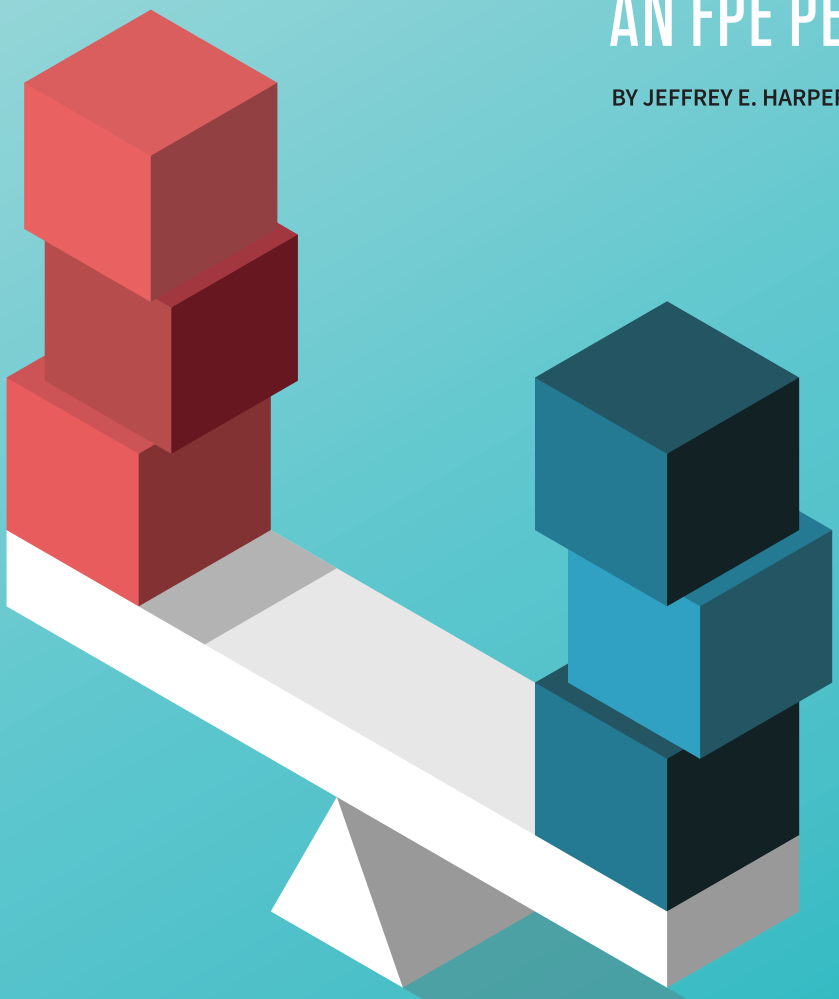
THE EVOLVING Fire/Security RELATIONSHIP

AN FPE PERSPECTIVE

BY JEFFREY E. HARPER, PE, FSFPE



WHETHER YOU REALIZE IT OR NOT, protecting people, property, and assets is the overarching objective in fire protection engineering and life safety. As fire protection engineers, we aim to achieve these objectives on every project. Quite interestingly, those are the same overarching objectives guiding professionals planning physical security for the built environment.

After 25 years of working as an FPE, I had the fortunate opportunity to work closely with some outstanding security professionals to begin to understand physical security. Like many FPEs, my original perspective was that they want to lock the doors we need open for egress…and how is that supposed to work? Quite often, it does not, and then the design team is scrambling to secure administrative relief or perhaps an equivalency. When this occurs, usually there was insufficient consideration given to the coordination of life safety and security during the early design phases. Unfortunately, this scenario prevalently plays out today many times over.

It is fascinating that there are a number of commonalities that exist between fire safety and security. Fire safety practitioners would better serve our ultimate clients, the general public, if we learn and understand some basic principles of security. At the very least, especially early in design, wearing security tinted glasses while offering our fire safety counsel on projects can help to minimize the almost inevitable coordination problems down the road when the contractor is working to secure the certificate of occupancy. This article will help fire practitioners understand those similarities at a high level.

Before exploring the overwhelming similarities, a couple of quick comments about the two biggest differences between fire and security: First, while minimum fire safety requirements are established within ordinances, laws, and their associated/referenced codes and standards, security is (for now) largely unregulated within the United States, and is, rather, an individual preference. Many countries throughout the world mandate minimum security requirements, and that appears to be changing for the United States. The 2021 Edition of NFPA 5000®, *Building Construction and Safety Code*®,[1] will incorporate a new Chapter that, when required by an occupancy Chapter, will outline minimum security requirements.

Second, the tools practitioners use in the delivery of fire safety solutions are largely driven by the physical sciences; whereas every device, feature, and system deployed in the development of security solutions is driven by human behavior. Yes, we can count many fire safety technologies that have evolved because of human behavior (i.e. the use of 10 year permanent batteries in smoke alarms), but the deployment of the technology (i.e. the location of smoke alarms) is driven principally by the physical science of understanding the primary enemy: fire. The primary enemy in security is a determined aggressor continually adapting their means and methods to thwart the most stalwart of security solutions. So, security technology continues to evolve because of human behavior like fire technology evolution; unlike fire/safety solutions, the deployment of technology in a security solution is driven solely by understanding and anticipating human behavior, which (for now), is something less than a physical science.

Common Principles

Because security and fire safety solutions employed within a building are protective in nature (and not to make a building stand tall or make it useable and comfortable while occupying it), those protective solutions are predicated on risk management. Minimizing or mitigating risks is at the heart of protective solutions. Understanding what levels of risk are deemed acceptable is a critical first step in the process of managing those risks. Generally, this requires an assessment of the risks and vulnerabilities anticipated in each project.

In the case of fire safety matters, risks, and vulnerabilities due to fire are generally well known, and society is universally averse to accepting them. The minimum levels of acceptable risk are essentially documented in the form of requirements outlined in our model construction codes and related standards. Historically, building fire codes and standards were largely related to the mitigation of risks due to fire. Over the past decade or so, the purview of building and fire codes has expanded beyond the narrow focus of fire. One obvious example of this is the scope of the requirements included in Chapter 24, Emergency Communication Systems, first introduced in the 2010 Edition of NFPA 72®, *National Fire Alarm Code*®.[2] While the systems addressed in Chapter 24 certainly could be used for fire-related purposes, their intent was for the communication of information regarding emergencies of any nature.

The risks and vulnerabilities associated with security can vary considerably. Similarly, tolerance to acceptable levels of risk also varies. Therefore, the risks and vulnerabilities and plans to mitigate them need to be discussed with project ownership to understand the organizations' tolerance for different types of risks. Documentation of these discussions forms the basis of the security program for the given facility. Absent a codified set of security codes or standards to establish minimum security requirements, development of the security risk analysis is a necessary step to determine the correct type of security to be deployed.

Development of protective solutions to mitigate the identified security risks will utilize the following security principles to mitigate the risks. Interestingly, fire safety protective solutions utilize comparable principles to mitigate fire risks.

Security	Fire
Deter	Prevent
Detect	Detect
Delay	Control
Deny	Contain
Respond	Respond

TABLE 1: Commonalities Between Security and Fire Safety

From a security perspective, the principle of "deter" is to include systems, equipment or processes to dissuade the undetermined from committing a nefarious act; or, another perspective is to prevent the preventable acts. Determined aggressors will find ways to succeed at their intended actions but deterring someone not intent on untoward activity may be as simple as providing a visible lock on a door, which will likely result in an undetermined individual to move on from trying to make entry through the door. In essence, the property owner makes his/her facility look more challenging to defeat so an undetermined individual may go and find another not-so-challenging property to invade. Similarly, in the fire safety arena, we do something fundamental and basic to prevent a fire from occurring. So, for example, a homeowner can prevent a fire by making sure a burning candle is not placed near combustible materials, placing it in a container that will not permit the flame from moving beyond the container.

The security principle of "detect" is to include the systems, equipment, and processes necessary to detect when the determined aggressor defeats the door lock and enters the room or premises the lock was intended to protect. It is similar in concept to the use of fire detection in the fire safety program. As with fire detection, there are several different ways to detect the presence of the determined aggressor. In both security and fire safety, detection is necessary to implement the "respond" principle.

The security principle of "delay" is to include the systems, equipment, and processes necessary to slow down the ability of a determined aggressor to make access to a room or premises. A perimeter fence with control gates is an example of a system that could be used in the security delay principle. The fire safety equivalent might be the deployment of a fire barrier to delay the movement of a fire through the barrier for a determined amount of time. Much like in fire safety, security systems used to delay the determined aggressor may be categorized by the amount of time a properly constructed system can delay the determined aggressor through application of standardized test protocols.

The security principle of "deny" is to include the systems, equipment, and processes necessary to deny access to a determined aggressor. The vehicle barriers depicted in Figure 1 are an example of a system designed to deny vehicular access to a facility by a determined aggressor.

The fire safety counterpart of the security principle "deny" is to contain or not permit spread of a fire from one building to another. Properly constructed fire walls are intended to deny the spread of fire between buildings so that collapse of one building will not adversely impact the stability of the other.

The security principle of "respond" is to summon and provide human intervention to mitigate the determined aggressor. Response is necessary if the determined aggressor ultimately makes access to the facility. Likewise, in fire safety, human intervention is necessary to ensure the fire has been suppressed and fire by-product impacts to the rest of the facility have been minimized.

PHOTO: JEFFREY HARPER

FIGURE 1: System Designed to Deny Vehicular Access

Comprehensive security and fire programs have plans in place to detail how and when response is to be initiated. Quite often in both cases, response is automatically initiated.

Common Design Methodologies

Security program elements generally fall into three disparate groups: architectural systems, technical systems, and the programs needed to operate the physical program. Robust physical security programs employ a mix of three groups of security elements in much the same way that robust fire safety programs are a balance of comparable design methodologies.

DESIGN METHODOLOGIES	
SECURITY	**FIRE**
Architectural	Passive
Technical	Active
Operational	Operational

TABLE 2: Design Methodologies, Security vs Fire

The architectural elements of physical security programs are similar in nature to the passive systems employed in fire safety programs. Both employ barriers of various sorts to mitigate unwanted impact to the facility. Examples of architectural elements that could be incorporated into a physical security program for a facility may include (but are not limited to) the following:

- Physical barriers
- Building hardening and survivability
- Ingress and egress design to manage access
- Electronic access control systems
- Infrastructure survivability

The technical elements of physical security programs are, again, similar in nature to the active systems employed in fire safety programs. Examples of technical elements that could be incorporated into a physical security programs for a facility may include (but are not limited to) the following:

- Electronic access control systems
- Video surveillance systems
- Inventory tracking systems

- Personnel and package screening
- Chemical and biological mitigation systems
- Security lighting
- Intrusion detection systems
- Duress and emergency reporting systems

Compared to fire safety programs, there is more emphasis placed on the operational elements of physical security programs to address the individualistic nature of security. Many of the operational elements of fire safety programs are mandated through applicable ordinances, codes, and laws. Examples of operational elements that could be incorporated into a physical security programs for a facility may include (but are not limited to) the following:

- Policies and procedures
- Post orders
- Visitor management
- Workplace violence programs
- Active shooter plans
- Vulnerability and risk assessments

Figure 2 shows the relationship of the three main groups of elements in a physical security program. This diagram suggests that the most successful security programs are those that properly blend several physical security elements from each group in a proportion that suits the individual facility and the owner's needs and preferences. Determining that balance is contingent upon the individual preferences for physical security and risk aversion/acceptance of the facility owner or occupant.

Too much emphasis can be placed into one of the groups of elements, which can weaken the overall ability of the physical security program to respond to future demands on the system. For example, having a guard force and a plethora of policies and procedures are likely to be ineffective without some level of architectural and technical elements of physical security being incorporated into the facility.

Figure 2 is easily adapted to fire safety. Fire safety design methodologies today employ three primary elements: active fire systems; passive fire systems (including both fire resistive construction and egress design); and development of programs necessary to ensure proper response and operation of those systems. Balance of these three elements is critical to achieve a holistic, robust fire protection program that will serve the facility and its occupants for decades to come. We can install the best fire detection and occupant notification system in the world, but if it is not regularly inspected, maintained, and tested to verify proper operation, it will ultimately fall into a state of dysfunction. Unfortunately, economic and contractual forces often result in the operational element of fire safety being left up to building ownership/management once the structure is complete, which can easily result in some significant gaps.

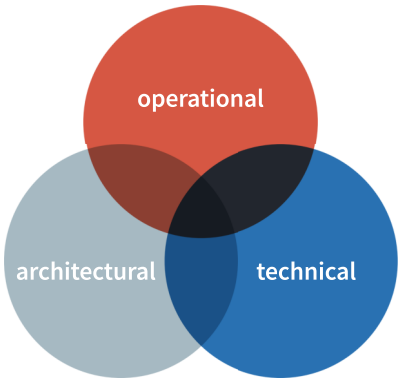


FIGURE 2: Relationship of the Three Main Elements in a Physical Security Program

What the FPE Can Do

Realizing the overwhelming number of similarities between fire safety and security, at least at a high level, how one affects the other is important to the success of a project. Asking the architect or owner about the following subjects early in a project can result in better overall project design and coordination of fire safety and security.

- **Will there be areas of the building that require special locking or access control provisions?** This may affect architectural design of a specific area to assure adequate and proper egress from within and around these areas.
- **Will there be any site access restrictions or controls needed for deliveries to the building/site?** These issues can adversely impact fire department access.
- **Will there be any building hardening incorporated, especially into the façade?** This can impact ability of the fire department in their access or ventilation efforts.

Asking questions about these subjects and having discussions about the potential pitfalls surrounding these issues may result in the design team realizing they need to bring in security professionals to help guide security program development early in the design process. In the end, having an awareness of how security is intended to be incorporated into the project is comparable to understanding how fire rating of the building structure is going to be achieved; all things fire interface with all other disciplines in some way, and it's up to us as the fire professionals to best understand those impacts.

JEFFREY E. HARPER, *PE, FSFPE, is with JENSEN HUGHES.*

References

1. National Fire Protection Association, "NFPA 5000®, Building Construction and Safety Code®," Quincy, MA, 2021.
2. National Fire Protection Association, "NFPA 72®, National Fire Alarm Code®," Quincy, MA, 2010.