

# Planning an Enterprise System Integration

*A clear plan of attack can lead to smooth security design and implementation*

by David G. Aggleton, CPP, CSC

**B**efore starting any endeavor, not just a security system design project, we must understand the rationale or reason and the objective or goal before we can implement any solutions — the solutions should be dependent on the goals, not vice-versa.

For security projects, we need to focus on the specific assets that require protection, the threats against those assets and the probability of those threats occurring. Armed with this basic information, we can study existing security measures to identify gaps or vulnerabilities. Only then do the objectives of our potential solutions become clear.



## Phase I: Planning

Before we can move to the design phase, we need to identify any design constraints that may be imposed on the project. In the past, these have included considerations related to organizational culture, the image that it projects to the public, the need to perform regular business functions and the cost budget. In the past, we also relied on our own dedicated communications infrastructure but today, for any enterprise-level system design, we must integrate with the corporate network and hurdle the constraints imposed by the information technology department.

The IT constraints may not be insignificant, and failure to involve the IT gurus early in the planning process has derailed more than one project. IT will want investigate any hardware connected to its network; in addition to servers and workstations, which they may insist on providing. IT will also want to look at IP cameras, networkable digital video recorder, IP-addressable door control units and networked access control field panels.

IT's policy may require field testing of any device they have never seen before — maybe for 6 months. Unless addressed early, this could have a big impact on the project schedule. If this leans you in the direction of dedicated security networks, be aware that the IT department's responsibilities may cover any and all networks installed in the facility. To minimize any possible headaches, the best approach is to get the IT department involved very early in the project and include someone on your team who not only understands the security devices and their connectivity, but also can speak the same language as the IT folks.

## Phase II: Design

With the goals of the system and all constraints completely understood, we can concentrate on the second phase of the project, design. Depending on the size and complexity of the project, there are a bunch of other design disciplines with whom the security design needs to be coordinated. On new construction or major renovation projects, the architect may schedule weekly design and planning meetings to discuss coordination issues. Examples of such issues include:

With the architect: the look, colors and mounting methods of exposed security devices; space allocation for monitoring and control locations; and space for security equipment such as field panels and power supplies. While the later has traditionally been mounted on plywood backboards in utility closets, newer designs look at rack-mounting this equipment in a raised-floor data center environment.

With the electrical engineer: main voltage power requirements for security equipment; rough-in for security devices (back and junction boxes, conduit, etc.); and fire alarm system interfaces for life safety code compliance.

With the telecom engineer and/or the end-user's IT staff: structured cabling; network switches; data center racks; and IP addresses.

Planning for the procurement of the security systems, the third phase, should be addressed early in the design phase because the method of procurement will dictate the form of the design documentation. For example, an invitation for bid (IFB) will require specifications with complete details of every component. For a request for proposal (RFP) the level of design detail is not as stringent since this format assumes more of a partnership where the security contractors' experience and input are requested in their response.

While IFBs may be publicly bid, RFPs are distributed to a more select group of security contractors. Pre-qualification of those on the list should be planned well before the construction documents are ready to release. Also plan to include with the bid documents a description of the response format, so proposals are easier to analyze and compare.

## Phase III: Implementation

The last phase is the implementation of the systems and their integration. Planning the installation steps is very important regardless of size of the construction site. For example, before a card reader can be mounted on the wall next to a door, studs are installed, then rough-in electrical (back-box and stub-up conduit), followed by dry-wall, taping, spackling and painting.

The larger the system and the more complex the integration, the more planning is required for the commissioning and testing tasks. Items to include on the list are credential provisioning, interactions between systems, redundancy and failure mode (power and communications) testing, and as-built documentation.

Project planning tools, such as Microsoft Project, are invaluable in forcing the project manager to consider all of the tasks that are needed to be performed and the order, duration and interrelationship of each. Smooth and problem-free design and implementation happens with effective, thoughtful planning. **ST&D**

*David G. Aggleton, CPP, CSC, is president and principal consultant at Aggleton & Associates, a security systems design and consulting firm. He has been planning and designing security systems for more than 30 years. He can be reached at [dave.aggleton@aggleton.com](mailto:dave.aggleton@aggleton.com).*