Unit 5

Security Systems Integration

Learning Outcomes

By the end of this unit the learner will be able to:

- ✓ Discuss the primary benefits of an integrated security management system
- ✓ Understand the various elements that can be connected in an integrated system

Unit 5

Security Systems Integration

1. System integration opportunities

Strategic and successful system integration can be beneficial in a variety of ways. In this unit, we will be taking a closer look at some of the various security systems and safeguards that can be enhanced and improved through effective integration.

1.1. Access control systems

An access control system can be configured to enable or restrict entry to any area of your premises, in accordance with the requirements and general protocols of your business. System integration that incorporates access control can offer the following key benefits:

- Knowing which doors are being opened and closed at any time
- CCTV images linked directly with entry and exit events
- Integration with intruder detection and alarm systems
- Automated door and gate release when a fire is detected

1.2. Time & Attendance (T&A) monitoring

Convenience and efficiency can also be achieved by linking an access control system with a time and attendance monitoring system. In practice, this would result in the badge or token an employee uses to gain access to the premises automatically recording the time and date of their entry, along with their subsequent exit. This can be used monitor attendance, control absence and keep tabs on working hours.

1.3. Visitor Management Systems (VMS)

The same also applies to visitor management systems, which can be implemented and integrated to replace the traditional paper-based system. Visitors are issued with special access cards or tokens, which subsequently track their activities as they enter, move around and eventually exit the premises.

1.4. Lift control

The inclusion of a lift control system can ensure that both workers and visitors alike are barred entry to areas of your business they do not need to access. Detailed information of elevator use is automatically collected and stored.

1.5. CCTV systems

One of the most important of all system integration opportunities, which links CCTV systems with other security installations and safeguards around the workplace. For example, video cameras and recording hardware could be automatically activated when a door or gate is opened or closed, or simply when motion is detected in a specific area.

CCTV systems can also be linked with time and attendance monitoring systems, helping prevent the dishonest practice of employees signing in or out on behalf of others - a practice known as ‘buddy clocking’.

1.6. Intruder alarms systems

An intruder alarm system can also be linked with various other security assets and installations around the premises. For example, if an individual attempts to force entry or bypass an access control system, the intruder alarm system is triggered automatically. Likewise, the triggering of an intruder alarm could automatically disable digital door locks and access readers, in order to secure the area in which the incident was detected.

1.7. Fire systems

It is essential to ensure that fire systems are integrated with other systems, for the health and safety of the workforce and visitors to your premises. For example, it is now commonplace for fire detection and alarm systems to be linked with locking mechanisms, in order to ensure that fire doors around the premises automatically close upon detection of a fire, or when someone triggers a manual fire alarm.

In addition, an effective automated access control system will ensure a detailed and accurate record is available of all persons present on the premises at the time. This will subsequently be important to ensure everyone is accounted for.

There's also the option of linking CCTV cameras with a fire detection system, in order to provide a visual alert of the incident taking place.

1.8. Building Management Systems (BMS)

Building management systems concern various installations around the business, including air conditioning, heating, lighting, ventilation and so on. The idea being that by linking business management systems with other systems, you can ensure such facilities are only activated when necessary. For example, shutting heating, lighting and ventilation down when there is nobody in a specific area.

1.9. Car park management

If you have restricted access car parks around your premises, an effectively integrated security system can automate the process of monitoring the use of your car parks, while at the same time taking note of who is using them. This could include automatically monitoring the number of spaces available, or using cameras to read number plates for automatic entry.

1.10. External perimeter detection

To detect and deter would-be criminals at the outermost perimeter of an organization is to eliminate the threat they would pose if they were to gain entry. This is why an intruder detection system at the perimeter of a business can and should be linked with access control and CCTV systems, in order to bar their entry and ensure they are captured on camera.

2. Integration connection methods

The appropriate integration level and type of integration appropriate for your business will be determined by your own requirements and objectives.

***Note**: British Standard DD CLC/TS 50398:2009 Alarm systems - Combined and integrated alarm systems - General requirements - offers recommendations for interconnected systems.*

2.1. The non-integrated approach

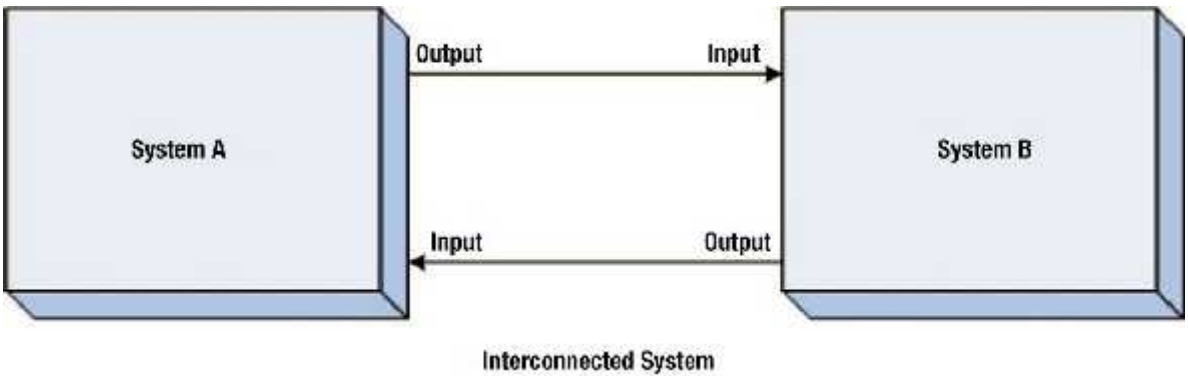
One of the available options when planning integration is to keep every system entirely separate. This may not seem like the most convenient or efficient solution, but may be the *only* option if certain systems are located in different places or different buildings entirely.

2.2. Using a common token

It's becoming the norm for most organisations to operate with several different systems on the same premises, which require an access cards or token to use. In this instance, a card or token used to gain access to the premises could also be used to operate the photocopier, access locked storage to retrieve certain resources and so on.

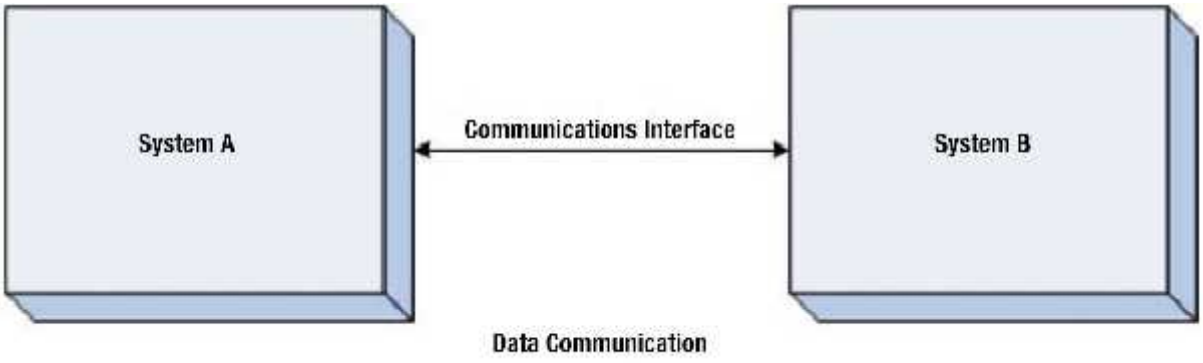
2.3. Interconnected systems

A typical example of an interconnected system would be when an access control system is linked directly with a fire alarm panel. Each of the systems technically runs entirely independent of the other, though are connected in a way that information is exchanged between them as required. When a fire alarm is triggered, the access control system automates the closure of fire doors accordingly.



2.4. Data communication

It is also possible to set up a system wherein data is shared between systems using common data transfer methods like Ethernet over a LAN. Data can be sent in both directions between the connected systems, along with control data. This is a more sophisticated alternative to the classic interconnected system, and is often used to link CCTV systems with access control systems. In the event that an access control event triggers an alert, a data string is passed to the CCTV system to prompt it to automatically turn on a specific camera



and port it to a specific monitor.

2.5. Physical Security Information Management (PSIM)

Physical security information management software is used to integrate a wide variety of non-associated security devices and applications through a unified user interface. Such software is designed to collect, analyse and act upon data collected from security systems around the premises - access control, fire detection, CCTV etc. - and provide clear prompts or alerts when necessary.

2.6. Hybrid systems

There will always be instances where the total integration of systems is impossible or impractical, due to issues concerning infrastructure, expense or compatibility. In such instances, a certain level of integration may be possible - i.e. the integration of some systems, leaving others to operate independently. This is referred to as a hybrid system.

3. Considerations

3.1. Audit trails

Audit trails are of the utmost importance with integrated systems, in order to ensure total accountability if an incident takes place. For example, if somebody attempts to gain forced entry to a restricted area and a guard responds to the prompt, detailed records should be kept (automatically) with regard to when and where the incident took place, who responded to it. What action was taken (if any) and who printed out the subsequent report.

3.2. Data security / encryption

One of the biggest risks associated with establishing and operating integrated systems is that of a data security breach. Anyone who has access to the network could technically gain access to the security system in its entirety, which is why it is important to ensure the messages passed between the different elements of the system are encrypted.

These days, it is considered prudent to conduct regular 'penetration tests' on connected systems such as these. This is where individuals with appropriate knowledge and experience attempt to perform 'soft hacks' on the security system. By assessing the robustness of your security differences from the perspective of a hacker, they're able to pinpoint potential vulnerabilities that may otherwise have been exploited.

It is rarely possible for these kinds of checks to be performed in-house by existing employees, instead calling for professional third party support.

3.3. Data integrity / bandwidth

Another important consideration is that of ensuring there is sufficient bandwidth available for the various elements within the integrated system to send messages and communicate accordingly. The amount of bandwidth required will vary in accordance with the type of data being sent - high-definition video transmission in real-time having far greater bandwidth requirements than the communication of a simple prompt to activate an alarm.

Issues occur when high volumes of data must be communicated at the same time and the system does not have the required resources to handle it. The result of which could be slowdowns or disruptions of the integrated services, which could subsequently leave the organization wide open to a variety of risks.

3.4. LAN / WAN availability

Likewise, it is important to plan carefully for potential network outages. If your integrated system runs solely on a local area network and your LAN goes offline for any reason, your integrated system in its entirety grinds to a halt. This is why an effective integrated system is one that is able to continue running as separate entities, if your primary communication network between these entities ceases functioning. Your integrated system should be set up in a way so that if your LAN or WAN goes down, everything continues to function as normal.

3.5. Recovery from power failure

In a similar vein, the importance of factoring potential power outages into the equation cannot be overstated. There are countless reasons why a business as a whole or any of its systems could be cut off from their primary power source at any time.

While it may not be possible to provide an immediate source of emergency backup power for your integrated systems, it is essential to make sure that all devices and applications associated with the system restart or reboot automatically after a power failure. The more elements within your integrated system you need to restart manually, the greater the disruption and risk to your business.

4. Standards & legislation

When hiring third parties to assist with the development, installation and optimisation of your integrated system, it is essential to ensure they are compliant with all applicable standards and legislation in your jurisdiction. In the United Kingdom, for example, it is advisable to work exclusively with BSIA companies - those who comply with the norms and standards of the British Security Industry Association.

Both British and European standards are available for associated equipment and their constituent parts. DD CLC/TS 50398:2009 (Alarm systems - Combined and integrated alarm systems - General requirements), along with industry specifications (e.g. ONVIF and PSIA), codes of practice and legislation for privacy and data protection.

5. Steps in defining an Integrated Security Management System

The development, implementation and optimisation of an integrated security management system should be viewed as an ongoing process. One that begins by consulting with anyone who is likely to use the system at any level throughout your organization, which will include IT, HR and security personnel among others.

When consulting with third-party contractors and consultants, it's likely you will be introduced to options for system integrations and security enhancements that you didn't even realise existed. The field is evolving at such a pace that what was considered cutting-edge just a couple of years ago may today be considered effective and inappropriate.

Along with figuring out which of your systems could be integrated for enhanced security, accountability and convenience, it is also important to carry out a detailed risk assessment. The primary goal of your system integration project is to mitigate as many of these risks as possible, through the strategic selection of components.

Likewise, the additional risks posed by establishing an integrated security management system (such as hacking, system outages etc.) should also be factored into the equation.

Ultimately, you should be able to reach the conclusion that the integration of various system components will enhance security coverage for your organisation, boost efficiency and reduce long-term costs. If this is not the case, it may not be necessary or advisable to integrate your systems.

During consultations with suppliers and service providers, it is essential to ask for a detailed explanation of the potential benefits of integration, along with which existing elements can and cannot be integrated into the

system. The supplier should be able to clearly and concisely quantify the potential benefits of system integration, providing you with a clear value proposition for the services they are offering.

And again, ensure that the suppliers you work with are members of an appropriate body or authority - such as the British Security Industry Association (BSIA).

Some of the most important considerations to factor in when defining an integrated security management system are as follows:

- The level of integration required and the range of equipment to be integrated
- The scale of the project and the number of systems for integration
- The extent to which employee training and education will be necessary
- The user-friendliness of the proposed integrated system
- The requirement for support and after sales service long-term
- The upfront costs and the ongoing costs of operating the system
- The extent to which the system will generate a quantifiable ROI
- The possible benefits of alternatives to system integration

Further Reading:

- ✓