applications

   Key Points:

- Systems and associated devices should be installed according to the specifications of the manufacturers
    - System control and storage devices and the equipment for connecting recorders and the control and storage devices should be installed within the protected areas or restricted access areas or in areas that are monitored round the clock and alarms will be generated when tampered with.

- Different applications will require different functions of the components. Before selecting a component, it is necessary to understand:
    - What is the purpose of application of a system?
    - What images/views are required for each camera, e.g.: facial recognition, differentiating actions, monitoring of scene?
    - What are the requirements for live monitoring or recording?

- Essential parameters of camera functions

  Including:
    - Frame Rate
        - The number of photos taken per second (If it is 10 frames, it means 10 photos are taken per second.)
        - Considerations for this parameter
            - Too high: recorder storage will be wasted
            - Too low: events cannot be effectively recorded
            - Appropriate frame rate should be proportional to the speed of activities of the events to be recorded
    - Resolution
        - Resolution of each photo (picture element or short for pixel)
        - Considerations for this parameter
            - Too high: recorder storage will be wasted
            - Too low: events cannot be effectively recorded
            - Appropriate resolution should be proportional to the size of the recorded area
    - Lens Focal Length
        - Video angle
        - Considerations for this parameter
            - Too high: the video angle will be too narrow, and the video range will decrease
            - Too low: the video angle will be too wide, and the resolution of the video will decrease
            - Appropriate lens focal length should be based on the range that the camera is required to monitor
    - Lux requirements
        - Minimum lux requirements for video recording

  - Too high: unable to record under normal conditions
  - Too low: the cost of cameras will be increased unnecessarily
  - Appropriate lux requirements should be the lowest lighting in the range that the camera is required to monitor

- Video-recorder Functions

  Including:
  - Storage Bandwidth
    - The upper limit of bandwidth at which videos can be saved to the hard drive
      - Too high: the cost of recorders will be unnecessarily increased
      - Too low: videos may fail to be saved to the hard drive
      - Appropriate storage bandwidth should be twice the maximum storage bandwidth of the recording videos
  - Channel Limit
    - The maximum number of cameras that a recorder can manage
      - Too high: the cost of recorders will be unnecessarily increased
      - Too low: the number of cameras will be restricted
      - Appropriate Channel Limit should have 10-20% spare reserved for future expansion
  - Video Search Function
    - Video-recorders can search and provide results based on specific parameters
    - Common search parameters
      - Time range
      - Motion detection
      - Colour

- System application and personal privacy

  Video recording or CCTV surveillance systems may capture large number of personal images or personal data. When deploying such a system, the following two guidelines of the Office of the Privacy Commissioner for Personal Data should be familiarised with:
  - Guidance on CCTV Surveillance Practices
  - Privacy Guidelines: Monitoring and Personal Data Privacy at Work - in respect of CCTV monitoring

  It is recommended that the Trainer should guide the learners to discuss about how to comply with the requirements of the “Personal Data (Privacy) Ordinance (Laws of Hong Kong, Cap. 460) regarding the collection of personal data and avoid applying the system wrongly resulting in a breach of the privacy of personal data.

4. Relevant International Standards

- BS EN 62676 series "Video Surveillance Systems for Use in Security Applications"

Assessment Guidelines

Assessment Mode

Multiple Choice Questions

Scope of Assessment

Sample Question	**Model Answer**
Which of the following is the biggest difference between a CCTV camera and an IP camera? A） Maximum frame rate B） Minimum lux requirements for video recording C） Lens focal length D） The connection method between the camera and video recorder E） All of the above answers are incorrect	D

Marking Rubrics

To be able to select the Model Answer

List of Training Aids

- Diagrams of video recording or CCTV surveillance systems
- Samples of CCTV cameras
- Samples of IP cameras

References

(Remark: These references are intended for trainers. Their scope may exceed the depth and breadth of relevant topics in the UoC. Training institutions should tailor the materials to suit the needs and abilities of the learners if they decide to adopt them as training materials for the use of the Learners. Copyrights should also be observed. Some of the References may not provide Chinese translation of the materials. Training institutions should translate the materials for the use of the Learners where necessary.)

- ASIS International publication – Facilities Physical Security Measures Guideline ASIS GDL FPSM-2009

- BS EN 62676 series “Video Surveillance Systems for Use in Security Applications” https://landingpage.bsigroup.com/LandingPage/Series?UPI=BS%20EN%2062676

- Guidance on CCTV Surveillance Practices https://www.pcpd.org.hk/english/publications/files/CCTVpractices_e.pdf

- Privacy Guidelines: Monitoring and Personal Data Privacy at Work - in respect of CCTV monitoring https://www.pcpd.org.hk/english/data_privacy_law/code_of_practices/files/Monitoring_and_Personal_Data_Privacy_At_Work_revis_Eng.pdf

Topic: The basic configuration and application of an access control system

Teaching Guidelines

Intended Learning Outcomes

Upon completion of this lesson, it is expected that learners will understand the basic configuration and application of an access control system.

Contact Hours

It is recommended that the contact hours for this lesson should be not more than 3 hours.

Self-study Guidelines for Learners

Not applicable

Suggested Scope, Contents and Materials

It is recommended that the lesson should focus on the following four areas:

1. Key Functions

   Key Points:

   - Conditional access control
     - Types of credentials
       - What you are (such as fingerprints or iris)
       - What you have (such as electronic card or key)
       - What you know (such as password or line pattern)
     - Time (such as office hours, non-office hours, holidays, etc.)
     - Location of exits (such as main door, back door, computer rooms, etc.)
     - Alert status
   - Recording IN and OUT activities
   - Create/delete/modify information of credential holders

2. System Components

   Key Points:

- Electric locks (such as electromagnetic locks, mortise locks, key locks, handle locks, etc.)
- Credential readers (such as card readers, fingerprint readers, keypads, etc.)
- Door release buttons
- Door contacts
- Emergency Break Glass
- Key switches
- Backend Terminal, including system panels and metal enclosures
- Power supply and backup power
- System operation interfaces (normally computer software interfaces)

3. System Application

Key Points:

- Systems and associated devices should be installed according to the specifications of the manufacturers
  - System control and storage devices and the equipment for connecting recorders and the control and storage devices should be installed within the protected areas or restricted access areas or in areas that are monitored round the clock and alarms will be generated when tampered with.

- Considerations
  - Centralised systems are used in locations of high people traffic such as an office
  - Decentralised systems / stand-alone devices are used in locations of low people traffic such as a private dwelling

- Basic frontend setup
  - Single or double-leaf swing door
    - Credential reader
    - Electric lock (concealed mount)
    - Door release button
    - Door contact
    - Emergency Break Glass
  - Fire Exit Door
    - Push-bar lock approved by the Fire Services Department

    (<u>Remark</u>:
    According to Clause B13.2 of the Code of Practice for Fire Safety in Buildings 2011 (October 2015 version) published by the Buildings Department, if it is necessary to secure an exit door against entry from outside, the following conditions must be complied with:

- The locking device should be of the type that is capable of being readily opened from the inside without the use of a key.
- When a push plate, push bar or a single action level handle is installed, it should not be encased.
- A locking device which is electrically operated should be capable of automatic release upon actuation of:
  - An automatic heat or smoke detection system; or
  - The operation of an alarm system; or
  - A central manual override designed and installed to the satisfaction of the Director of Fire Services.
- Upon power failure, the electrical locking device should be released automatically.)

4. Relevant International Standard

- BS EN 60839 series - Alarm and electronic security systems. Electronic access control systems.

Assessment Guidelines

Assessment Mode

Multiple Choice Questions

Scope of Assessment

Sample Question	Model Answer
Which of the following items can be used as credential for access control? A） Password B） Iris C） Electronic card D） Fingerprint E） All of the above answers are correct	E

Marking Rubrics

To be able to select the Model Answer

List of Training Aids

- Diagrams of access control systems
- Front view diagrams of single and double leaf swing doors
- Samples of various types of electric locks

References

(Remark: These references are intended for trainers. Their scope may exceed the depth and breadth of relevant topics in the UoC. Training institutions should tailor the materials to suit the needs and abilities of the learners if they decide to adopt them as training materials for the use of the Learners. Copyrights should also be observed. Some of the References may not provide Chinese translation of the materials. Training institutions should translate the materials for the use of the Learners where necessary.)

- ASIS International publication – Facilities Physical Security Measures Guideline ASIS GDL FPSM-2009

- BS EN 60839 series - Alarm and electronic security systems. Electronic access control systems. (https://shop.bsigroup.com/SearchResults/?q=60839)

- Code of Practice for Fire Safety in Building 2011 (October 2015 version)
  Subsection B3 – Doors in Relation to Exits Clause B13.2
  (https://www.bd.gov.hk/en/resources/codes-and-references/codes-and-design-manuals/fs2011.html)

- List of Fire Service Installations and Equipment accepted by the Fire Services Department
  (https://www.hkfsd.gov.hk/eng/source/licensing/approved_fsi.pdf)

Topic: Designing basic premises security systems

Teaching Guidelines

Intended Learning Outcomes

Upon completion of this lesson, it is expected that learners will understand the process and factors for consideration when designing basic premises security systems.

Contact Hours

It is recommended that the contact hours for this lesson should be not more than 3 hours.

Self-study Guidelines for Learners

Not applicable

Suggested Scope, Contents and Materials

It is recommended that the lesson should focus on the following four areas:

1. It is recommended that the Trainer should guide the learners to revise:
    - The principles and functions of physical security
    - The components of physical security
    - The roles of security systems in physical security

2. Explain the design process

    Key Points:

    - Understand the client’s security risks and daily operation
    - Understand areas or assets requiring special protection
    - Conduct site survey to understand its environment and identify gaps in security
      Key points:
        - Arrangements for multiple layers of protection (perimeters, exit points and barriers)
        - Measures and resources for handling security incidents
    - Deploy security systems (intrusion detection alarm system, CCTV recording system and access control system) and the associated equipment to enhance the

effectiveness of physical security

3. Explain the skills for Site Survey

   Key Points:

   - Collect site layout diagrams and related information in advance
   - Understand basic information about the site environment before the survey, including:
     - Site zoning concept: public, semi-public, and private
     - Site perimeters (for separating public and private areas)
     - Boundaries and the exits
     - Fire escape routes and emergency exits
     - Location of sensitive areas, functional areas and areas requiring special protection
     - Security measures and resources for handling security incidents on site
   - Start the survey from the outside to the inside of the site and identify vulnerabilities and gaps in the security measures by carefully observing along the perimeter of each layer of protection.
   - Determine the effectiveness of deploying security systems to plug deficiencies or loopholes

4. Designing premises security systems

   Key Points:

   - Designing an intrusion detection alarm system
     It is recommended that the Trainer should explain to the learners about how to deploy security systems and related equipment, by making use of layout diagrams and other related diagrams of various premises (such as residential, commercial and office sites), including:
     - System overview
     - Frontend devices (such as infrared motion sensors, magnetic door contacts, etc.)
     - Frontend devices performance specifications and selection of devices
     - Methods to reduce false alarms
     - Design of the terminating resistor
     - Design of the arming and disarming route
     - Design of the system zones, including distribution of sensors, entering and evacuating routes, delayed triggers, etc.
     - Quality of cables and calculation of their quantity

   - Designing a video recording or CCTV surveillance system

It is recommended that the Trainer should explain to the learners about how to deploy security systems and related equipment, by making use of layout diagrams and other related diagrams of various premises (such as residential, commercial and office sites), including:

- System overview
- Basic networks
  - Ethernet
    - Most common
    - The cost is comparatively lower
    - For use within 100 meters
  - Fibre-optic network
    - Less common
    - The cost is comparatively higher
    - For use beyond 100 meters
- The required video resolution, number of frames and angle of the location being monitored
- Transmission of electricity through network switches
- Calculation of storage space
- Calculation of cabinet space and heat dissipation considerations
- Quality of cables and calculation of their quantity

- Designing an access control system
  It is recommended that the Trainer should explain to the learners about how to deploy security systems and related equipment, by making use of layout diagrams and other related diagrams of various premises (such as residential, commercial and office sites), including:
  - System overview
  - Types of doors (such as leaf doors, sliding doors, roller shutters, etc.)
  - Door frontend devices (such as credential readers, electric locks, door contacts, door switches and Emergency Break Glass)
  - Frontend devices performance specifications and selection of devices
  - Fire escape doors devices (such as push-bar and lock cylinder, etc.)
  - Metal enclosures and anti-tampering devices
  - Backend type (such as centralized or decentralized)
  - Power supply and backup power
  - Quality of cables and calculation of their quantity

Assessment Guidelines

Assessment Mode

Multiple Choice Questions

Scope of Assessment

Sample Question	Model Answer
Which of the following should be included in a site security survey? A) Fire exit doors B) Passenger lifts C) Cargo lifts D) Computer rooms E) All of the above answers are correct	E

Marking Rubrics

To be able to select the Model Answer

List of Training Aids

- Various sample diagrams

References

(Remark: These references are intended for trainers. Their scope may exceed the depth and breadth of relevant topics in the UoC. Training institutions should tailor the materials to suit the needs and abilities of the learners if they decide to adopt them as training materials for the use of the Learners. Copyrights should also be observed. Some of the References may not provide Chinese translation of the materials. Training institutions should translate the materials for the use of the Learners where necessary.)

- The Design and Evaluation of Physical Protection Systems (2nd Edition) by Mary Lynn Garcia

Topic: “Knowledge and skills associated with designing basic premises security systems”

Teaching Guidelines

Intended Learning Outcomes

Upon completion of this lesson, it is expected that learners will understand knowledge and skills associated with designing basic premises security systems, which will include diagrams, charts and proposals associated with security systems.

Contact Hours

It is recommended that the contact hours for this lesson should be not more than 3 hours.

Self-study Guidelines for Learners

Not applicable

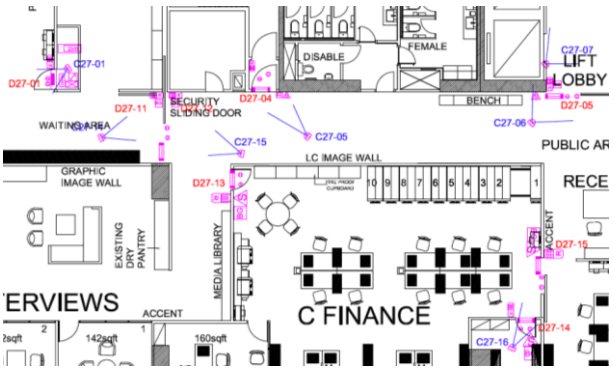
Suggested Scope, Contents and Materials

It is recommended that the lesson should focus on the following two areas:

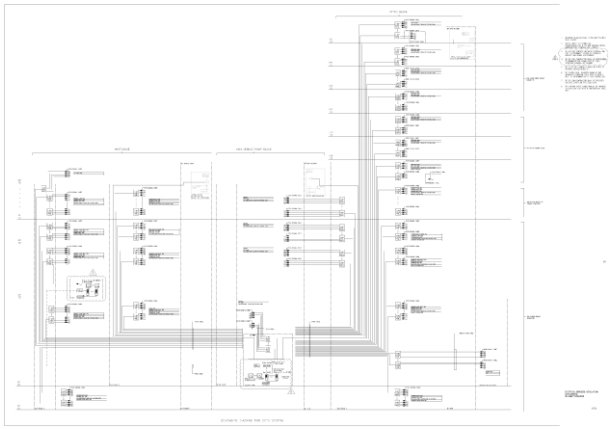
1. Diagrams and charts associated with designing security systems

   It is recommended that the Trainer should explain to learners about the purpose and content of each of the following diagrams and charts.

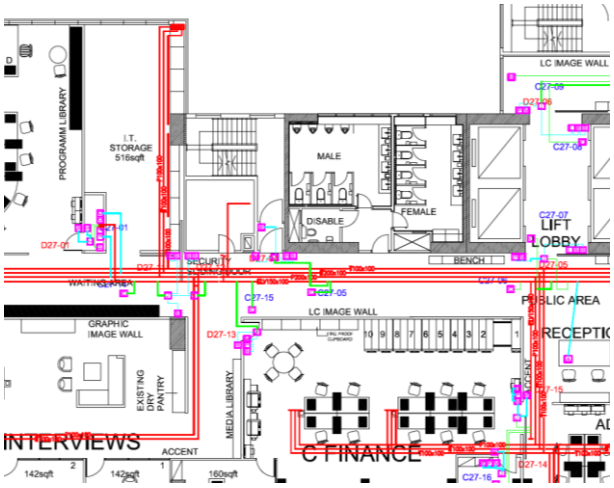
   - Layout diagram - Illustrating the actual location of the devices



- System schematic diagram - illustrating the inter-relationship of the devices



- Conduit layout diagram – illustrating the actual location of the cable containers

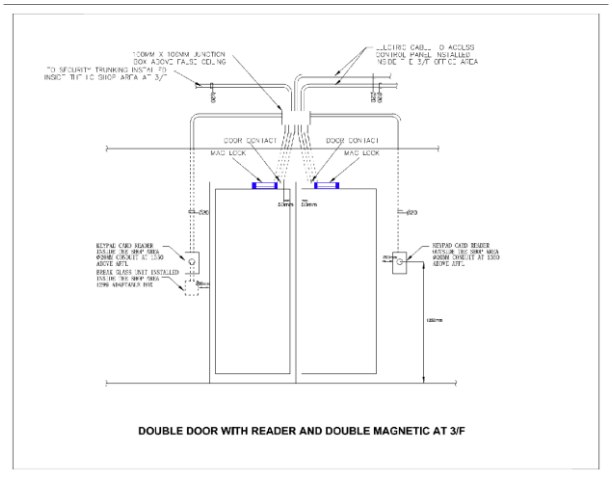


- Cross-floor conduit layout diagram – illustrating the actual location of cross-floor cable containers

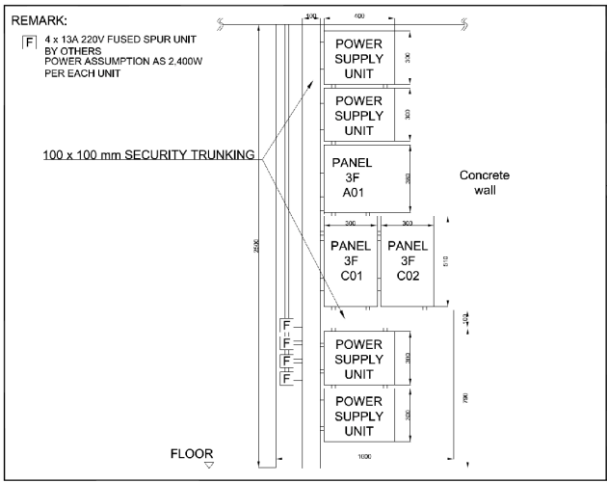
- Door Schedule – illustrating the parameters of each door for design consideration

Door Mark	Door Type	Clear Opening		Door Core								
		Width (mm) [X]	Height (mm) [Y]	Door Leaf			Thickness (mm)	Vision Panel	Door Louvre		Double Door	Mate
				Material	Finish				Clear Width (mm)	Clear Height (mm)		
					Pull Side	Push Side						
D01	A	2100	2100	WD10	PL1	PL1	50	YES	-	-	YES	WD
D01a	A	2100	2100	WD10	PL1	PL1	50	YES	-	-	YES	WD
D01b	A	2100	2100	WD10	PL1	PL1	50	YES	-	-	YES	WD
D01c	A	2500	2300	WD10	PL1	PL1	50	YES	-	-	YES	WD
D01d	A	2100	2100	WD10	PL1	PL1	50	YES	-	-	YES	WD
~~D01e~~	~~A~~	~~2100~~	~~2100~~	~~WD10~~	~~PL1~~	~~PL1~~	~~50~~	~~YES~~	~~-~~	~~-~~	~~YES~~	~~WD~~
D01f	A	2100	2100	WD10	PL1	PL1	50	YES	-	-	YES	WD
~~D01g~~	~~A~~	~~2100~~	~~2100~~	~~WD10~~	~~PL1~~	~~PL1~~	~~50~~	~~YES~~	~~-~~	~~-~~	~~YES~~	~~WD~~
D01h	A	2100	2100	WD10	PL1	PL1	50	YES	-	-	YES	WD
D01j	A	2500	2300	WD10	PL1	PL1	50	YES	-	-	YES	WD
D02	B	1050	2100	WD10	PL1	PL1	50	YES	-	-	-	WD
D02a	B	1050	2100	WD10	PL1	PL1	50	YES	-	-	-	WD
D02b	B	1050	2100	WD10	PL1	PL1	50	YES	-	-	-	WD
D02c	B	1050	2100	WD10	PL1	PL1	50	YES	-	-	-	WD
~~D02d~~	~~B~~	~~1050~~	~~2100~~	~~WD10~~	~~PL1~~	~~PL1~~	~~50~~	~~YES~~	~~-~~	~~-~~	~~-~~	~~WD~~
D02e	B	1050	2100	WD10	PL1	PL1	50	YES	-	-	-	WD

- Door Elevation Diagram – illustrating the actual location of cable containers and frontend devices for the door



- Wall Elevation Diagram – illustrating the actual location of wall mount devices and cable containers



- Server rack elevation diagram – illustrating the actual location of devices at the server rack

Server Rack #1 - 14U

14	Video Encoder 16 Port (1U)
13	Reserved for Heat Dissipation (1U)
12	POE 16 Port Network Switch (2U)
11	
10	POE 16 Port Network Switch (2U)
9	
8	Reserved for Heat Dissipation (1U)
7	Camera Power Supply (2U)
6	
5	Reserved for Heat Dissipation (1U)
4	Video Recorder (4U)
3	
2	
1	

2. Proposals

It is recommended that the Trainer should introduce to the learners of the content of proposals and how to put together the associated information, including:

- Quotation
- Equipment Schedule
- Work Timeline
- Layout diagram
- System diagram
- Workmanship standard
- Maintenance service level agreement

Assessment Guidelines

Assessment Mode

Multiple Choice Questions

Scope of Assessment

Sample Question	Model Answer
Which of the following is not an item of information in the Door Schedule? A）Door number B）Door specification C）Door type D）Cable containers of related security devices E）All of the above answers are incorrect	D

Marking Rubrics

To be able to select the Model Answer

List of Training Aids

- No suggestions

References

(Remark: These references are intended for trainers. Their scope may exceed the depth and breadth of relevant topics in the UoC. Training institutions should tailor the materials to suit the

needs and abilities of the learners if they decide to adopt them as training materials for the use of the Learners. Copyrights should also be observed. Some of the References may not provide Chinese translation of the materials. Training institutions should translate the materials for the use of the Learners where necessary.)

- No suggestions

Topic: “Practical exercises about designing basic premises security systems”

Teaching Guidelines

Intended Learning Outcomes

Upon completion of this lesson, it is expected that through the practical exercises, learners will gain further understanding of the factors to consider when designing premises security system; how to illustrate the security systems and devices in diagrams; and how to persuade clients to accept the recommended security systems.

Contact Hours

It is recommended that the contact hours for this lesson should be not more than 4 hours.

Self-study Guidelines for Learners

Not applicable

Suggested Scope, Contents and Materials

1. Process of Practical Exercises

   It is recommended that the Trainer should prepare no less than 6 sites for practical exercises.

   The learners should be formed into groups of no more than 5 persons each. A site will be assigned to each group.

   Each group should design a security system for their responsible site in no more than 1 hour.

   Lastly, based on 30 minutes per site, the Trainer should lead the whole class to review the system designed for each site.

2. Topics for Practical Exercises

   It is recommended that the topics should be based on small and medium-sized or non-high-risk premises, which may include:
   - Residential units or buildings
   - Shops for different nature of operations or different industrial or commercial purposes

- Office units or floors for different nature of operations or different industrial or commercial purposes

The Trainer should define the purpose of use of each site, basic background information and the security risks that it is faced with. The Trainer should also provide the layout diagrams and associated photographs to help learners understand the site environment. The Trainer should also specify the learners’ tasks.

Trainers may refer to the following sample when designing practical exercises:

After a detached house of 2,000 square feet in a remote area of Sai Kung was burgled into, its owner engaged the company that you work for to design a security system to prevent recurrence or to detect the next burglary and report to the police early.

The owner has a family of 3, which includes husband and wife and a 15-year-old son. There are also 2 domestic helpers and 2 cats.

Outside the house, there is a garden which is surrounded by a fence. The external layout diagram is at Figure 1 and the internal layout diagram is at Figure 2. Relevant photographs can also be viewed at this web page (https://www.rightmove.co.uk/properties/68547768#/media?activePlan=1)

Your task is to design an effective and feasible security system for this house within 1 hour:

- You are required to consider all relevant factors in full
- You are required to mark your recommended system components and their location on the layout diagram

Figure 1：External Layout Diagram

Figures 2： Internal Layout Diagram

3. Presentation of Design Concept and Assessment

Upon completion of the system design, each site will be given no more than 30 minutes:

- In the initial 10 minutes, the responsible group will present the design concept, components, and devices of the system.
- Afterwards, the Trainer and the whole class will review together:
  - Assess whether the group has illustrated the system completely, accurately, and clearly
  - Discuss the feasibility and cost-effectiveness of the system
- Lastly, the Trainer will conclude and evaluate the performance of each group, correct any mistakes made in the process and answer any questions that the learners may have.

It is recommended that the Trainer and learners should records their observations in writing, which will be referred to by the Trainer as well as the assessment records. Reference may be made to the Appendix “Sample Assessment Form of Practical Exercises”.

4. Intended Learning Outcomes of Practical Exercises

Through the practical exercises, learners will:

- Enhance their knowledge and understanding about points to consider when designing premises security systems
- Practise how to illustrate system design and components in diagrams
- Practise how to persuade clients to accept their proposed security systems

5. Venue and Facilities for Practical Exercises

   It is recommended that work benches for teamwork, layout diagrams and photographs should be provided to help learners understand the environment of their assigned site.

Assessment Guidelines

Please refer to “Sample Assessment Form for Practical Exercises”

List of Training Aids

- Sample layout diagrams

References

(Remark: These references are intended for trainers. Their scope may exceed the depth and breadth of relevant topics in the UoC. Training institutions should tailor the materials to suit the needs and abilities of the learners if they decide to adopt them as training materials for the use of the Learners. Copyrights should also be observed. Some of the References may not provide Chinese translation of the materials. Training institutions should translate the materials for the use of the Learners where necessary.)

- The Design and Evaluation of Physical Protection Systems (2nd Edition) by Mary Lynn Garcia

- NFPA 731 Standard for the Installation of Premises System Systems

Appendix

- Sample Assessment Form for Practical Exercises

Sample Assessment Form for Practical Exercises

Exercise Ref.# _____ Topic: _____

Name of Group Members:

_____ _____

_____ _____

_____

Name of Assessor/Observer: _____ Date: _____

Item	Good ◄---------- Bad ----►				Total Scores
	8 scores	6 scores	4 scores	2 scores	
Risk Assessment	•Familiar with relevant risks •Comprehensive consideration •Accurate evaluation	•Familiar with relevant risks •Insufficient consideration •Slightly inadequate evaluation	•Unfamiliar with relevant risks •Insufficient consideration •Wrong evaluation	•No risk assessment	
Design Concept	•Relative to risks •Relative to environment •Relative to operation	•Relative to risks •Slightly not relative to environment •Slihgtly not relative to operation	•Not relative to risks •Insufficient consideration of the client's needs	•Not relative to risks •No consideration of the client's needs	
Knowledge about the system	•Familiar with the system and its operation •Familiar with the component characteristics •Comprehensive design	•Familiar with the system and its operation •Familiar with the component characteristics •Slightly incomplete design	•Unfamiliar with the system and its operation •Slightly insufficient knowledge about the component characteristics •Slightly incomplete design	•Unfamiliar with the system and its operation •Insufficent knowledge about the component characteristics •Incomplete design	
Presentation of the system	•Accurate illustration of the design and components on diagrams	•Slightly inaccurate illustration of the design and components on diagrams	•Fail to illustrate the design and components on diagrams in full	•Confusing illustration	
Feasibility of the design	•Clear objectives •Design can achieve the objectives	•Slightly unclear objectives •Design is relative to objectives	•Unclear objectives •Design can achieve certain level of effect	•Unclear objectives •Effectiveness of design is in doubt	
Total Score:					

Other Suggestions and Comments:

Section 3: Self-study Guidelines for Learners

Intended Learning Outcomes

Upon completion of self-study, learners will understand relevant knowledge and can apply what they have learned in class discussions.

Hours of Self-study and Time of Completion

It is recommended that self-study should be no less than 3 hours and should be completed before the start of the relevant class.

Scope of Self-study, Contents and Suggested Materials

The contents for self-study are extracted from government websites and described in detail in the respective topic in Section 2. They are summarized below:

Topic: "Relevant Laws and License Requirements" - self-study in respect of the following areas:

Relevant Materials	Website Addresses
• "Security and Guarding Services Ordinance" (Laws of Hong Kong, Cap. 460)	
➢ The Security and Guarding Services Industry Authority is established under the "Security and Guarding Services Ordinance" (Laws of Hong Kong, Cap. 460) to regulate the security industry. What are its key functions?	https://www.sb.gov.hk/eng/links/sgsia/index.html
➢ Definitions of "Security Work" and "Security Device"	https://www.sb.gov.hk/eng/links/sgsia/howto-spp.html
➢ Categories of "Security Work"	
➢ Application Procedures of a Security Personnel Permit	
➢ Which category of "Security Work" does the "design of premises security systems" belong to?	
➢ What are the criteria that one must meet when applying for a security personnel permit for providing services in relation to "installation, maintenance and/or repairing of a security device and/or designing (for any particular premises or place) a system	https://www.sb.gov.hk/eng/links/sgsia/pdf/GN%20-%20Criteria%20for%20Security%20Personnel%20Permit%20(Eng).pdf

incorporating a security device"?	
• "Occupiers Liability Ordinance" (Laws of Hong Kong, Cap. 314)	
➢ Purpose of the "Occupiers Liability Ordinance"	https://www.elegislation.gov.hk/hk/cap314!en-zh-Hant-HK
➢ Definition of an "Occupier"	
➢ What is "common duty of care"?	
• "Occupational Safety and Health Ordinance" (Laws of Hong Kong, Cap. 509)	
➢ The purpose of the "Occupational Safety and Health Ordinance"	https://www.labour.gov.hk/eng/legislat/content4.htm
➢ The roles of the duty holders	
➢ Key provisions of "To prevent fire" and "To provide a safe and healthy work environment" under the Occupational safety and Health Regulation	

Topic: "The basic configuration and application of an intrusion detection alarm system" – self-study in respect of the following areas:

Relevant Materials	Website Addresses
"Noise Control Ordinance" (Laws of Hong Kong, Cap 400) Section 13A	https://www.elegislation.gov.hk/hk/cap400?xpid=ID_1438403155940_001
The Police Phased Response for Intruder Alarms	https://www.police.gov.hk/ppp_en/04_crime_matters/cpa/iaiu.html

Topic: "The basic configuration and application of a video recording or CCTV surveillance system" – self-study in respect of the following areas:

Relevant Materials	Website Addresses
Guidance on CCTV Surveillance Practices	https://www.pcpd.org.hk/english/publications/files/CCTVpractices_e.pdf
Privacy Guidelines: Monitoring and Personal Data Privacy at Work - in respect of CCTV monitoring	https://www.pcpd.org.hk/english/data_privacy_law/code_of_practices/files/Monitoring_and_Personal_Data_Privacy_At_Work_revis_Eng.pdf