Leveraging Safety Programs to Improve and Support Security Programs

J. Leach, M. Snell, R. Pratt, S. Sandoval

Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185-1234

Abstract

There has been a long history of considering Safety, Security, and Safeguards (3S) as three functions of nuclear security design and operations that need to be properly and collectively integrated with operations. This paper specifically considers how safety programmes can be extended directly to benefit security as part of an integrated facility management programme. The discussion will draw on experiences implementing such a programme at Sandia National Laboratories' Annular Research Reactor Facility.

While the paper focuses on nuclear facilities, similar ideas could be used to support security programmes at other types of high-consequence facilities and transportation activities.

Introduction

Security programmes at research reactors containing less than Category I nuclear material tend to have considerable constraints in terms of cost and personnel. For example, at some facilities there may be one person responsible for security for which it is merely one job among several.

Reference 1 describes recommendations on physical protection of nuclear materials and nuclear facilities[1]. Even for Category III facilities, recommended physical protection requirements are extensive and include:

- Development and maintenance of security plans (to include assigned physical protection responsibilities);
- Means and procedures for evaluations, including performance testing, and maintenance of the physical protection system (PPS);
- Development and maintenance of security culture;
- Quality assurance programmes covering design, implementation, operation, and maintenance of physical protection systems;
- Establishment of sustainability programmes for the PPS, to include operation procedures, human resource management and training, equipment updating, maintenance, repair and calibration, performance testing, configuration management, resource allocation and operational cost analysis; and

[1] Reference 2 addresses physical protection of radioactive material and associated facilities.

- Development and maintenance of contingency and emergency plans and exercises of such plans.

Comparatively, there are several inherent advantages of safety programmes over security programmes, such as:

- Safety, as a field, is comparatively more mature and has very detailed processes;
- Safety processes and techniques can be shared nationally and internationally without security concerns; and
- Nuclear facilities tend to have more extensive and comprehensive safety programmes than security programme.

Much of the motivation for this paper was the recognition that safety may already support capabilities that security organizations could leverage so as to be more effective within the security resource constraints. The title reflects this specific interest. While such leveraging will indeed benefit security, there is significantly more value in addressing safety and security in combination rather than individually.

There are also competing, and in some cases, conflicting safety and security priorities and these need to be addressed. For example, security principles may suggest consolidation of material to reduce the number of target locations. However, from a safety perspective, consolidation of material may result in a criticality event. A combined approach to safety and security explicitly takes such conflicts into account.

This paper addresses three sets of programmes to implement a more holistic approach to safety and security:

- Integrated management systems;
- Formality of operations and maintenance of an organizational culture; and
- Exercise programmes.

An integrated management system based upon a formality of operations approach will evaluate the conflicts between security and safety and produce a culture that supports both objectives with available resources. Exercises can then be used to measure the effectiveness of these three programmes. The paper discusses these programmes based on experiences at Sandia National Laboratories' Annular Research Reactor Facility.

There are some aspects of security programmes that do not have direct parallels with safety; these are addressed in a final section of the paper.

Incorporation of Security in a Management System

The intention of an Integrated Management System (IMS) is to be inclusive of interrelated elements as a means to ensure facility mission achievement in an efficient and effective manner.

As such, all aspects of research reactor operations, to include security, health, and quality are included. An IMS incorporates safety into all facets of day-to-day tasks to ensure work is successfully accomplished, the operational mission of the facility is satisfied, and personnel, the public, and the environment are protected. An IMS is an institutional program that consists of five overarching principles:

- **Plan the work** – Ensure safety missions are uniformly translated into objectives, expectations established, tasks are defined and prioritized, and resources equally allocated.
- **Analyze the risks** – Identify, categorize, and communicate risks to life and asset(s).
- **Develop controls** – Establish administrative and engineering controls and allocate resources to address safety considerations.
- **Perform the work** –Worker competence shall be commensurate with responsibilities and personnel shall possess the experience, knowledge, skills, and abilities necessary to carry out their responsibilities.
- **Feedback and improvement** – Feedback information on the adequacy of controls, identify opportunities for improving the planning or execution of work.

The IMS is one approach to strengthening the relationship between safety and security as security elements can be applied to each of the five principles. Another management system approach is detailed in the IAEA Safety Report Series (SRS) No. 75, *Implementation of a Management System for Operating Organizations of Research Reactors*. SRS No. 75 is a useful document for new or part-time management system staff for many reasons, one of which is the "Plan-Do-Check-Act" management system cycle. For each step in the cycle, the report provides process flowcharts. Facilities with limited resources can leverage this approach as a way to help overtaxed security staff spend time following management system processes instead of having to develop them. In new or immature security programs, having an established approach to guide personnel could increase the probability of success.

Both the IMS and Plan-Do-Check-Act management system approaches[2] represent continuous improvement cycles that align with facility objectives to achieve and enhance safety. When taken a step further, these approaches can easily be adapted to include security. Figure 1 combines the IMS and the Plan-Do-Check-Act cycle to highlight the applicable security and safety elements at each step.

[2] IAEA requirements and guidance documents have adapted the term 'management system" rather than "quality assurance". All references to management systems in this paper is inclusive of quality assurance.

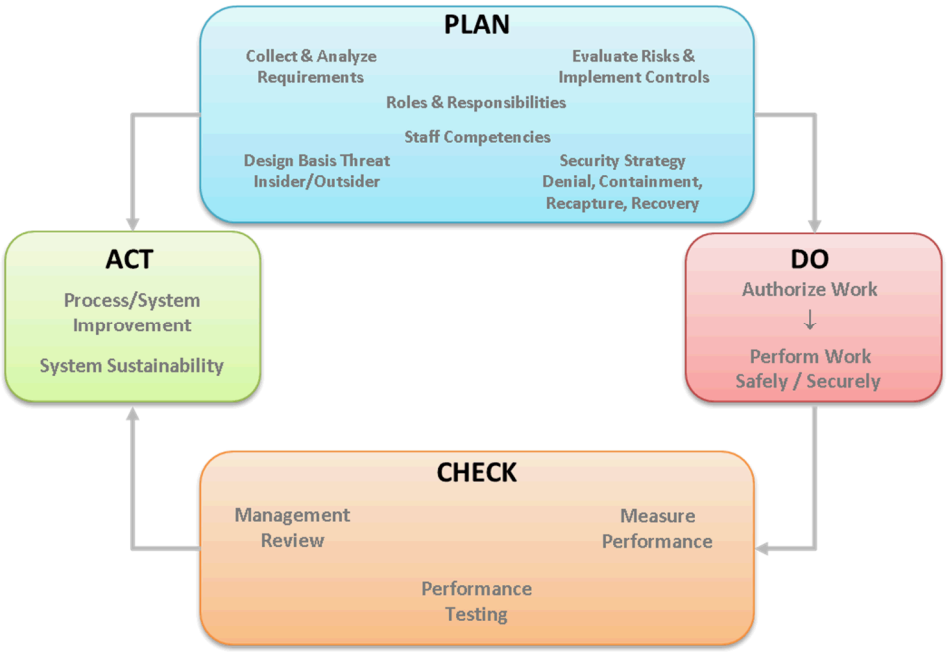

Figure 1. Safety and Security Management System Continual Improvement Cycle

Security programs can capitalize upon the maturity of safety programmes particularly through the integration of a management system. Take for example the event that occurred at the U.S. Department of Energy's (DOE) Y-12 National Security complex. Y-12 is a key facility within the National Nuclear Security Administration's (NNSA) Nuclear Security Enterprise. The facility operates an extensive security programme that relies on a well-trained and extensively equipped protective force, advanced intrusion detection technology, and a variety of physical fortifications. In the early morning of July 28, 2012, three activists gained access to the Y-12 compound and subsequently to what is called the Highly Enriched Uranium Materials Facility (HEUMF) and physically defaced the building before site security forces apprehended them. The DOE Inspector General (IG) conducted a special inquiry of the event and identified multiple system failures:

- Inability to respond to alarms;
- Failure to maintain critical security equipment;
- Misunderstanding of security protocols;
- Poor communication; and
- Weakness in resource management

While an unfortunate event, this has served as a major lesson learned for the US nuclear security community and illustrates issues that a properly executed management system based upon the features identified within this paper may have prevented. For instance, an integrated management system would have identified safety, security, and safeguard objectives and, established expectations with prioritized tasks for qualified and trained personnel. Further, risks

would have been identified with appropriate controls in place for mitigation with a constant evaluation in place focusing upon system performance. Such an evaluation is inclusive of a feedback process, which, in cases where deficiencies such as those identified by the IG, are brought to management attention could have been remedied.

Lessons Learned from the Implementation of a Management System Programme

Prior to 2009, Sandia National Laboratories' Annular Research Reactor Facility had a traditional quality assurance (QA) system that operated as a separate program. As such, the QA personnel performed verification of products and services to meet requirements prior to delivery. The advantage of QA autonomy was its flexibility to operate independently. However, the disadvantage was that QA only functioned when a process or person existed to bring it into the management system. When QA was not included, the result was a gap. These gaps became increasingly unacceptable as the regulatory environment increased. At the same time, the growth in the regulatory environment made it increasingly difficult to ensure that people and processes remained up-to-date with requirements. In short, the paradigm of QA as a separate organization was failing.

In 2009, the Annular Research Reactor Facility integrated QA into a formal quality management system. One of the goals of transformation was to reduce the gaps in requirement implementation and the addition of layers of protection so that potential gaps were less likely to be missed entirely. This goal was achieved by changing QA from something that was bolted on at the end into something that was integrated from the beginning. Individual QA procedures were replaced with a holistic management system that assigned responsibilities to specific groups and explicitly incorporated the quality assurance checks into implementing procedures.

Prior to transformation, each group had grown organically. Operations did operations work, security did security work, and quality assurance did quality assurance work, but the interfaces between each group were not managed. When a changing requirement generated new roles and responsibilities (R2) each group would determine independently if it applied to them and adjust accordingly. Most of the time the new R2 was clear and this system worked. However, when the task was not clear, sometimes both or neither group would assume it, leading to either waste or a gap. Setting up a formal structure that assigned responsibilities to individual programs reduced the likelihood that a requirement would not be assigned at all. It also had the advantage of creating a single source of truth that was independent of either organization. This was useful when there was a conflict as to who was responsible for a given responsibility. Today, the integrated management system at the Annular Research Reactor Facility is comprised fourteen primary programs and four subprograms (Figure 2). Each programs/subprogram has elements of security, safety, and QA incorporated throughout and has a consistent voice for interactions with other organizations.

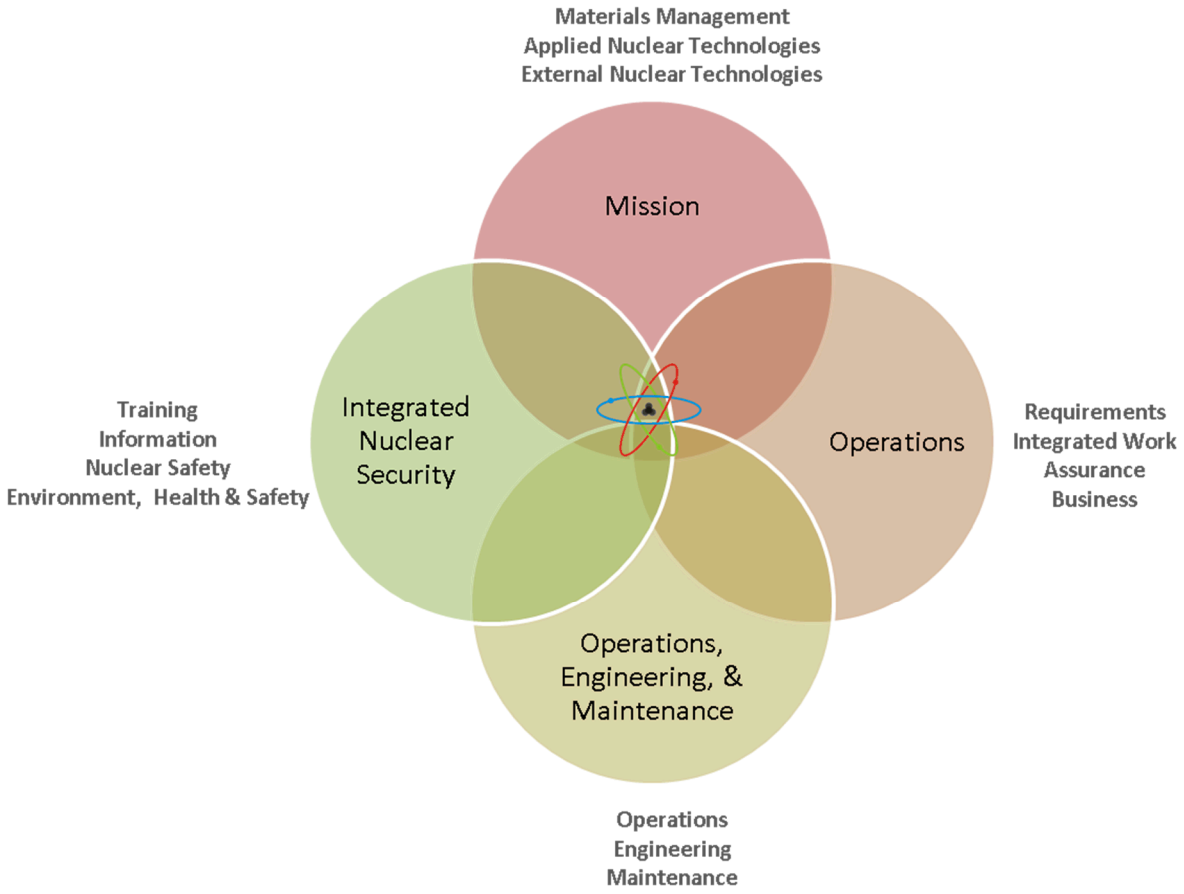

Figure 2. Overview of the Integrated Management System at the Annular Research Reactor Facility

A second problem mitigated by transformation was the implementation of new or changing requirements. Prior to transformation, subject matter experts (SMEs) would track stakeholder requirement(s) for their particular area of expertise. This represented a potential single point of failure for requirement implementation. To mitigate this risk, TA-V stood up a Requirements Management Program.

One of the specific functions of the Requirements Management Program was to review all changing requirements from internal or regulatory bodies and ensure that the appropriate SMEs are aware that the change exists, thus removing a potential single point failure. Requirements Management also reviews implementing procedures to ensure that regulatory requirements are met if the procedure is followed as written. This review ensures quality is built in at the beginning of a process instead of tested in at the end. The review also provides a backup to the author who may not have much experience in how to read and implement a requirement that was not present before.

One of the similarities between a quality assurance management system in general, and safety and security fields in particular, is that both require a practitioner to remember to consider many

different small details or items. Many of these items may not be clear to someone with limited experience. The obvious solution is to create guides that a staff member can use as a basis for their work. The IAEA Safety Standards Guide No. GS-G-3.5, *The Management System for Nuclear Installations,* provides a detailed list of all of the objectives that a facility implementing a quality management system should consider. While such items also exist for nuclear security, one point where you can leverage information is to look at the items that quality assurance considers, but security does not.

For example, research reactors typically have small groups of staff who have to fulfill many different roles, including both quality assurance and security. To help research reactors establish quality management systems, the IAEA published the SRS No. 75. This document is quite helpful for a new or part-time quality assurance staff because it provides not only a list of requirements or items to consider, but it also provides a flowchart on how to accomplish it. For example, it is one thing to read in a document that "the levels of calibration… should be defined" (GS-G-3.5), but it is much more helpful to have a complete flowchart of how to perform and document calibration such as the above SRS provides. The approach could be leveraged by security as a way to help new or limited staff by allowing them to spend their limited time following processes instead of having to develop them.

Figure 3 is an example flowchart of a hypothetical access control process. The flowchart documents and communicates the chronological steps involved in entry and/or exit and at which step the procedure is enforced by electronics. Flowcharts such as these are useful tools to assist the author or management to identify gaps in processes before it is rolled out to personnel.

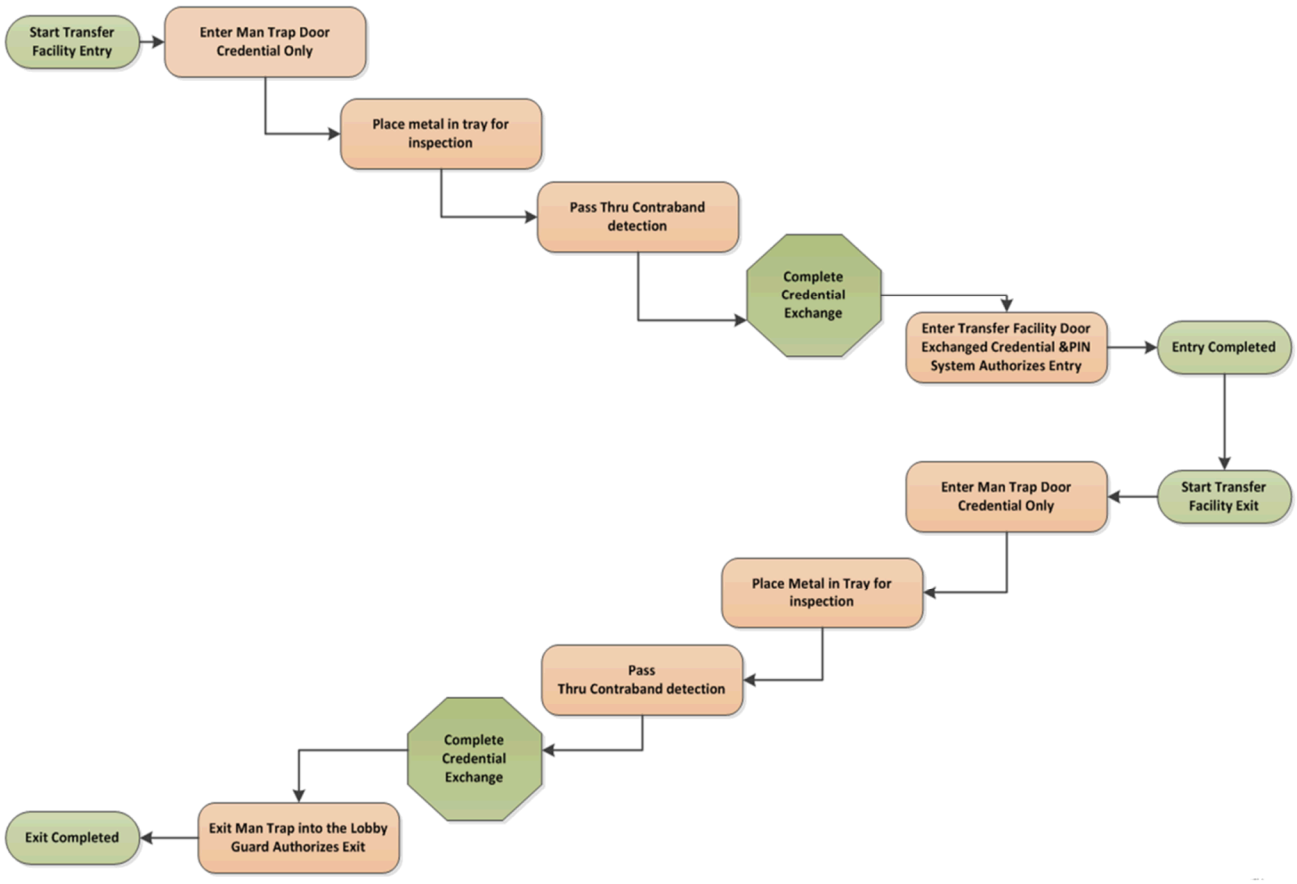

Figure 3. Example Entry / Exit Process Flow Chart

Leveraging Formality of Operations to Develop Organizational Culture

One of the most difficult things to define within a management program is what makes up a solid culture. Culture receives specific attention in documentation of management systems; however, the emphasis is primarily safety culture. As part of a management system, organizations of all sizes develop procedural norms referred to as "formality of operations". High-consequence facilities document these formalities of operations in the form of policy and procedural documents as a means to achieve desired practices. Similar to management systems, formality of operations has a safety-based origin. When integrated with a management program and security aspects, formality of operations establishes an organizational culture of surety that institutes excellence in the performance of every task while minimizing variations in performance.

There are four key intertwined principles of a formality of operations programme that result in a desired organizational culture:

- Conduct of operations
- Maintenance and surveillance
- Training and qualification, and

- Configuration management

Simply stated, formality of operations ensures that operational activities are performed based upon documented procedures (conduct of operations) using equipment that is functional, (maintenance and surveillance) controlled and configured as per documentation (configuration management) by staff that is trained and knowledgeable (training and qualification). A formality of operations program is the equivalent of a check and balance process that results in the formation of an effective surety program creating a motivated organizational culture that focuses upon consistent performance improvement.

Formality of operations is part of a facility's day-to-day operation and represents an ongoing commitment to reliable operations. This aspect of the program translates directly to the development of a culture consistent of high-level human performance. Research has yielded those facilities that lack a developed organizational culture typically have less than adequate levels of human performance which adversely influences other aspects of operations. At high-consequence facilities, as the complexity of operational activities increase, a commensurate increase in organizational culture must also occur in order to ensure safe, secure, and consistent performance of critical tasks.

To foster an organizational culture, a facility must start with a statement of objectives and risk tolerance. While it may appear that safety and security have opposing threats, there is commonality in that both seek to protect against risk to the environment via malevolent adversarial use or accidents due to the human factor. Further, management must reinforce policies and procedures in its formality of operations so that culture becomes second nature. Such a culture would combine recognition of a facility's hazards, evaluation of risk, design for safety, security, and quality assurance, by trained and qualified personnel.

Use of Exercises to Measure Effectiveness of a Management System, Formality of Operation and Organizational Culture

Training exercises are perhaps one of the simplest measures to examine the effectiveness of a management program, its formality of operations, and their impact on organizational culture. Exercises provide an environment to test staff capabilities, familiarize personnel with roles and responsibilities, and foster meaningful interactions and communications across various levels of personnel. In addition, exercises can also eliminate lingering divisions in cultural-based beliefs. For instance, a safety culture believes that *accidents* can and will happen. In comparison, security culture belief is that there are credible *threats* to targets at all times. Training exercises bridge the sharing of security and safety procedures and policies and fosters a unified sense of threat and the need to mitigate these risks.

Prior to determining exercise scope, management must establish system priorities. These priorities can be based upon threat and hazard identification, capability assessments, or contingency planning and drive the development of exercise objectives. In turn, each objective

should align with one or more organizational core capabilities. Once priorities and objectives are identified, the method of training is selected. There are varieties of training exercises that can be used to assess how well a management system influences organizational culture. For instance, if the intent is to review and discuss new policy, plans, or procedural sets, a discussion-based exercise may be appropriate. If the intent is to assess personnel knowledge of plans, policy, procedures, an operations-based exercise may be appropriate.

Regardless of the exercise approach, it is important that safety, security, and management personnel participate, and that exercise scope and objectives encompasses these three elements. It is equally important to capture exercise data for the purpose of analysis and reporting. A representative of facility management should designate an individual to capture notes during the course of exercise play, identify demonstrated strengths, and document areas for improvement. The captured information will identify the underlying reason for or root cause behind issues revealed during exercises. When completing the analysis, evaluators should consider:

- Were personnel capability targets met? If the targets were not met, what factors contributed to this result?
- Did discussion or activities suggest critical tasks were executed to meet capability targets? If not, what was the impact or consequences?
- Do current plans, policies, and procedures support critical tasks and capability targets? Where participants familiarized with these documents?

Analyzing exercise events will help management determine the underlying cause of issues and aide in the development of corrective actions to remedy the situation. To ensure that corrective actions are taken, management must identify which issues fall within which organization's authority and ensure said organization takes responsibility for corrections.

Unique Security Considerations

Security programmes include several aspects that do not have direct parallels with safety:

- Unique PPS functions that need to be performed: detection (including access control and intrusion detection), delay, and response;
- Compliance requirements and, where applicable, performance-based security requirements (to include performance testing) as addressed in security plans;
- Use of policy threat statements about security threats, as opposed to more readily observable safety hazards; and
- Confidentiality requirements for information about the threat as well as physical security measures (in terms of personnel, procedures and equipment) that constitute a PPS.

As PPS functions and requirements have little connection to the functions of a safety system, there is a need to maintain separate technical and operational expertise in these security areas. Some of this expertise must exist at the facility, to support facility management, development of

plans and procedures, and maintenance of quality programmes. For smaller facilities, significant capabilities may be maintained offsite. For example, security system components may be installed, monitored and maintained, and tested using technical personnel contracted from private entities. Further, armed response may be provided by offsite organizations, such as the police or military. At the same time, confidentiality requirements for information may necessitate use of different personnel to perform work on security as opposed to safety or other programmes.

These unique aspects will probably not disappear within the near future, thereby providing limits to how much security can practically leverage safety[3]. Still, a holistic approach to safety and security may identify better ways to plan and provide oversight of outside technical contractors or maintain coordination with outside response organizations.

Conclusions

Though the terms safety and security are used together, there is a distinct difference between the two. Safety strives for protection against hazards while security strives for protection against malevolent threats. The basic underlying idea of safety and security is asset protection via the creation of a safe, secure, risk-free environment. This can be achieved through the institution of a management system based upon a formality of operations approach.

An integrated facility management system takes a holistic approach for facility operations from initial planning, execution, evaluation, and corrective actions. Each step in the cyclical process can easily incorporate safety, security, and safeguard activities. Incorporation of these activities at each steps ensures that there is communication and interaction amongst various members of personnel and encourages cooperation between staff members. Such cooperation is a crucial steps towards the formation of an organization culture where personnel understand their roles and responsibilities as well as those of their coworkers, thereby forming a collective sense of responsibility.

Training exercises are useful for facility management to determine if management systems and culture are effective. These exercises, if designed properly, yield insight as to how personnel may perform in a real-world event. If deficiencies are identified, corrective actions can be created and implemented.

[3] There may also be some differences between managing a security organization versus a safety organization that are not as easily categorized in the discussion provided here. Based on historic experience, effective security management appears to require more active probing – "turning over rocks" as it were – to look for problems before they become serious. If true, this may occur because safety typically has more performance indicators that can be tracked directly.

References

1. *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5)*, IAEA Nuclear Security Series No. 13, International Atomic Energy Agency (IAEA), 2011.
2. *Nuclear Security Recommendations on Radioactive Material and Associated Facilities,* IAEA Nuclear Security Series No. 14, International Atomic Energy Agency (IAEA), 2011.
3. *Implementation of a Management System for Operating Organizations of Research Reactors* IAEA Safety Report Series (SRS) No. 75.