

# The Security Business

Author: Alistair Freeborn, Sales Manager - High Security and Commercial - Quadrant Security Group

***The separate disciplines that can make up a security system are Closed Circuit Television (CCTV), Access Control Systems (ACS), Intruder Detection Systems (IDS), Perimeter Intruder Detection Systems (PIDS). Whilst some installations may only need one discipline to fulfil the security requirement, an increasing number will now involve one or more technology, which presents opportunities to increase system effectiveness by interlinking (or integrating) the systems.***

All electronic security systems are designed to present information to a system operator to enable him/her to act on that information. This information will range from annunciation of alarm events to display of video images, however with increased adoption of electronic security than ever before, it is too easy to flood operators with information to the point of making the systems ineffective. It is critical that the operator is considered as a key part of the system, and attention should be given to operator work-loads, level of training and manning, procedures, and control room design during the technical design process.

The term 'integration' will be used to identify connection of systems from different disciplines, however some may argue that 'integrated' and 'interconnected' systems are distinct. The difference between fully integrated 'Common Platform systems' and 'interconnected' systems will be expanded upon, however they will be considered together here under the 'integrated' title.

Intelligent buildings take integration a step further and can encompass not only security systems, but Fire, Heating, Ventilation, Air Conditioning (HVAC) and Building Management Systems (BMS). The systems can work together, reacting to personnel activity and environmental conditions, often using common platforms and communications infrastructure.



## Operational Requirement & Specification

As with all security systems the design starting point should be the operational requirement. The requirement should drive the use of technology rather than the other way round. In particular, the response of the system to an event must be clearly defined, including the required timing.

An example would be:

The system shall present the text and graphic image on the workstation to the operator within 0.5s of the event occurring, and the CCTV image of the event should be displayed within 1s of event. In the case of pan and tilt cameras the camera should reach the preset position within 2s of the alarm event. A human target of 1.6m should be displayed as a minimum 10% screen height at all positions.

The recording of the event shall start within .5s of the alarm event and finish when the alarm is cleared by the operator.

Note that it is of little use if the system response time is beyond what is required by the Operational Requirement, i.e. the image is presented after the target has potentially left the scene.

Equally the process of all actions, sequences of events and keystrokes should be understood as part of the design process in order to gain best value from the integration. It is important that all 'what if' scenarios are explored to ensure the system meets the requirement. Changes made after the system has been commissioned, particularly if any custom software has been written, may be expensive.

### Increased Effectiveness

Integrating systems can offer a number of benefits to the user of the system such as greater effectiveness, reduced manning, less control room space and reductions in equipment, infrastructure and maintenance costs.

Effectiveness of systems is greatly improved by providing information to operators when they need it, and in a way that increases the value of the people and systems involved and in the best cases, by giving only the information actually required..

### CCTV/ Alarms Integration

A typical integration is linking of CCTV response to alarm or other sensor activations. Rather than separately presenting alarm event information to an operator, who then has to select and direct a camera to view the cause of event, the alarm information is fed directly to the CCTV system. For instance, a perimeter alarm is triggered and the CCTV system presents the operator automatically with the images associated with the event, which may be a fixed camera image, or a pan, tilt and zoom (PTZ) camera that is directed automatically to view the scene via pre-programmed presets. This not only tells the operator that there is an event, but allows him/her to verify the cause, and therefore react in the appropriate manner. This basic integration between alarm event and CCTV greatly increases the effectiveness of the alarm system through rapid verification. This applies equally to the CCTV system by only presenting the operator with images when he/she needs them, i.e. when there is an event or activity to view. Some video monitors are sometimes designated as 'blank screen', only having video images routed to them when there is an image associated with an alarm event. Equally the alarm event can also trigger the recording system to record only the event-associated information and images, or perhaps record events at higher resolution or frame rates when an event occurs, which both saves recording capacity and increases detail.

Extensive systems with large numbers of alarm points and associated CCTV cameras need to be carefully managed, as simultaneous events can flood the system. The potential number of events in relation to the number of operators required to manage and respond to them must be considered. For example the number of events in a major shopping complex will be considerably more than at a largely unmanned, high security data centre.



Not only do the number of operators need to be considered, but also how and what type of events are presented to them, or indeed perhaps just logged for analysis later.

## The Operator Interface

In the more complex systems the alarms handling and CCTV triggering process should be handled by a dedicated alarm management computer (or access control system acting as the alarm management system), which will often be aided by site graphics maps displayed on a PC screen, usually called the Graphical User Interface (GUI). The programming of a series of data tables ensures that the correct camera at the right preset is presented to the right operator simultaneously with the alarm event and recorded at the right time. Updating the data tables when cameras are added or the geographical layout is changed is clearly a vital, and often neglected, requirement. Some CCTV systems contain all the programming data and others are stored within the alarms management control system computer. The viewed alarm 'stack' list should present alarms to the operator in sequence, either by time or by importance. Some systems with multiple operators define which operator will deal with which event, or allocate the work on a 'next available basis'.

All alarm sources may be interfaced or integrated to the CCTV system via contact closure, RS 232 interface or in some solutions, via a software interface between two different computer programmes within a common host computer.

Such sources may be:

- Intruder Alarm Systems: internal alarm events
- Access Control Systems alarm events ( i.e. door forced, left open, invalid card presentation etc).
- Perimeter Alarm Systems: verification of external alarm events which are most susceptible to false alarms caused by weather, animal activity etc.
- Fire Systems
- Shop alert systems
- Critical plant alarms

All can be displayed, identified, and controlled from the same workstation, irrespective of source, in a common format. Not only can such systems display information from a variety of sources but they can create 'output actions', such as directing cameras to preset, opening doors, operating recorders etc.

More advanced GUI systems can communicate with and control, not only security systems but other technologies such as intercoms, help points, telephone and radio systems and locking systems, thus giving operators a workstation with a common "look and feel" for all the systems they operate.

## Control Room Design

Fundamental to an integrated system is the control room design, which must be sized to take into account the workload, the number of workstations and CCTV monitors, and the number of operators, supervisors etc. Workload may vary and the number of operators at peak times may well be different to quiet hours.

Systems integration using multifunctional workstations can help manage the variable workloads, by routing particular tasks to specific operators, or sharing activities to next available operators. More complex tasks can be routed to senior officers, while the more straightforward go to less senior personnel. (Example: a door left open alert could be dealt with by a less senior officer, whereas a Personal Attack alarm from the Chief Executive may be handled by the duty supervisor). If workloads reduce in the silent hours, all categories or types of event can be routed to the duty officer. This routing using a multifunctional workstation is far more effective than making the operator move to multiple control positions or different pieces of equipment.

Current control room design is favouring the 'workstation' approach, where operators control alarm events, access control and video via flat screen monitors, while the wall of 'conventional' monitors has been replaced by computerised multi-screen displays, often using advanced back-projection technology, plasma screens or high quality video projectors.



These systems offer very flexible display formats, from multi-screen video with perhaps a large central control or spot image, or a mix of graphics maps, text and images. The format of display can be programmed to accommodate different scenarios, workloads and system manning.

Some installations may not need a control room at all. For example, many access control systems now feature the ability to present the video image relating to an event on the same workstation screen as well as the conventional graphic map and text display.

This gives the operator all that is required in many installations, and may negate the need for larger separate video monitors. However this will be driven by the operational requirements and what is actually being viewed, and the detail required. The same interface may also control the recording functions, and allow rapid playback of video footage matched with the alarm events.

The 'control room' may now be anywhere with a network point, perhaps remote from the site in question either at a central, company owned facility, or at a third party monitoring centre.

## Event logging

All events, images and operator actions can be logged to hard disk for later analysis post event, or can be used to audit the system or operator performance (i.e. the number alarms logged as 'false' or caused by 'bad weather'). In this way, the overall system can be refined using data collected over a period of time to identify technical issues that need to be corrected or further training requirements for operators.

## Common Platforms

The above describes the system as a series of subsystems, Alarm source, CCTV matrix, CCTV recorder (digital generally), Access Control System and Alarm Management System. A number of these features are, however, now commonly being combined into single products, or Common Platforms.

For instance a digital recording system may now include the video switching, alarms presentation, graphic maps, and interfaces to the alarm devices all in one 'package'.

Access control systems are also becoming central to integrating systems, not only managing the administrative and control functions of door access and personnel records, but also the alarm management functions and integration with CCTV switching and/or recording systems.

The display of video cameos of personnel (from the cardholder database on the access control server) and live video images from cameras associated with key entrance points allows the operator to compare the cardholder record with the actual person entering. The same operator workstation may also control the display of CCTV images relating to alarm events, and replay of images from a digital recording system.

The benefit of a Common Platform is in the reduction in hardware and special software, and therefore also costs. The down-side may be an almost complete reliance on one system to display and control alarm events, and to display and record images.

## System redundancy

While the technology is available to combine disciplines onto a common platform, consideration must be given to the effects on security of a single point failure.

Combined, single platform solutions are perhaps the most vulnerable, and have the potential to leave the user without their electronic security, and increases dependency on the manufacturer/ supplier to affect a rapid fix.

Dual processor or redundant servers, and multi-path or resilient networks may need to be considered to counter such issues.

Where separate systems are managed by a common control system (or GUI) with no Common Platform, loss of security from failure of the control system can be mitigated by a fall-back to operating the individual systems.



## Common Communications Infrastructure

Most security systems installed prior to the last decade have used different methods to collect data from devices in the field. This is partly because the individual disciplines have been considered or contracted singly, for resilience or cost. eg:

- CCTV- Point to point co-axial cable or fibre optic
- Access Control- RS 485 cabling to control panels either copper data cable or fibre optics, point to point or daisy chain.
- Intruder Alarm- Bespoke bus, multiple panels connected by RS 485 either copper data cable or fibre optics, point to point.

This excludes the potential to collect data from BMS, HVAC and Fire.

The adoption of internet protocol data (TCPIP) by an increasing number of security equipment manufacturers means that the corporate or dedicated security IT network may be used to communicate with remote devices, creating a common communications infrastructure.

CCTV systems now can use 'IP' cameras and network video recorders (NVRs) which may incorporate centralised video data storage. Access control systems commonly use network connectable control panels and now some incorporate network connectable card readers.

Subject to the resilience issues previously mentioned, most security systems and building control systems can use a common infrastructure. This can not only save costs in terms of infrastructure installation, but allows corporate IT departments to manage this data transmission on behalf of the security user.

However, at the time of writing, Fire and NACOSS Intruder alarms systems need their own dedicated networks, not only for the differing technical requirements, but to meet the agreed system standards laid down by their respective certifications.

## Intelligent Buildings

As with pure security systems, operator workloads must be considered, and also whether it is appropriate for security staff to manage or control systems other than Security and Fire. There is no technical reason, however, why building systems which traditionally control HVAC and lighting should not use displays and workstations in common with the security system.

Integration between the systems can enable control of HVAC and lighting by taking data from the access control system, which is after all controlling and monitoring occupancy. Again, this integration may be by serial link between systems to a common display, or by multiple applications working on the same workstation linked within the software application.

