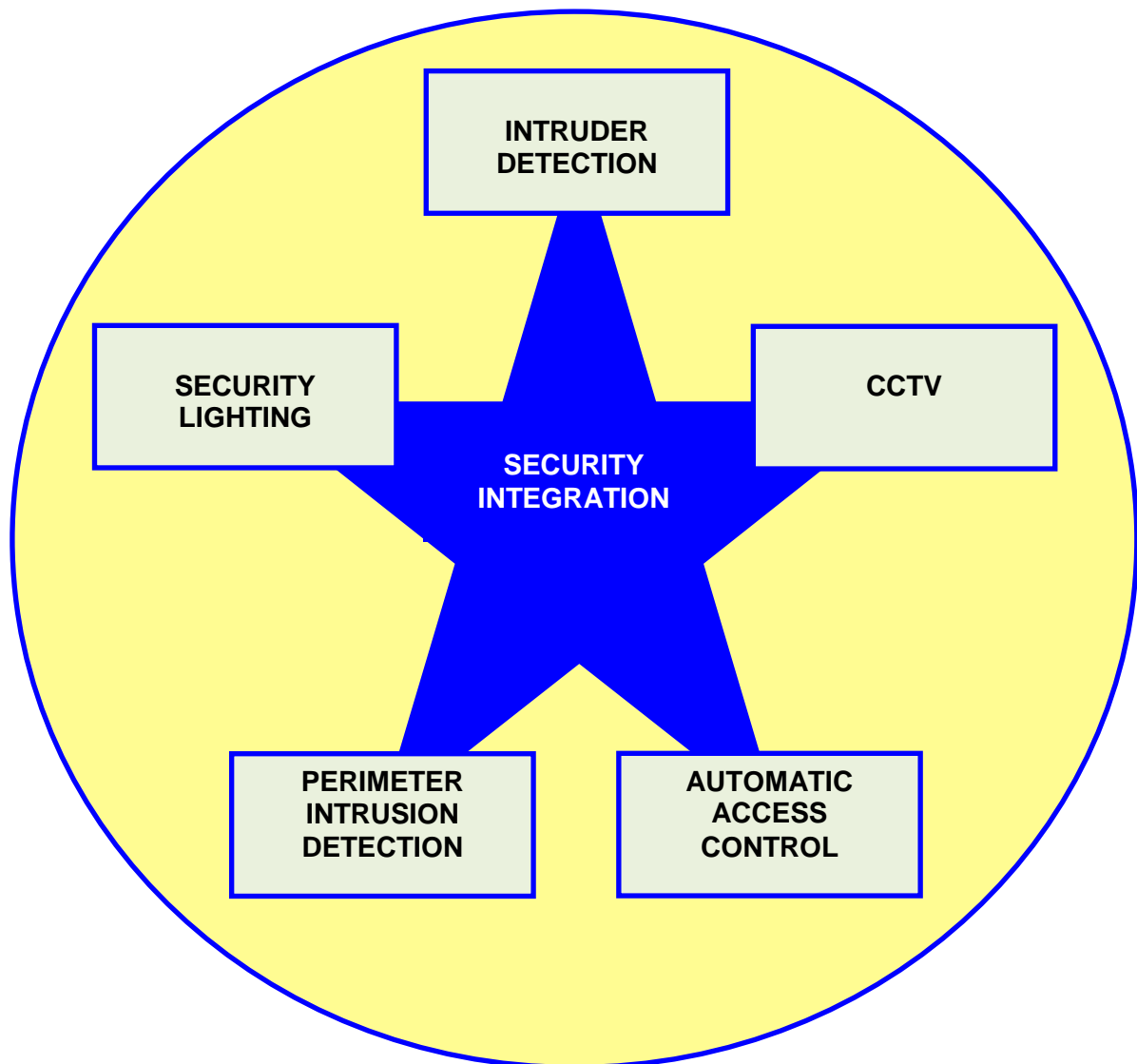


INTEGRATING ELECTRONIC SECURITY MEASURES

MARCH 2012



CPNI GUIDANCE DOCUMENT INTEGRATING ELECTRONIC SECURITY

Document History

Version	Purpose	Originated	Reviewed	Reviewed	Date
0.1	Draft Outline for Comment	J Boothroyd			Dec 09
0.2	Comments included, document reformatted	J Boothroyd	M Smalley		05/01/10
0.3	Draft for Proof Reading	J Boothroyd	M Smalley		17/03/10
0.4	Page numbering revised . Appx clarified	M Smalley			06/04/10
0.5	CPNI Comments added	M Smalley			19/10/11
0.6	Circulated for wider review	M Smalley			24/01/12
1.0	Initial Issue	M Smalley	CM	SK	06/03/12

Any comments or suggestions regarding this document should be directed to:

TDF/22 – Inner Envelope

Central Support – *Outer Envelope*

PO Box 60628

London

SW1P 9HA

Correspondence to this address must be under double cover. The outer envelope should be addressed to: Central Support, PO Box 60628, London SW1P 9HA and not to any individual.

(c) Crown Copyright 2012

The text of this publication may not be reproduced, nor may talks or lectures based on material contained within the document be given, without written consent of DE Security Services Group and Centre for the Protection of the National Infrastructure.

Foreword

This document has been produced by SSG, as part of a programme of research and development funded and directed by CPNI.

Following this guidance does not in itself confer immunity from legal obligations.

Users of this guidance should ensure that they possess the latest issue and all amendments.

Acknowledgements

This document was produced following consultation with members of the CPNI Electronics & Imaging Systems Programme, Detection & Control Working Group. Content is drawn from previous CPNI sponsored studies & discussion documents as well as publicly available material published by manufacturers.

Thanks are also given to those central government as well as wider CNI bodies who were prepared to openly pass on their experiences regarding the integration of security systems

Contents

Forward	3
Acknowledgments	3
Contents	4
Introduction	5
Scope	
Exclusions	
Definition	
Elements	
Justifying Integration	8
Grading / Classification Issues	10
Where Electronic Integration Takes Place	10
The Process of Integration	12
Which Systems ?	13
Design Responsibilities	17
Installation	17
Maintenance	17
Training	18
Hand-over Documentation	19
Glossary	20
Standards and References	23
Appendices	
A Cause and Effect Table	24
B Types of Communication	25
C Security Control Centre Considerations	30
D Security Control Centre Operational Philosophy	33

Introduction

Scope

This document has been prepared to provide users with guidance on the integration of SEAP Graded Security Systems. When creating a protected area, defining the systems to be used is only part of the solution. Equally important is the way in which the systems integrate together both in their deployment and coverage and in their presentation to the user/operator. The design guide covers the technical aspects of integrating systems as indicated in Figure 1.

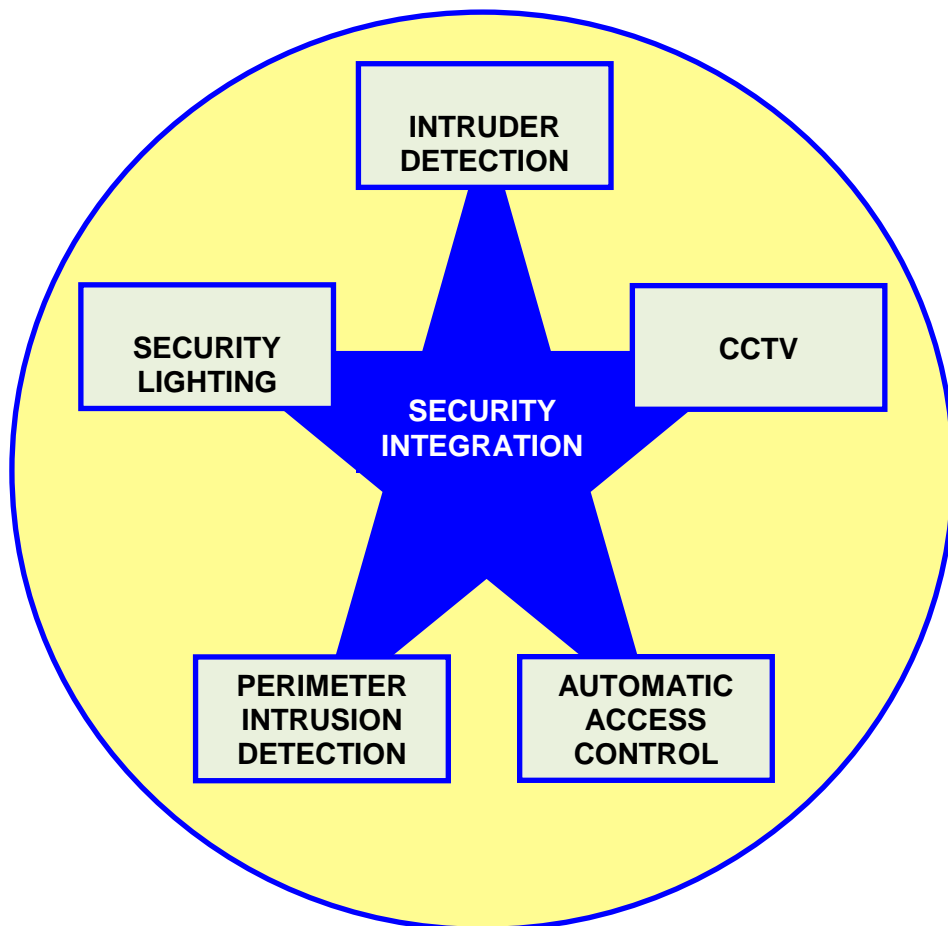


Figure 1. Scope of Integration

Exclusions

Only integration of SECURITY systems are considered. This document does not include fire, building management, gas suppression, or social alarms.

Defining a specific Integrated Security System should follow the guidance given in the CPNI Operational Requirement procedure document. This document highlights areas of the operational Requirement where integration is critical.

This document does not cover the 'sub-system' design elements, for which CPNI guidance is available, but focuses on how elements inter-operate and are managed.

Definition

The term 'Integration' is applied in a number of different ways making it open to misinterpretation. The Oxford Dictionary definition is "the action or process of integrating" which is further detailed in terms of political, economic mathematic and psychology. 'Integration' is a verb and for our purposes, security systems achieve this by communicating between themselves.

A more meaningful term is the pro-noun, 'integrated', the definition, again from the Oxford Dictionary, being given as "with various parts or aspects linked or coordinated".

Systems can be integrated together:

- by virtue of their physical location, for example a gate being installed into a fence line or PIDS zones aligning with CCTV fields of view.
- by their fundamental interaction, for example by illumination from lighting supporting CCTV. Failure to integrate could reduce operational efficiency at night.
- by communicating locally, for example a light being switched on by a detector.
- by the sharing of information, for example two detectors acting together to reduce unwanted alarms.
- by combining the presentation of information provided by the systems, for example by the use of a Security Management System, simplifying operators duties.

Elements

It is important to recognise that different security areas tend to be designed separately, but must work together as an integrated whole. These broad areas are:

- Intruder Alarm Systems, IDS
- Automatic Access Control, AACS
- Closed Circuit Television, CCTV
- Perimeter Intruder Detection Systems, PIDS
- Security Lighting
- Alarm Signalling
- User Interface

Other elements that should also be considered include:

- Resources on site and in the control room.
- Procedures and management.
- Control room facilities: layout; security; space; equipment room; workstations; ergonomics; lighting; power; air-supply; UPS/generators.
- Communications systems: telephone; email; radio.
- Health and Safety measures e.g. fire protection, detection and extinguishing (hydrants etc).
- Resilience/Crisis Management including emergency preparedness and contingency planning
- Legislation.
- Responsibility for the outcome and continuing operation of the integrated system.
- Human resources including assessment of operating staff and response forces.

Justifying Integration

Before commencing a project a clear understanding of the benefits provided by an integrated system should be identified. In some cases integration is a necessity if systems are to function effectively, for example by alignment of PIDS zones with respective camera fields of view to provide visual verification of alarms. The main issue here is determining which element should take precedence in the design and subsequently ensuring that responsibilities are clearly defined. This is particularly important when attempting to resolve faults.

In other situations integration may be undertaken to achieve a particular benefit such as cost savings, for example by investing in technology, could allow a reduction in guard manning levels offering a long-term cost saving to be made.

Often the realisation of one benefit may be at the cost of some other element which may suffer a detrimental effect. This may be in terms of cost, reliability or other increased risk. An example may be where technology is considered to reduce guarding but the resulting system requires a more technically astute person in the control room. This in turn could require additional training for existing operators or renegotiation of contracted guarding services imposing a running-cost increase.

It should also be considered that integration of sub-systems may generate additional information requiring increased manpower both to manage the volume of data and to exploit the capability which was not available with discreet systems.

Providing a common platform for systems can realise cost savings but the risk of introducing a single-point-of-failure or a common mode failure must be considered. Should the control system fail it may be necessary to have the means to operate the sub-systems independently.

Benefits of Integration

Some of the features and benefits that integration may offer include.

- Automation of actions. Following an event / alarm an appropriate camera can be displayed on a specific screen to allow alarms to be verified. The camera could also be automatically directed to a pre-programmed position
- Flexibility of manpower. There is no need to employ multiple dedicated operators at times of low activity
- Provision of a graphical interface for improved site management. The specification must define what is to happen such as whether maps should be zoomable, active icons used for opening gates, selecting a camera or selecting a camera's pre-set position.

- Provision of consolidated audit trails of events and operator actions.
- Improved alarm/event management providing integrated clear instructions, informing specific authorities and providing their contact details. For example a tamper alarm may require a guard response which in turn may need the police or a maintenance engineer to be called.
- Improved management reporting. Statistical analysis of events including, audit guarding responses becomes possible.
- Situational awareness. Provide central report management from many/diverse systems giving a 'big-picture'
- Incident response. Provide enhanced/escalating response on event combinations.
- Provide management functionality For public areas automatically close entrances when a security breach has occurred.
- Improved functionality not achievable through disparate systems.

Drawbacks from Integration

Some of the negative aspects of systems integration can include:

- Increased complexity. This can impact on the overall reliability of the installed system and may require increased skills from both system operators and maintenance / support staff.
- Conflict. It may require a level of co-operation between different suppliers at design, installation, commissioning, maintenance and support. If responsibilities are not clearly defined a 'blame-culture' can ensue when inter-operability issues occur.
- Emergency response. Reductions in manpower can reduce flexibility when dealing with 'multiple-incidents' which may have to be treated sequentially.
- Single point of failure. Single point or common mode failure may be introduced into the overall security system.
- Compromises. Mandated requirements, either from local policy or legislation may require to be addressed and resulting compromises accepted.

NOT PROTECTIVELY MARKED

NOT PROTECTIVELY MARKED

Grading / Classification Issues

The effect of integrating multiple security systems must be undertaken with due consideration to the implications for the security grading of the individual elements. It is not always obvious how a final system will be affected. For example some physical elements are deemed to be cumulative but for electronic systems the resulting system may have to adopt the classification of the lowest graded element.

Due consideration must be taken of security policy documents relative to organisations, particularly where security elements relate to the operating license.

The CPNI Grade of installed systems can be reduced by implementing a poorly designed integration solution.

Where electronic security systems, for example PIDS, IDS, AACS and CCTV are integrated at the security control centre using a security management system it is important that provision is made for the individual systems to still function autonomously in the event the management system fails. This allows the elements to retain their individual classification as there are currently no CPNI Graded security management systems.

Where Electronic Integration Takes Place

Integration can occur at many different levels within a system and in some cases is limited either by the functionality of the sub-systems or the information it is possible to transmit. This in turn may limit the level of integration that is achievable. The primary locations where integration can be undertaken are:

- At device level. This maybe at the periphery of your security network e.g. a movement sensor triggering security lighting.
- At a common node. This maybe at a cabling junction box where the sub-systems happen to come together e.g. an alarm device connected to a multi-door access control interface.
- Centrally in the equipment or control room. Many peripheral alarm devices are often brought back through a networked alarm system and used to select which cameras are displayed on which monitor.
- Remotely at a regional security control centre. This is similar to the central location, except the sub-systems signals may be transmitted from remote sites before integration takes place.

The positive and negative aspects of each option depend on what functionality is desired or required. One of the primary reasons so much importance is given to the Operational Requirement¹ is to ensure the system designer selects systems that are able to offer the functionality the client requires and provides suitable interfaces at the most efficient and cost effective point.

Consider a simple example:

A CCTV system is required to do two things when an alarm is triggered:

- | | |
|------------------|---|
| First Objective | Move a camera to pre-set position |
| Second Objective | Display the camera image on a specific operator's monitor |

Many remote telemetry controllers (often built directly into cameras) have alarm interfaces to trigger the camera to the desired position, which achieves the first objective easily. The second objective, displaying the image may be achieved by the telemetry controllers providing a common alarm output which is triggered whenever any of its alarm inputs are active. This must be routed into the control room and connected to a video matrix to select the camera and monitor.

For telemetry controllers without a common output the alarm input would need to be 'managed' by some other means possibly utilising common networked alarm systems.

Other CCTV systems may only monitor alarms in the control room, when the matrix has sent a message to the camera or dome (as if an operator had commanded the camera to move to a pre-set position manually via their keyboard).

There are merits to each method depending on the overall requirement. Selecting the wrong system at the outset may limit how easy integration may be achieved later. Other issues may also be considered, for example a direct connection at the camera may be more cost effective and reliable but will not provide remote testing or data-logging for audit purposes.

Larger CCTV systems may require more complex solutions, however the move to digital systems with networked interconnections and with Digital or Network Video Recorders offering virtual video matrices means that implementation of integration may become easier in future. This will be at the cost of requiring an up-skilling of both designers and installers who will require additional knowledge to maximise the benefits offered.

The Process of Integration

Integration is a generic term which is generally understood to mean interconnection of sub-systems and offers no clarity of understanding of the actual requirement. Unless expectations are clearly defined, including what is expected from the system and how operators, security staff and users will undertake their duties the final outcome may fall far short of expectations.

The term 'security management system' has a range of interpretations. The client may expect it to encompass management of all alarms on site with site graphical maps and active flashing icons and automatic control of cameras in the vicinity to verify alarm activity and define the most appropriate response, listing actions, contacts and contact details. The security installer may interpret it simply as a graphical interface (GUI) for a digital recorder.

In an ideal situation the security elements are designed and installed together, in practice many systems 'evolve' over time. This can be in response to a number of factors which may include:

- Financial limitations – where funding is available for particular elements or becomes available intermittently.
- Cost savings - where technology is procured to replace human resources.
- Obsolescence - where existing installed equipment becomes obsolete and needs to be replaced.
- Requirements - changes in standards, whether security, environmental or political
- Threat - changes to the perceived threat requires enhancements.
- Operational changes – 'Mission-Creep'.

Before any systems suppliers are approached it is essential that the user defines what systems may need to be integrated and what functionality they require. This should be in the form of an Operational Requirement Level 2 and include all relevant stakeholders, which may include:

- Departmental security advisers/officers
- Senior security staff, including guarding supervisors
- IT department/contractor, to understand any impact on IT/networks (but not offer solutions, at this stage)
- FM contractor or maintenance manager
- HR and possibly unions
- Data protection manager
- CPNI Advisors
- Regulators

The user must review or develop the relevant Level 2 ORs for the sub-systems reflecting their current requirements. The systems which need to be integrated must be identified, together with the level of functionality

required. It is useful to define whether functions are essential or just desirable. Without this guidance integrators may be driven to expensive solutions which may not be cost effective.

For instance a fully automated alarm, graphical interface and CCTV system may be desirable, but a simple graphical alarm display showing the alarm point, most appropriate camera with its' matrix and camera's preset number without automatic control of the cameras could achieve a similar result far more cheaply and minimise service and maintenance costs.

Once a clear understanding of the requirement has been established solution providers should be approached.

Desirable functions considered should be costed separately to allow the user the ability to determine whether they are cost effective.

Before undertaking the tender process all Level 2 ORs should be aligned, whether integration is to be achieved at a simple device level between the sub-systems or incorporate a fully managed security management system. In all cases the Level 2ORs should be supplemented with a 'Cause and Effect' Table - see Appendix A, to capture all functions.

Which Systems ?

Ideally, the decision to integrate should be made at the start of a project to ensure that when preparing the OR system designers can be made aware of the 'overall-picture' and clear responsibilities can be assigned.

It is recognised that in many cases integration into the existing arrangements is required when a new security element is introduced, for example where a PIDS is being installed on an existing fence line with existing CCTV the system should be zoned to match the camera fields of view.

Legacy systems may not have the functionality required for effective integration as for instance, many older PTZ cameras operate very slowly and may not offer pre-positioning or alarm inputs, (in other cases software may need to be upgraded to ensure full support by the manufacturer and with the greater reliance on licensed operating systems this may be expensive). Other manufacturers do not offer Software Development Kits (SDK) required for integration at a data level, as they are unwilling to release their protocols for exploitation by third parties..

There is little point developing an integrated solution around sub-systems that have exceeded or are nearing the end of their expected life.

Open architecture solutions are preferable as they maximise future integration and give flexibility. If proprietary solutions can not be avoided then consideration may be given to keeping any unique development software in escrow. This provides a level of protection in the case support from the manufacturer / developer is lost should they cease to trade but

could be a costly solution that may be of little benefit if obscure or obsolete operating systems are used.

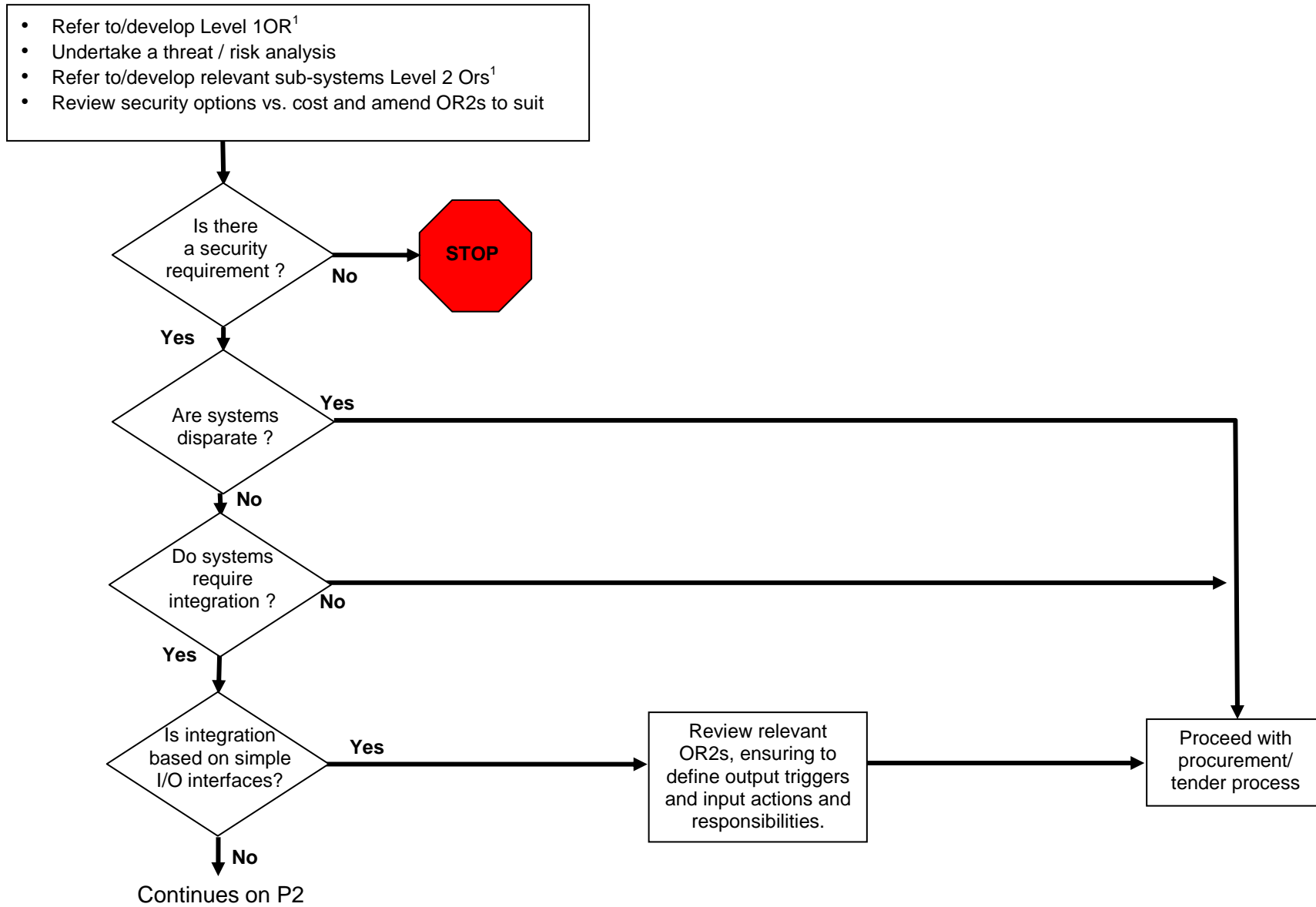
Commonly, integrated systems are designed with an over-reliance on the central security management system which replaces the sub-systems' control method; keypads, mice, joysticks etc. Where systems cannot be operated in isolation they are unable to be operated during any central system failure. Service and maintenance service level agreements must cater for the fastest possible resolution. Reliance on such systems must be entered onto the risk register and accepted at the appropriate organisational level.

Integration should not be considered without relevant and up-to-date Level 2 ORs for each of the sub-systems. The sub-systems should be reviewed and aligned to the ORs as part of the integration exercise.

Any issues arising from the above points may require whole or parts of sub-systems to be replaced.

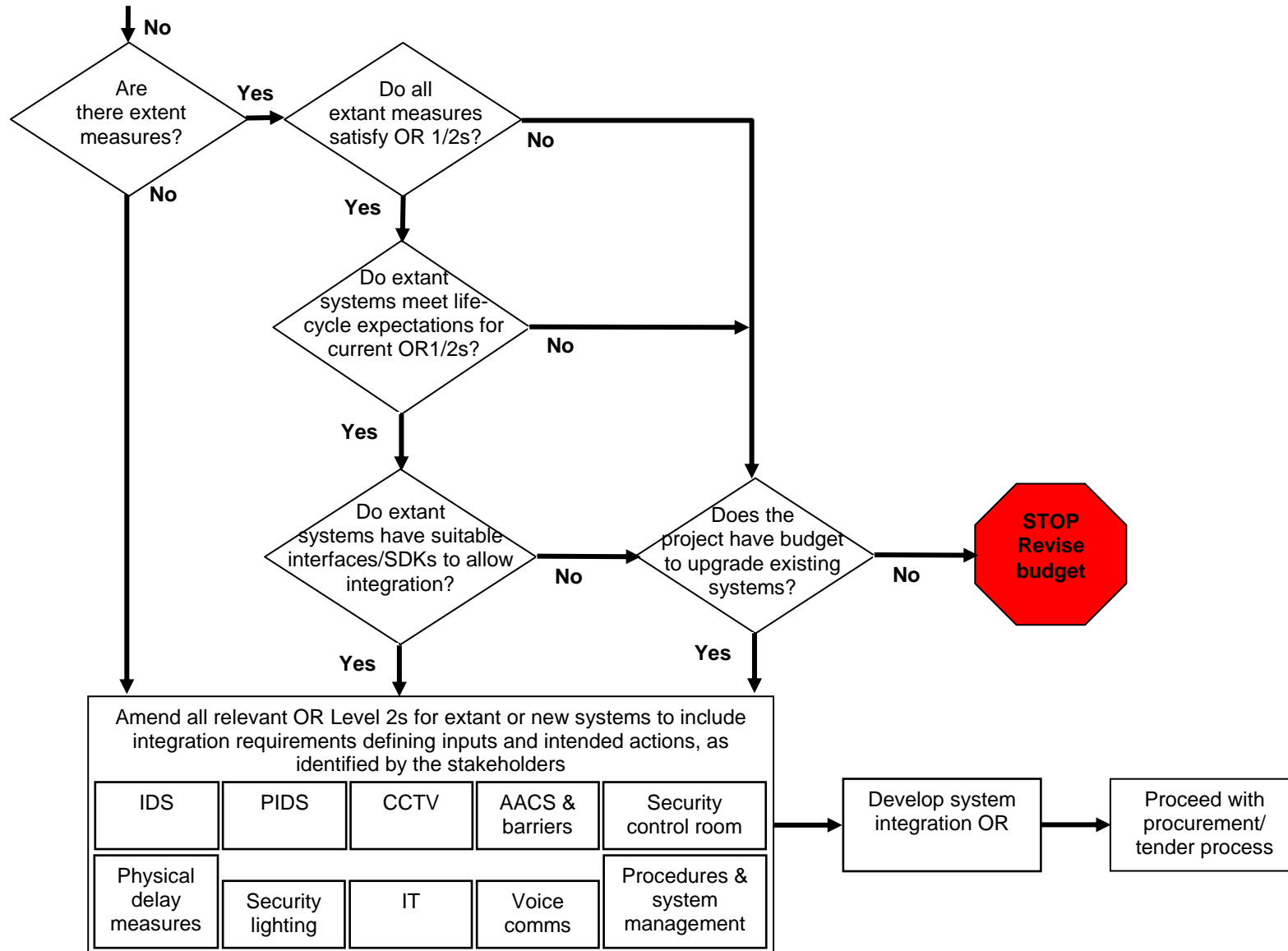
Once the sub-systems have been reviewed an OR Level 2 should be developed for the integrated system (unless performed solely at device level, which should be defined at sub-system Level 2 ORs).

Flow Chart 1 summarises many of these stages offering a decision process which may be followed when considering integrating systems.



Flow Chart 1. Which Systems? (Page 1 of 2)

Not Protectively Marked



Flow Chart 1. Which Systems? (Page 2 of 2)

NOT PROTECTIVELY MARKED

Design Responsibilities

Consideration should be given to employing an independent advisor / designer to avoid the potential vested interests of individual companies responsible for installation / maintenance of sub-systems. Existing installation and maintenance companies as well as the manufacturers should also be approached since they are best placed to advise whether the current systems are suitable, whether components or software would need to be upgraded or replaced in their entirety and may be able to offer more cost effective solutions. Alternative suppliers and manufacturers should also be approached to ensure a variety of solutions are considered.

Involving multiple bodies, either manufacturers or maintainers brings a level of risk. In the event of difficulties there will always be the temptation to blame difficulties on others. This can be addressed by ensuring that responsibilities are clearly defined at the outset, including who is the Prime-Contractor and who are Sub-Contractors.

Installation

Where integration of sub-systems is undertaken, the interface needs and configuration requirements may be covered by secondary training courses only available to business partners of the sub-system manufacturer.

Customised security management systems with proprietary software solutions or new device drivers will invariably need assistance from the sub-system manufacturer, especially where haven't worked with a particular product before. This may require adjustment of software protocols and timing etc. For this reason solutions should only be considered where the contractor is willing to provide field support. Should this be provided from overseas the lead time and expense must be considered.

As part of the hand-over documentation a complete system back-up should be provided on removable media (as well as any for sub-systems). This should be handed to the client along with the acceptance certificate.

Maintenance

The key to successful long term operation of any system lies in the development of an appropriate maintenance regime. Clear responsibilities must be defined and this could require having one appointed contractor who then sub-contracts others for specialist services or skills.

Any electronic system which has a power source WILL fail. It is not a matter of 'if' but 'when'. The failure all too often happens at the most critical time and consequently properly managed service and maintenance arrangements are critical.

Many SMS developers and AACS companies offer remote dial-in support as a method of reducing the time to fix faults. Invariably it is offered for the supplier's / maintainers' benefit as fewer on-call engineers need to be available, which is where the bulk of service agreement costs lie. Many CNI members are unable to accept remote dial-up systems as this could leave their security systems vulnerable to electronic attack.

These points need to be addressed at the outset directly with the SMS developer or the security system installer (often described as integrators) before systems are installed, commissioned or accepted.

Systems (and sub-systems) back-ups should be taken as a matter of routine by the maintainer at the outset of any Preventative Maintenance) visit. This ensures that any changes which may have been made, for example during fault-call-out, will be captured. Also in the event that the maintenance activity itself causes a fault the system can easily be restored back to a working state.

Where remote maintenance is undertaken measures must be in place to ensure only the minimum access is allowed to the central management system.

Training

The scope of the training will be determined by the size and complexity of the installed system. At least two people of each level must be trained on the system (system manager and each level of operator). Training should be undertaken on the actual system and may warrant a temporary workstation to be installed outside the Security Control Centre.

It is recommended training is undertaken in two stages: introductory at hand-over; detailed (back-ups, archives etc) about 6 weeks later. Occasional refresher training should be included in the maintenance package which may be undertaken by engineers during maintenance visits, consist of separate planned sessions by a trainer provided by the company or consist of IT based elements.

Hand-Over Documentation

In addition to the required documentation for each individual sub system being integrated, details for which are contained in the respective guidance documents, it is necessary to document how they are integrated together and the resulting cause and effect. To allow maintenance to be undertaken it is also necessary to detail where responsibilities lie and to indicate where elements may be non-standard.

The following additional hand-over documentation is suggested:

- Overall system schematic indicating all sub-system
- Operating manuals
- Maintenance manuals
- Any recommended preventative maintenance procedures, along with details of who should undertake them.

The following procedures must be included in the hand-over documentation:

- System shut-down.
- System start-up.
- Complete system/s back-up.
- Procedures for archiving and retrieving data.
- Procedures for clearing archive files of unwanted data in line with data protection requirements.
- Routine functional checks

Glossary

AACS	Automated Access Control System.
ARC	Alarm receiving centre. Generally a 3rd party off-site facility to monitor intruder and fire alarms requiring 3rd party keyholder, police or fire brigade response.
Baud rate	Information data rate = bit per second.
Bits	A unit of binary data equal to a value of '1' or '0' (sometimes 'true' or 'false')
BMS	Building Management System. An integrated control system encompassing elements of a buildings' services including lighting, heating and ventilation and security.
bps	Bits per second. Alternative to baud rate (and could be specified as kbps, mbps corresponding to 1,000 or 1,000,000 bits per second)
Byte	A group of usually 8 Bits forming a 'Word'. Lesser known formats are 6 and 7 bit Bytes.
CCTV	Closed Circuit Television
Checksum	An error detection method. All or a standard number of bytes are added and truncated to one byte for checking after receipt. If the second calculation (usually after transmission) doesn't create the same value an error is flagged. This is not a self healing error check and usually causes a re-transmission of the data group.
CRC	Cyclic redundancy check. An alternative error detection method to checksums. Again usually causes a re-transmission of the data group.
Data rate	Speed of data transmission. This could relate to bits, bytes or words.
DEOL	Dual end of line. A method of detecting whether an alarm circuit has been interfered with. It has four states: secure; alarm; open circuit; short circuit.
Dome	A modern high speed pan, tilt and zoom (PTZ) camera station. It's performance usually exceeds that of traditional moving cameras and offers very high speeds, very accurate pre-positioning, built-in telemetry receiver boards with a variety of protocols and offers privacy zone blanking, required as a data protection function.
DPA	Data Protection Act ⁴ .
Hand-shake	A method of allowing or preventing transmission of data between two devices. It prevents data over-load which usually results in

Not Protectively Marked

	inexplicable behaviour.
IDS	Intruder Detection System
I/O	Input/output..
kbps	kilo bits per second – see bps.
mbps	mega bits per second – see bps.
NDA	Non-disclosure agreement. A legal document intended to prevent one company passing on sensitive information about another. Often used where two companies wish to co-operate to produce an integrated solution for a user without the shared data being made public.
NSI	National Security Inspectorate. An independent body that audits electronic security installers, manned guards and ARC and RVRC staff.
OR	Operational requirement. CPNI process for defining the assets, risks, threats (OR Level 1) and sub-system requirements, along with test criteria for the implementation of security systems. These are intended as source documents for the system designers and installers.
Parity	An error detection method. Usually the bits of a byte are counted and a 'parity' bit appended to the byte indicating whether there are an even or odd number of '1'. A byte along with parity and possibly start and stop bits form a 'Word' in serial data links.
PIDS	Perimeter Intrusion Detection Systems
PM	Preventative maintenance. Usually refers to the frequency and work undertaken during regular equipment checks. The 'preventative' indicates the work undertaken to prevent catastrophic failures occurring, but often the measure causes problems. Hence the phrase 'if it isn't broken don't fix it'.
Polling	A communication method used with a 'master' device requesting the status of remote devices all interconnected on a common 'bus' (an electrical data channel). The 'master' asks each remote device in turn what its' status is. In some cases (usually where the status changes) this creates an extended transfer of data between the master and remote device. It is often used to detect if communications channels have failed.
Protocol	A definition of messages sent between two devices. Both devices must use the same protocol – similar to languages in verbal or written communication.
PTZ	Pan, tilt and zoom. Description for camera that can be rotated in three dimensions and zoom to magnify the image.

Not Protectively Marked

Pre-set	A pre-determined orientation and zoom limit for a PTZ camera, ensuring it always points in the same direction. Most modern PTZ cameras and domes can cater for anything from 6-100 or more pre-set positions, usually used for monitoring the most important positions on site. One is usually set as the power-up and time-out default position, such as a vehicle entrance gate. Pre-sets are often used with alarm detectors in integrated systems.
Pre-position	An alternative name for a pre-set.
RVRC	Remote video receiving centre. Similar to ARCs but related to remotely monitoring CCTV systems. Generally systems should be designed to BS8418 Remotely monitored alarm activated CCTV systems, requiring 3rd party keyholder or police response.
SCC	Security Control Centre, the focal point for managing security operations for a building or site. On some sites this will be the Guardroom.
SDK	Software development kit. This defines the protocol messages, electrical interface and data transfer rate for allowing a 3 rd party system to control or accept data from one system to the other.
SEOL	Single end of line. Similar to DEOL except it can only detect three states: secure; alarm; tamper.
SLA	Service Level Agreement. A document (contract?) defining the performance of a service company. It is only a specification of performance, which could be poor but often interpreted as a measure of quality.
SMS	Security management system. Generic description of the overarching system managing the security sub-systems. Many AACS system offer many of the facilities.
SQL	Or 'sequel'. A database interrogation protocol. Commonly used for integration purposes at a database level. It allows an authorised software package to request specific data (based on search criteria) from a database. Often used for producing custom reports or integrating AACS personnel records with the HR system (very dangerous).
SSAIB	An alternate security auditor to NSI, but generally focusing on electronic security installer.
System integrator	Usually an installer with the skills to interconnect diverse systems.
TZ	An AACS term defining a weekly (usually) time pattern used to enable users to gain access at only designated times, or to inhibit alarms during the working day.
VPN	Virtual private network. A way of using LAN, WAN or internet connections securely.

Not Protectively Marked

NOT PROTECTIVELY MARKED

Standards and References

- 1) CPNI Guide to preparing Operational Requirements
- 2) BS 5979 - Code of Practice for Remote Centres Receiving Signals from Security Systems
- 3) BS EN 50132 Alarm Systems – CCTV surveillance systems
- 4) Data Protection Act
- 5) BS 7807 Code of practice for design, installation and servicing of integrated systems incorporating fire detection and alarms and/or other security systems for buildings
- 6) Disability Discrimination Act

APPENDIX A

CAUSE AND EFFECT TABLE

The table below is a sample of a 'cause and effect' summary for basic I/O (closing contact) integration. The completed table should accompany the sub-systems Operational Requirements.

ITEM	SOURCE SYSTEM	TRIGGER DESCRIPTION	INTERFACE	DESTINATION SYSTEM	ACTIONS	RESET MECHANISM	PRIORITY
1.1	Building 'N' alarm system	General alarm		Internal	Trigger sounders for 10 mins	Automatic/keypad	Regulatory
1.2					Trigger strobe	Local keypad	Regulatory
1.3			I/O	Master alarm panel	Annunciate alarm on keypad	Master keypad	Essential
1.4				Local dome 'X'	Go to preset 'Y'	Time-out/operator control	High
2.1	Master alarm panel	Building 'N' general alarm	I/O	Central matrix	Select ch 'X' on monitor 'Z'	Operator control	High

APPENDIX B

TYPES OF COMMUNICATION - Pros and Cons

There are four common types of communication employed which are indicated generically in Figure 1. The pros and cons of each are described below.

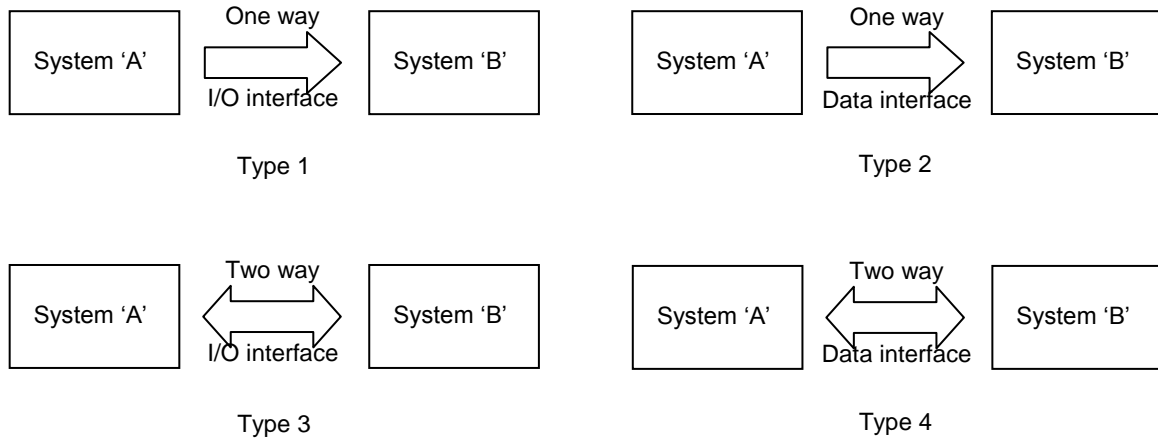


Figure 1. Generic Types of Integration

1. One-way only by simple opening/closing contact (I/O interface).
2. One-way only by data.
3. Two-way by simple opening/closing contact (I/O interface)
4. Two-way by data.

I/O or Closing Contact Interfaces

An I/O or closing contact interface, whether one or two way, is the most common interface between different systems and is virtually universally supported. It is often the chosen method of inter-connecting disparate equipment by system integrators as integration can be achieved without any input from either manufacturer, assuming the integrator is familiar with both systems. The method does not require any development, just a little cabling and configuration time. It is therefore the cheapest solution and as there is no development involved has minimum affect on the installation program.

By providing a reverse link outputs from System 'B' could be monitored by System 'A' achieving a two way interface. For instance many alarm systems offer functions such as arming, dis-arming and isolation by closing contact method. This may reduce the classification or grade of the alarm.

A variation of a closing contact interface which is preferable in most cases is monitored inputs. System 'A' still provides an opening or closing contact to indicate an event has occurred. System 'B' however uses a resistor bridge to indicate whether the circuit is: secure; insecure; open circuit; or closed circuit. In most interfaces single, SEOL, or dual, DEOL, resistors

Not Protectively Marked

are used (some interfaces use more resistors to indicate even more line states). Dual end of line resistors should be used by preference and they should be installed in the connector at System 'A's end of the cable.

Monitored inputs are commonly used in alarm systems to prevent an intruder simply cutting a cable or looping a contact out, before breaking in. In an integrated system it is required simply to indicate a cable has accidentally, inadvertently or deliberately been disconnected, preventing System 'B' operating as expected.

Integration at device or closing contact level should be defined in the sub-systems ORs and is not considered in any greater detail in this document. The ORs should however define what should happen when an event is triggered and would benefit from a 'cause and effect' summary.

Data Interfaces

Data interfaces are usually more involved than closing contacts and normally requires some form of custom software to be developed and tested, irrespective which of the methods are used. Many specialist system integration companies retain a suite of drivers for systems they have worked with before. These are usually made available at a cost, which is far less than developing a new interface, which be expensive.

Where timescales are tight inadequate testing maybe undertaken which may come to light during commissioning at the end of a project or during operation. This can add significant delays and require further input from the software developer, who may have to produce a suite of bug-fixes taking months to resolve.

It is often declared the true development time for any software (or hardware) is actually twice as long as the developer originally estimated. So allow a lot of extra time in the program and expect some on-site difficulties where a new interface has to be developed.

Some of the more common data interfaces are discussed below.

Simple Printer Interface

In its simplest form a data interface may require the printer port from System 'A' to be monitored by System 'B'. The printer messages are usually filtered to strip off unwanted messages, such as operator triggered events e.g. user access level changed, and then delimited to collect time and date, device identity and the type of event. This will usually require the manufacturer of System 'B' to write some custom software, unless they have integrated with System 'A' before. This type of interface by its nature is one way (although printers can produce status messages, such as out-of-paper, these are unlikely to be of any benefit for controlling System 'A').

The delimited fields can then be used for any desired requirement, such

Not Protectively Marked

as:

- Simply recorded for integrating into event archive for future reporting purposes.
- Used in system status displays for management or diagnostic purposes.
- Indicate a site graphic showing an alarm.
- Used in conjunction with other events, such as alarms, to only draw attention of the operator to critical events e.g. reduce false alarms by ensuring at least two events from disparate systems occur, such as a movement sensor and a CCTV analytics alarm. In more sophisticated systems many events can be linked using if-then-else logic.

Whereas printer interfaces are simple to implement and reduce development costs they should be used with care as they cannot indicate if the interface has failed or the cable has simply been disconnected.

Serial Interface

At the electrical level this type of interface is identical to the printer interface but rather than simply monitoring a printer message the manufacturer of System 'A' would offer a software development kit (or SDK). The kit usually comprises:

- A specification of the electrical interfaces. This is usually one of: RS232; RS422; or, RS485 and the type of hand-shake used, which maybe software, hardware or in the case of poorly managed interfaces, none. Hand-shaking is required to prevent one system sending out multiple messages before the other is ready to deal with them.
- A definition of the word format and data rate. Examples are: 9600 bps, 8 bit, no parity; 1200 baud, 7N.
- The interface protocol. This is a description of the message sent or received, how the message must be constructed with identity words, user defined parameters e.g. camera channel number or pre-set number and any data integrity checks. Data integrity checks should be adopted by well defined protocols to ensure adverse effects are not produced simply because a message has been corrupted by some form of electrical interference. Examples are: checksum, CRC (cyclic redundancy check) and even parity. Where data integrity has not been retained the protocol must use acknowledge messages or alternatively System 'B' can send a re-send request. Each system will need to track repeat messages so multiple events are not triggered simply because of corruption.
- Test equipment. This is essential to ensure the software developer has fully interpreted the specification correctly. For example many CCTV systems are integrated by replacing an operator's keyboard with the computer interface. Keyboard interfaces are extremely simple, have no hand-shake functions or data integrity checks. Keyboards do not usually require them as an operator would simply key the command again if the system does not do what they want. Timing is also critical. Electronic interfaces however can

Not Protectively Marked

stream many commands together far too quickly for the other system to respond. This is a common fault overlooked by a developer simply obeying the written specification. Indicators for the CCTV system may be: dome or PTZ cameras jumping to pre-sets randomly; dome or PTZ cameras going into set-up mode; dome or PTZ cameras continually spinning or driven against their stops.

Such interfaces are usually two way if only to allow System 'B' to send an acknowledgement or 'please repeat' message back to System 'A'. This provides a level of robustness which is desirable to cater for data corruption. If this is all that the reverse messaging achieves then it is unlikely to affect the grading or classification of System 'A'. Where control messages, such as isolate or setting an alarm are sent then undoubtedly the classification will be affected and maybe reduced to 0.

Integration at this level usually requires the system integrator and/or the manufacturer of System 'B' to sign a non-disclosure agreement (or NDA). NDAs are legal documents and can be contentious especially, as often is the case, they are one sided. Again this can lead to project delays.

Robust interfaces involving two way communication and some type of polling should allow System 'B' to warn of a failed link.

TCP/IP

Many off-the-shelf integrated systems use TCP/IP at the core of integration. In terms of development many of the issues raised under Serial Interfaces apply, such as SDKs and NDAs. The basic difference is at the electrical level where a TCP/IP rather than serial interface applies. This particularly applies where CCTV images are being routed from one system to the other, which is difficult to achieve using a slow serial interface.

Complications may arise due to network issues, especially if this is done over a corporate network to take advantage of existing remote WAN connections, for example monitoring remote building alarms and CCTV systems from a regional headquarters building. Where this is being considered the IT department or contractor will certainly need to be consulted at the operational requirement stage.

Integration via TCP/IP may also have other issues at a different level. If you consider integrating your access control system with an HR database this is often undertaken at an SQL database level. Best practice dictates that where both databases reside on the same network they are tightly locked down to prevent unauthorized changes to the database. (Stories abound where access databases are poorly secured and staff find themselves locked out of their buildings.)

Care has to be taken by specialists on each database application to only open database access to specific applications and perhaps at specific times. Where possible exhaustive tests should be conducted between the

Not Protectively Marked

systems to ensure inappropriate changes are not made. Tests should preferably be undertaken on test copies of the databases so they cannot affect day-to-day operations.

Integration using TCP/IP will certainly affect the CPNI Grading of any system.

APPENDIX C

Security Control Centre Considerations

To get maximum benefit from a SCC, operators will require adequate time to deal with an incident. For example, traditionally the operator simply needed to acknowledge alarms at a keypad. However if you wish to audit operator performance the operator will need to acknowledge an alarm, review the incident and often add a cause code message before the alarm can be cleared. If redundancy has been included then the alarm may also need to be cleared at the keypad.

Regarding incident codes, these should be preferably chosen from a pre-defined list, for consistency, which should be short enough to display without scrolling. A user defined entry option should also be provided but not as the default.

This all takes time and therefore additional manpower may be required in the SCC at peak times.

Even a small SCC managing a single site may have 2 x operators and a supervisor. They shall all need access to the SMS and sub-system controls. A review of requirements may determine the need for a larger SCC with a separate equipment room addressing issues such as noise pollution, temperature control associated with acceptable working environments as well as assisting maintenance and service personnel.

The cost of a custom SMS can be expensive therefore it is essential that functional requirements are prioritised. The SMS developer should provide an option list with costs, allowing users to select the system to suit their initial and on-going support budget. As with any security system element it will have an expected life. Unless identified otherwise, plan to replace the systems in their entirety within 7-10 years.

Note that simply removing one roving guard and replacing them with an additional operator in the SCC may drive up costs - the SCC operator will need to be able to manage the equipment - this is far more demanding than simply walking a site, checking windows and doors are locked etc.

SSC operators' skills need to be constantly reviewed. This should then be applied to existing staff, identifying if they require additional training, even providing replacement staff which may require renegotiation of manned guarding contract.

All management workstations should be restricted in functionality to the minimum required.

Systems must offer multiple operator levels. CPNI have produced a 'Password Tree' which indicates the responsibilities which can be assigned to different users. The key to achieving security is to ensure that only those rights which are needed are given to any user and no 'Super-Users' are created who may abuse their authority.

Users must log-in with individual password. Card / proximity / biometric

Not Protectively Marked

log-in maybe considered. Three levels would be a minimum :

- **Installer** - full functionality, but should be pre-authorised by the system manager no access to employee data, hardware configuration only.
- **System Manager** - all functionality other than essential configuration settings including isolating parts of the system.
- **Operator** - there maybe sub-levels of operator, some with acknowledge only and others with acknowledge, low level set-up (perhaps user/password) and review.

For security reasons it is recommended that Auto-log-off be implemented after a pre-defined period of inactivity.

All user activity should be logged for later incident analysis. Full recording of operators screen in real-time would be preferable and easily selectable on incident review reports etc from a manager's screen outside the SCC for privacy purposes. This feature could also be useful for post-event training etc. Consideration of DPA must be made if PC is used for admin purposes, also it is important that operators are aware they may be monitored and that they give their consent.

Suitable network-security measures should be adopted, as outlined in CPNI document 'Physical Protection over IP Networks'

When employing disabled persons .the disabilities of operators must be taken into account where they could impact on the integration process. Many SMS's struggle for screen space and this could hinder staff with visual impairment. Where touch-screens are operators with limb and movement disorders may struggle to cope (this may equally apply to systems employing keyboards and mice). Where alternative controls are provided consideration must be given to their cleaning, calibration and maintenance.

Use of colours maybe beneficial to highlight critical and non-critical events and highlight different alarm/event priorities. The colour scheme defined in EN 60073 should be adopted unless demanded by other standards.

Sound can be useful to bring attention to critical alarms. However a high number of false alarm or incorrect prioritisation of non critical high frequency events will lead to the audible alarm being ignored or disabled locally.

Choice of display screens, particularly with CCTV systems will involve considering the options for displaying both live and replay information which may demand multiple screens. For alarm information, (PA, IDS, PIDS, AACS alarms) blank screen or always visible will need to be decided.

Operator controls, joystick, mouse or touch screen, must be chosen. It may be preferable to retain a separate joystick as these sometimes prove easier to use than on-screen mimics which can clutter screens with controls/icons etc. Screen controls may also introduce latency in the control room graphics & active icon controls.

Not Protectively Marked

Consideration should be given to setting up a controller within a SCC with greater privileges to allowing them to take over control of a CCTV system from a guard on a remote site. This is particularly the case with moves toward minimum levels of manning (where a single guard is employed who may need to take a comfort break). Primacy should reside with the remote guard who will almost always have the greatest situational awareness.

Functionality can include any of the following:

- Camera selection
- Camera pre-set
- Gate release / operation
- Operation of lighting

Interactive information for the operator may be provided which could include :

- Site plans
- Site instructions
- Contact details – police / response force
- Contact details - service and maintenance
- System set-up
- AACS employee records
- AACS reports
- status displays
- Standard Operating Procedures

Whereas it maybe considered beneficial to display detailed alarm procedures on-screen this maybe detrimental if other essential information is 'lost' e.g. a live video feed or the primary alarm list. Whereas overlaying a pop-up window over a site graphic may be acceptable.

Design of the SMS must not require operators to switch screen modes for critical applications. For instance the primary alarm/event window should always be available. This may or may not be supplemented with audible warnings. This may add to noise pollution and cause operators to lose concentration at a critical time.

To ensure correct management of the system all sub-systems should be time synchronised for efficient management, audit and evidential purposes.

The system design should allow for additional capacity. This capacity should be stated for each element of the system at the outset of the project.

Where provision is made to 'fall-back' to the subsystems in the event of failure of the management system, regular testing of the operators ability to operate these subsystems must be undertaken.

APPENDIX D

Security Control Centre Operational Philosophy

An SCC operational philosophy summary should be included in any site's standing instructions along with the latest OR Level 1, all current OR Level 2s aligned to the current installation (ORs will need to be amended to reflect any changes imposed through the design and installation phases of a project e.g. reduction in recording rate due to cost). These will assist during any audit or security review to fully understand the intent of the current systems.

The SCC operational philosophy summary should cover:

- Primary function of SCC and security staff.
- SCC facilities, workspace and number of workstations and their specific function.
- Any provision for equipment, including environmental, power etc.
- Summarise system capacities i.e.
 - Alarm systems
 - Alarm points
 - CCTV cameras
 - AACCS controlled doors
 - PIDS circuits
 - Workstations of each type, with locations.
- Number of operators/supervisors across a typical working week.
- Tasks covered by operators/supervisors - don't simply detail security tasks also include:
 - Who backs up the systems and how often
 - Archiving and subsequent deletion of CCTV footage
 - Patrols
 - Manual CCTV patrols
 - Mail services
 - Delivery duties
 - Monitoring of safety & BMS systems
 - Fire alarm drills and fire warden duties
 - Stop and search
 - Escort duties e.g. contractors; key management
 - Disposal services e.g. secure shredding
 - First aid
 - Liaison tasks e.g. police authorities
 - Visitor management
 - Telephone duties.

Not Protectively Marked

- Advise any special functions and management duties e.g. securing out-of-hours events or leasing of facilities. Highlight any significant impact on security resources.
- Overview of alarm/event handling expectations. Outline essential tasks and 'nice-to-haves'.
- Describe external communication systems e.g. telephone, radio, LAN/WAN, public address.
- Any scheduled major building or refurbishment works.
- Any planned upgrade or extension to the security systems, with schedule.
- Timescale constraints.
- Restrictions to site for installation/configuration works. Induction and/or safety procedures, permits to work etc.
- Risk assessment covering SCC locations. Offer alternative options if not completely satisfied to cover: low risk of fire, explosion, flooding, vandalism and exposure to hazard; located in basement or upper floor - not ground floor; operations are not visible from outside e.g. overlooked from adjacent buildings; fire ratings; physically robust to determined attack; air-supply; UPS/generator back-up; air-lock entry.
- If installed are panic/hold-up alarms independently monitored.
- Any alternative back-up facility in the event of a catastrophe.
- Major incident facilities, procedures, management centre (differs from SCC), comms and feeds from SCC.

The above is often included as a summary of requirements in tender documents, preceding the detailed sub-systems technical specifications.