White Paper
Site Security

Christophe Rémond, *Thales Security Systems*

SUPERVISED & INTEGRATED PHYSICAL SECURITY

This document is intended to explain the different steps that must be taken in order for a client to attain "integrated and supervised security" as we define it. Providing this level of security for people and material objects requires the use of many technical elements, including software and hardware. The operators of the system will not aware of or be concerned with the complexity of these components: they should fully focus on their job: security. The approach used is one of "layering" solutions, thereby offering a choice in the modules selected as part of a definitive, complete and efficient system architecture.

Key words: Electronic security, access control, video surveillance, intruder control, supervision, integration, operator desk, synthesis, layered architecture, analysis, Intranet.

1. INTRODUCTION

The problem. Providing physical security – defined as the protection of persons, goods and intellectual property – at one or several sites is a vast and complex task for the company assuming the responsibility. Major capital expenditures are required in electronic systems covering the following areas:

- Access control (persons), including card systems, biometrics, turnstiles, trap doors, management of parking areas, visitors management, etc.)
- Detection of intruders, including area surveillance sensors, volumetric sensors, high security perimeter protection, infra-red barriers, etc.,
- Video surveillance, including cameras, 360-degree surveillance domes, switching matrixes, IP video, digital recording, image analysis, privacy zone protection, etc.

There is a serious risk that such systems can be superposed without any interaction or consistency among them. To be sure, personnel access points are well-screened and troublesome visitors kept out, intruder alarms sound where security personnel can hear them and 360° color surveillance systems allow the security staff to monitor all that is going on in a given area. But, in very large areas where large numbers of people are present, security personnel are quickly bombarded with information from multiple sources as they carry out their daily duties. The multiplicity of monitoring screens serves to scatter their attention. Despite years of experience, it can also prove difficult for them to instantly make the connection between the area in which an alarm has gone off and the corresponding video surveillance screens. By the same token, when a serious event such as a theft or intrusion takes place, it may prove impossible to integrate information coming from systems that have been installed at different times in the past and that are not synchronised and indeed incompatible. Analysis of events becomes a highly inefficient process.

Possible Solutions. One way of tackling these problems is to find a single supplier capable of installing the full range of security equipment, configuration and operational software needed to meet the security objectives chosen. That of course creates a dependency on that supplier, and hence a proprietary technology approach that often fails to evolve with trends.

The alternative is to choose the right specialist in each of the major categories of security equipment, taking care that the company's products are open to other non-proprietary software in order to permit real-time interaction with the environment. The requirements in this area are a function of the kind of service the component provides,

e.g., the type of communications protocol employed by a card reader. Assembly of such components in a single, coherent system makes it possible to supply security operators with a relevant and fully synthesised system. This approach also makes it possible to provide security services with a decision-aid mechanism based on comprehensive control panels, thereby permitting the security managers to fully use the equipment they have chosen.

In this approach, computers and software play a major role in the electronic security system.

2. BASIC ARCHITECTURE

This White paper proposes a "functional levels" approach to building a coherent security system. If the integrated, supervised security system is made up of several sub-systems, each specialised in terms of its functions, it should also be possible to deploy each of them independently of the others.

A security sub-system — whether it is an access control, an alarm system or a video surveillance system — is usually made up of two distinct levels:

- Level 1, or Field Level (i.e., the entire physical site, in all three dimensions), includes on-site material such as access control equipment, intrusion detectors and set off alarm systems, cameras and switching matrixes, digital recorders, etc.
- Level 2 or Command and Control Level, contains the operation elements needed by the system's operators and administrators. While some systems are still without graphic user interface (keyboards only, of varying degrees of sophistication), large sites usually include a sub-system such as a server linked to several graphics PC work stations on Windows. This type of sub-system is usually an open one, making it possible to integrate it into a broader security system.

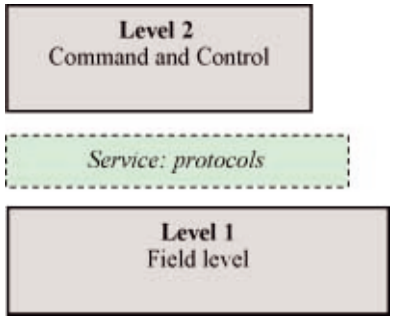

Fig. 1: Basic architecture of a security sub-system

Integration of levels 1 and 2 is possible thanks to a "service" layer placed between them. This includes information transfer from field level and dispatch of action messages top down. This link between levels 1 and 2 utilises industrial protocols, either proprietary or standardised. One example of a standardised protocol is TEDI/LCR, used in France to communicate with highway security equipment; another is ModBus, often used to send intrusion alarms. One of the most widely used in networks at present is TCP/ IP.

An integrated, supervised security system is made up of four levels, beginning with those described above. These are illustrated below, and include:

- Level 1: Field level
- Level 2: Command and control
- Level 3: Supervision
- Level 4: Decision making

Levels 1 and 2 are security sub-systems.

The key purpose of Level 3, Supervision, is to create a single operating interface with all user functions in place of separate interfaces for each sub-system. It is based on computer equipment.

Level 4, Decision making, consists of a set of computers that make it possible to do reporting tasks or a posteriori security data analysis, including intuitive multi-dimensional analysis of historical records, video archives retrieval on the basis of a single photograph, etc.

Throughout, the links between each level (except for the link between Levels 1 and 2) **(see figure 2, page 3)** are provided by a service layer, using computer protocols (usually TCP/IP) to ensure communication between these services. As noted below, these service levels must be taken into account in order to guarantee independence between levels. Protocol converters may also be used to provide these services.

3. SUPERVISION MEANS CONTROL OF THE SYSTEM

Level 3, Supervision, is the most visible level for operators because it provides them with a single control panel that enables them to bring together all the information they need, thus avoiding a multiplicity of control panels (one for each sub-system) within the control rooms. In this way, security personnel can concentrate on a single panel that synthesises all information from all sub-systems and likewise permits controlling all sub-systems from a single point.

The Supervision level includes the following data-pro-

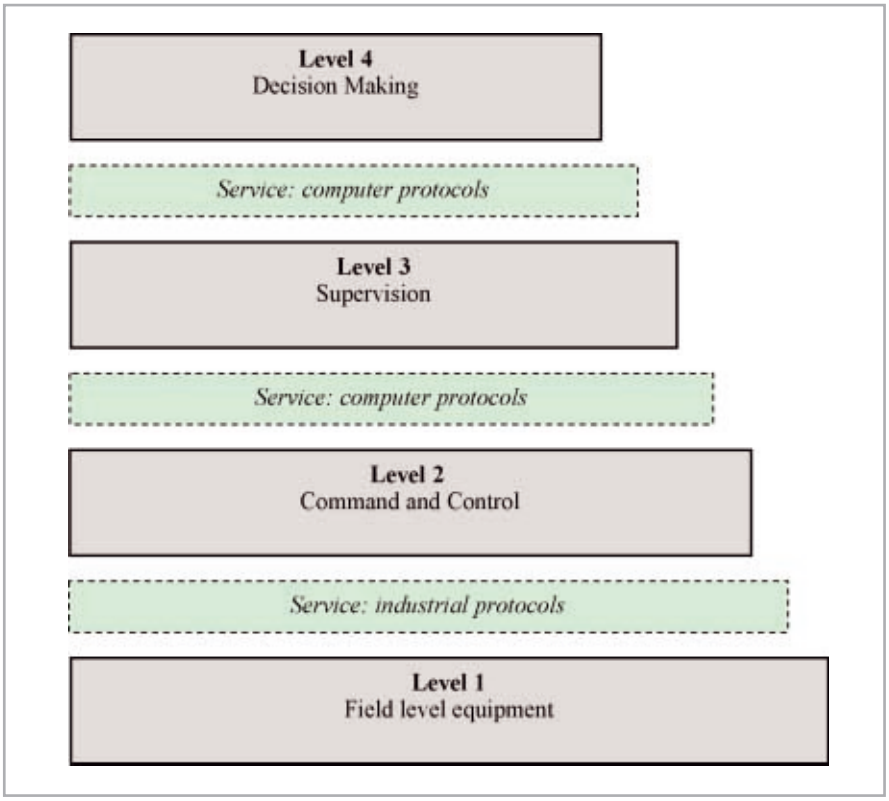

Fig. 2 : Basic architecture of an integrated security system

cessing equipment:

- A server that collects and synthesises information in real time and relays the operator's commands to the security sub-systems. This server has a database;
- Graphics User workstations (PCs using Windows) providing control of the system.

As a minimum, this type of supervision system should provide the operator with the following capacities:

- A complete alarm log recording the nature of each alarm (access control, intruders, video-detected motion, etc.) sound and voice messages when alarm events occur. This log file makes it possible to follow-up with the full process (alarm localisation on a map, handling and acknowledgement);
- A capacity to replay directly and instantaneously the video record of the incident for efficient doubt raising. If an alarm is configured to trigger a digital video recording, this record can later be recalled by simply pointing to the event on the log list. The video recording system includes a pre-alarm feature that starts recording 5 to 30 seconds (depending on the system) before the alarm event, hence providing a visual record of the situation that led to the alarm. This sequence is displayed directly on the operator's workstation screen. Recording of the alarm sequence is ended either through a timer or automatically after the operator has acknowledged the alarm;
- Multimedia instructions (either text or voice) to guide the operator in handling the location where the alarm appeared), enabling the security officer to reach that location with all needed information in hand;
- A set of graphic maps illustrating the site under surveillance. The organisation, breakdown and capacity to navigate in these plans have to be adapted to the organisational requirements of each operator. For instance, being able to integrate architect's plans in AutoCAD format directly into the system is a highly appreciated feature;
- A set of animated color icons representing field equipment such as access points, alarm locations, cameras, etc. These icons are interactive, so they can be designated and activated for opening an access point, deactivating or activating a sensor or other device, triggering the video recorders, etc. by simply using the PC mouse;
- The mouse can also be used to control the video surveillance cameras and 360° domes: selection, orientation (zoom, pan/tilt), presets, presets sequences, manual recording. The control of the mobile cameras is done using a virtual joystick on the operator's screen;
- A system for controlling the access points: opening or

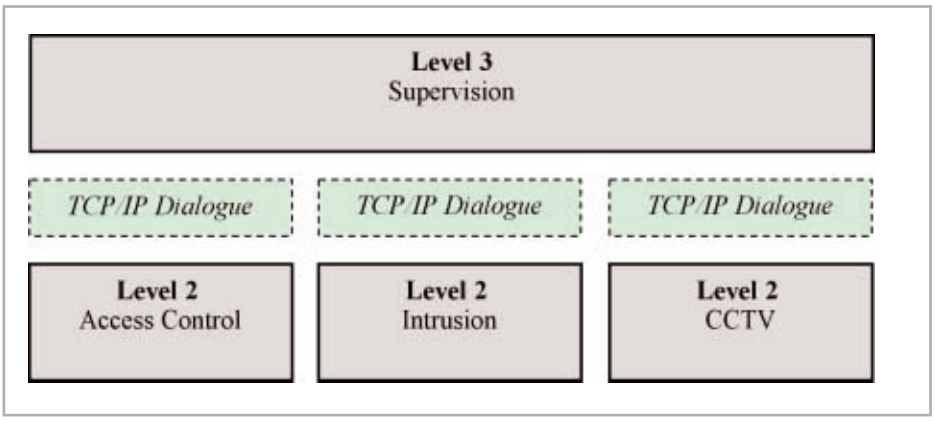

Fig. 3: Integration of 2 and 3

closing an access door or a set of access points, multi-criteria search in the access cards database with the possibility of viewing employees' photos and printing out identity forms;

- Control of user profiles, making it possible to limit fully or partially the functions that can be accessed by each operator;
- Breaking down the site into distinct surveillance areas if there are several security control rooms, as in the case of very large sites. In this case, operators are assigned to a specific area depending on their user profile;
- Synthesis panel to provide real-time data such as the number of alarms per sub-system broken down by area, the number of personnel on site, etc.

The server of the supervision system compiles a database including all events in the last several months, divided into three categories:

- Alarm events on all sub-systems;
- Access control data (enabling tracing of all valid and refused entries);
- Operators' actions (connection, disconnection, commands to field equipment, etc.)

This data remains accessible on line for several months and can thereafter be stored. It can also generate reports with simple filtering criteria selected by using simple graphic symbols and without requiring the knowledge of the SQL language.

Archives of video records can be consulted from a dedicated workstation.

The server of the supervision system should enable combined actions between sub-systems. This is generally carried out directly (wired) between the intrusion and video surveillance sub-systems, for example to trigger automatic operation of a camera when an intrusion alarm is activated. Alternatively, it is also helpful to use software to set up simple master-slave arrangements for temporary periods (during service periods for instance) without having to modify the wired connections. This function makes it possible to set-up simple controls (commands to field equipment to inhibit an access or to select a camera) that are triggered by events such as an access denied, intrusion detection, etc. These controls can also be programmed to be operative only for certain periods during a day or a week.

Integration between the supervision system at Level 3 and the security sub-systems at level 2 is done on Ethernet network using TCP/IP. This means that the sub-systems at level 2 need to have the necessary interface capabilities. The chart shows the service levels specific to each sub-system at level 2.

It is important to note that each sub-system can be operated independently, particularly when used in a layered context. For example, if control keyboards are available at level 2, they remain in active mode and can even be used by some operators at the same time as supervisor at level 3.

The configuration of each security sub-system is still managed at level 2. The parameters of each sub-system are imported to the supervisor's database at level 3, in order to avoid double entry of data and assure that all parameters are consistent with each other. The set-up at level 3 is therefore limited to the configuration of the following specific elements:

- Declaration of the operators and definition of their rights,
- Definition of the priorities among all alarm in order to have a single scale of priorities for all,
- Definition of the instructions for each type of alarm,
- Positioning the graphic icons for equipment on the graphic maps of the site.

The server of the supervision system has to be highly available and allow an automatic and transparent shift to a backup system in case of failure (cluster-type machine).

4. DEPLOYMENT OF SECURITY SUB-SYSTEMS

There is a wide variety of security sub-systems (levels 1 and 2) on the market. As noted above, the fundamental requirement for an integrated system is to include the communication protocols allowing these sub-systems to access level 3.

The following discussion aims at showing how the choice of the service layer between level 2 (Command and Control) and level 1 (field equipment) can have a real influence on the choice of electronic security components of each sub-system.

4.1. Access control

There are many efficient access control technologies. Access control systems usually have a central server that houses the database for the cards. The access points monitored are controlled at field level by LTUs (Local Treatment Unit), which manage the card readers and other elements of access control (locks, barriers, etc.). The LTUs can be linked to the server through serial lines or the standard Ethernet TCP/IP network.

Generally, the choice of LTUs will limit the choice of the type of card reader, depending on the specifications of the LTU supplier. This makes it worthwhile to develop junction boxes or "protocol converters," which allow the system to overstep the limitations inherent in the LTUs to broaden the range of card and reader technologies that may be integrated into the security system. This is all the more important to permit the access control sub-system to be renovated without having to modify all the readers already in place. In such cases, the concept of service layers for protocol links between levels 1 and 2 shows its full value.

It should also be possible to integrate biometrics identification technologies such as fingerprint, facial or iris recognition, etc. into the sub-system via the LTUs. These possibilities may vary, however, depending on whether they are used simply to authenticate the identity of the badge holder ("1 for 1 verification") or if they are intended to replace the card in the access control ("1 for n verification").

4.2. Intruder detection

Whatever type of field equipment used to detect an intruder (volumetric sensors, infrared devices, shock detectors, perimeter surveillance, etc.), the key question is to collect digital inputs from the intrusion detection system. There should also be a way of detecting possible system sabotage — cutting links, for example.

There are many products available on the market to provide the service level protocol links between levels 1 and 2. One example is use of the ModBus protocol on the Ethernet. Some even include an Internet web mini-server allowing data to be called up through any Internet navigator.

4.3. Video surveillance

Analog video surveillance sub-systems usually include cameras, one or several switching matrixes and specific keyboards for controlling the cameras. Larger systems need more sophisticated operator interfaces. These man-machine interfaces usually use Windows graphics and show the location of the cameras on the site map. In an environment with multiple operating stations, it is worthwhile to install video server software to ensure linkage among all operator consoles, on the one hand, and all field equipment (cameras, matrixes, digital recorders, video-based motion detectors, etc.) on the other. This approach makes it possible dissociate the choice of the matrix (and its communications protocol) from the choice of cameras (and their remote control protocol). In this case, all protocol-type links with field level elements are done by software in the video server. It is then possible to overcome the limitations on camera protocols set by a given matrix builder. The same applies to digital recorders, which can then be totally integrated with and controlled by the video server. Here again, the service level providing the protocol link between levels 1 and 2 allows each level to be independent.

Finally, in the case of very large-scale sites that must manage several matrixes, it also becomes easy to design a "partitioning" into independent surveillance areas. Inter-matrix links then permit video flows to move from one area to another, so that any camera can be picked up on any monitor screen on the site.

Another advantage of designing a software video server is that it provides easier access to digital video via Ethernet TCP/IP. In this configuration, the network becomes the matrix and camera switching commands are simply a matter of establishing an Ethernet (TCP/IP) connection between an encoder and decoder of video flows.

5. INTEGRATING THE COMPANY REFERENCE DATABASE

Access control systems are specific to the type of data they handle. Besides the field level (level 1 – secure access) elements, these sub-systems also have to include a personnel database. In a large company, there is a clear need to unify personnel data in a single database. This in turn means that access control sub-systems have to interface with the company's human resources management. Software for automatic update of card databases can then be provided. Connections between the databases are then possible through the import of data files or, more directly, by direct access to the personnel registries of the company if maintained on LDAP standard. Data on new employees is spread with ease and multiple entries of identity data are avoided.

Visitor management is a sensitive issue as it affects both site security (and protection of industrial information) and the corporate image. This fact underlines the importance of an integrated visitor management system, which can provide "active" visitor cards for access control. These cards give visitors access to limited and controlled areas within the site (whether alone or accompanied). Access control history files permit tracing a specific card. The system also makes it possible to compile visitor statistics, such as number of visitors per day, average visitor time on site, etc., and is an indispensable tool for efficient assignment of access personnel such as guards and hostesses.

One way of facilitating reception of visitors is a pre-registration system making it possible to prepare visitor cards the day before the visit. This limits the reception process to declare the time of arrival and activating the card. To be efficient, the pre-registration system has to be simple and available to all company personnel. Pre-registration systems can also automate more sensitive visits to protected sites (defence sectors, etc.) in permitting an approval step, controlled by the chief site security officer. Intranet-type technologies make such a paper-free system possible. In addition, management of the resources needed for meetings, such as reserving conference rooms, video projectors, teleconferencing, meal service, etc. can also be fully integrated into the same Intranet capacity.

Intranet methods are also useful for managing personnel access rights. On large sites, there are usually procedures and forms (often paper forms) for treating requests to modify the site access rights of an individual employee, as for example in the case of a new job assignment. These procedures are based on a hierarchical circuit of approvals that terminates on the desk of the person in charge of access control, who executes the approved change. Systems based on a company Intranet make it possible to manage such procedures from beginning to end through a computerised workflow, with the appropriate direct activation of access control.

6. THE DECISION MAKING LEVEL

Beyond daily management of the system, site security managers need very sophisticated tools to determine whether and how the systems and organisations set-up meet their intended goals. Two distinct issues are involved:

- Analysis of the performance of the electronic systems,
- Dissemination of security information and strategies to all persons concerned

The computer equipment/software for addressing these issues make up level 4 of the integrated and supervised security system.

A posteriori analysis of electronic systems is based essentially on all the history data compiled and synthesised by supervision at level 4. While research of the "tracks" of a past event, such as an intrusion or theft, is also largely based on such data, security managers are above all interested in searching the data for "abnormal" situations that can easily be overlooked without a very detailed examination of data, since some situations do not necessarily set off alarms at the Supervision level. One such would be repeated use of a lost card for entry attempts during successive nights.

In effect, a *multidimensional* analysis is required — one that permits cross-comparison of different types of data displayed on different axis, e.g. cards, access points data and time data. This type of analysis can provide more pertinent results while allowing user-friendly presentations adapted to people who are not computer experts. Many kinds of research can be carried out spontaneously, without pre-requests.

As concerns the dissemination of information, security is an important part in the drafting and implementation of in-house rules and procedures. Security procedures have a substantial effect on personnel organisation and daily activities. Examples would be receiving foreign visitors or taking delivery of packages, receiving telephone calls or bomb alerts. The key point in security is often "Show who you are, and you'll be recognised as such". The Intranet is the best way to make security procedures a living reality and to keep employees aware as they evolve. The full body of information on the subject can be available in a standard office data system (Word files, PowerPoint presentations, video, sound, etc.). Access to the documentation server is managed on the basis of user profiles, breaking down accessible data by personnel category. The

documentation is also organised in terms of professional activities. There is an "administrative" module that allows the editors to add new documents on-line once approved by the person in charge.

The text above has shown that there are many elements in levels 2 to 4 of a layered security system that can take good advantage of Intranet technology. This makes it advantageous to bring all these elements together under a real "security portal," which can reveal different functionalities depending on user categories and access rights. In effect, the degree of access is based on the employee's job requirements or on the degree to which carrying his/her daily task linked the physical security of the company. This is of course a vision of integrated security based on the needs of each participant in the system, and is hence more vertical as opposed to the horizontal layering system described above.

7. SUMMARY

This document provides a rapid survey of the issues and elements involved in an integrated, supervised physical security system. The proposed approach, with four distinct levels, each with a service layer providing an interface with the next one up or down, makes it possible for each level to be independent of the other. This conception should be a guide to the questions asked and the choices made by managers responsible for physical security who seek better integration of their physical security systems. Software components have been shown to occupy an increasingly important place in these systems. It is evident that it is the advances in software programming since the mid-1990s — of which the most spectacular of course concern the web and the intranet — that make it possible to construct such systems with an increasingly large choice of the physical components to be used. Future advances in information technology will take it possible to simplify further the work of security operators in the years to come. One of these is clearly wireless technology, which might be applied at all levels. Others that might be cited are the growing importance of digital video or the development of multi-service cards.