

Safety and Security Interface Technology Initiative
Mr. Kevin J. Carroll
Dr. Robert Lowrie, Dr. Michael Lehto
BWXT Y12 NSC
Oak Ridge, TN 37831
865-576-2289/865-241-2772
carrollkj@y12.doe.gov

Work Objective. Earlier this year, the Energy Facility Contractors Group (EFCOG) was asked to assist in developing options related to acceleration deployment of new security-related technologies to assist meeting design base threat (DBT) needs while also addressing the requirements of 10 CFR 830. NNSA NA-70, one of the working group participants, designated this effort the Safety and Security Interface Technology Initiative (SSIT).

Relationship to Workshop Theme. “Supporting Excellence in Operations Through Safety Analysis,” (workshop theme) includes security and safety personnel working together to ensure effective and efficient operations. One of the specific workshop elements listed in the call for papers is “Safeguards/Security Integration with Safety.” This paper speaks directly to this theme.

Description of Work. The EFCOG Safety Analysis Working Group (SAWG) and the EFCOG Security Working Group formed a core team to develop an integrated process involving both safety basis and security needs allowing achievement of the DBT objectives while ensuring safety is appropriately considered. This effort garnered significant interest, starting with a two day breakout session of 30 experts at the 2006 Safety Basis Workshop. A core team was formed, and a series of meetings were held to develop that process, including safety and security professionals, both contractor and federal personnel. A pilot exercise held at Idaho National Laboratory (INL) in mid-July 2006 was conducted as a feasibility of concept review.

Work Results. The SSIT efforts resulted in a topical report transmitted from EFCOG to DOE/NNSA in August 2006. Elements of the report included: Drivers and Endstate, Control Selections Alternative Analysis Process, Terminology Crosswalk, Safety Basis/Security Documentation Integration, Configuration Control, and development of a shared ‘tool box’ of information/successes.

Specific Benefits.

The expectation or end state resulting from the topical report and associated implementation plan includes:

- (1) A recommended process for handling the documentation of the security and safety disciplines, including an appropriate change control process and participation by all stakeholders.
- (2) A means to package security systems with sufficient information to help expedite the flow of that system through the process. In addition, a means to share successes among sites, to include information and safety basis to the extent such information is transportable.
- (3) Identification of key security systems and associated essential security elements being installed and an arrangement for the sites installing these systems to host an appropriate team to review a specific system and determine what information is exportable.
- (4) Identification of the security systems’ essential elements and appropriate controls required for testing of these essential elements in the facility.
- (5) The ability to help refine and improve an agreed to control set at the manufacture stage.

Executive Summary

The purpose of this paper is to describe a process developed to facilitate integration of security and safety elements, satisfying the current DBT expectations as well as safety basis objectives. The proposed process described in this technical report is the result of a series of core working team meetings in Germantown, Maryland, in early March 2006 and in Idaho Falls, Idaho, in mid-July 2006. The team worked to develop concepts that were initially discussed at several February 2006 meetings.

Process Summary

A cost effective, comprehensive process has been developed to simultaneously satisfy DBT and safety basis objectives for security systems. This approach is intended to facilitate sites meeting the defined dates to satisfy the DBT. An integrated project team approach has been proposed that contains multiple interrelated elements/processes: training, alternative analysis, document integration, configuration control, etc. Section 5 of the report lays out the overall process.

A key element of this process leading to cost savings for individual facilities is the toolbox approach that makes systems and key information transportable between facilities and sites and accessible by multiple DOE sites for review and use. The toolbox is populated with pertinent Security Information Data Set (SIDS) information that includes safety basis and security data for various security systems, including system evaluation and approval documentation. This data may be used as part of the information set required to obtain approval to deploy similar security systems at several sites.

For this process to be successful, safety and security professionals from around the complex and at DOE-HQ need to understand the parameters under which their counterparts work and possess a contextual understanding of the terms used by their counterparts.

Topical Report Elements

The key elements of the topical report are addressed below.

Drivers and End State

The key concepts and regulatory requirements to be considered to successfully deploy new or modified security systems at DOE nuclear facilities are identified and discussed. All requirements must be satisfied to successfully meet the objectives of the proposed process. The desired end state for this process includes successful implementation in the field, handling of related documentation, and the concept of a portable database or toolbox containing pertinent security and safety basis information suitable for multi-site use.

Establish Terminology/Concept Crosswalk

Effective communication between the security and safety basis professionals is needed for this process to be successful. In some cases the same or similar words have very different meanings depending on the venue. The reverse is also true; different terms can have the same or similar meanings. To help address this concern, a process to inform and familiarize Subject Matter Experts (SMEs) from each discipline is proposed.

Awareness Training on Project Approach, Selection of Tools, and Terminology

This element focuses on ideas and concepts related to training that would serve to enhance the understanding of procedures and programs on the various security systems and upgrades. The principal intent is to devise training that can be transported between multiple sites.

Integrated Project Approach to Safely Deploy Security Systems

To cost effectively deploy a new or upgraded security system, an integrated project approach is recommended. This section adapts this approach to security systems and presents a process flow that starts with the DBT, evaluates a series of candidate security systems, prepares security and safety basis documentation as required by the Nuclear Safety Rule (10CFR830 Part B), and selects and procures the optimal system or systems. Preparation of the project execution plan is a key component of this approach.

Alternative Analysis Process for System Selection

The alternative analysis process is an integral element in the proposed integrated project approach. This section describes this process in detail showing how an optimal security system is selected to satisfy both security and safety basis objectives. Representatives from security, safety basis, and DOE are part of the project team that exercises this process and selects the optimal system or systems.

Security System Toolbox: Development, Data Capture, and Data Sharing

This section presents a concept with the potential for universal application at DOE sites. The intent is to identify and provide information to the end users or sites that facilitate the deployment of security systems that meet safety basis requirements. Important data covering the security system, security analyses, and safety basis information can be captured in a data base (toolbox) and shared among the DOE sites that are required to meet the DBT. It is recognized that classification considerations with this toolbox will have to be managed based on a need to know. The ultimate goal is development of a “system in a box” concept, whereby individual sites can access the database and select security systems that have already been tested, evaluated, and approved for use within the DOE Complex. Thus, the new analysis may be limited to the site or installation of specific evaluations to assure that the specific installation/use is within the approved criteria and standards. This concept has the potential to greatly simplify the security system approval process.

Safety Basis and Security Document Integration

This section summarizes the documentation objectives associated with both safety basis and security. Clearly, a new or upgraded security system should be accurately reflected in both sets of documents. DOE approvals will also be necessary in some instances for both document sets. This section addresses the documentation implications in both venues. The major modification concept and its application in this arena are also discussed in some detail. However, the safety driven activities for major modifications and new projects are being developed in DOE-STD-1189, Integration of Safety into the Design Process.

Post-Installation Readiness

After installation of new or upgraded security systems, an appropriate level of review needs to be conducted to ensure that system operability and safety requirements have been met, and that design objectives have been satisfied. A graded approach should be used to the extent practical. This section also recommends using existing readiness review processes rather than creating new ones.

Configuration Control

The need for configuration control of security systems is apparent. The concept presented in this section assumes separate paths (one for the safety basis process and one for the security process) that interface at opportune points. The unreviewed safety question (USQ) process is required for security system changes to evaluate changes to the safety basis, as well as the DOE approval requirements on the safety basis documentation changes. A security change control process, which defines the DOE approval requirements, is required to evaluate changes in the security venue, whether the change was driven by security, safety, or operational requirements. This may be performed as part of the Site Safeguards and Security Plan (SSSP) configuration control.

Review Process for Improvements and Lessons Learned

The concepts presented in this topical report are intended to be “living processes” that are expected to be improved and updated over time. This section provides the framework for periodic reviews of the processes to incorporate lessons learned from, for example, external and internal assessments as well as process reviews.

1. Introduction

The scope of this effort is to develop an integrated process involving both safety basis and security allowing achievement of DBT objectives while ensuring safety is appropriately considered. This report was developed as a starting point for building a bridge between the requirements and practices within the security and safety disciplines. This report is not intended to be the final solution, but a catalyst facilitating communication and allowing the sites and facilities to meet the short-term DBT requirements and schedule. However, successful implementation has the potential of making this process a long-term solution for these facilities across the complex. This report proposes practices that are expected to reduce the cost of implementing the DBT evaluations and shorten scheduled implementation. In addition to establishing a database and framework for sharing data on security system design and implementation, this process addresses the separation of requirements and interfaces between safety and security needs. This process does not add any requirements to the existing DOE regulations for security or safety. This process is intended to be a guide, facilitating implementation of these requirements.

2. Drivers and End State

The key concept to consider in assuring that both the security requirements and safety requirements are satisfied for any security installation at a facility meeting the DBT is that the approach: 1) encompass all threats against which security systems are required to be designed and 2) be employed in an effective manner to assure neutralization and protect national security. The process outlined herein, while having attributes helpful for long-term application, was developed to concentrate on implementation of needed security features to meet the near-term DBT needs.

The implementation requirements (regulations) that drive the key actions for both security and safety derive from the following regulations:

- Design Basis Threat Policy (DOE O 470.3A)¹
- Safeguards and Security Program DOE Order 470.4² and associated manuals; (DOE M 470.4-6, 8-26-05)
- Salient Consideration Memorandum³
- Nuclear Safety Management Rule (10 CFR 830)⁴
- Facility Safety (DOE O 420.1⁵ and Guides)
- Integration of Safety into the Design Process (DOE-STD-1189-2006)⁶
- Worker Safety and Health Program Rule (10 CFR 851)⁷
- “Adversary Capabilities List (ACL) - Terrorist Adversary Capabilities List”⁸
- “Vulnerability Assessment Process Guide.”⁹

The expectations or end state resulting from this report and associated implementation program elements include:

- A recommended process for handling the documentation of the security and safety disciplines, including an appropriate change control process and participation by all stakeholders in the facility that may be impacted by the change [e.g., facility operations personnel, documented safety analysis (DSA) developers, facility management].
- A means to package security systems with sufficient information to help expedite the flow of that system through the process. In addition, a means to share successes (including all lessons learned) among sites, to include information and safety basis to the extent such information is transportable.
- Identification of key security systems and associated essential security elements being installed, and an arrangement for the sites installing these systems to host an appropriate team to review a specific system and determine what information is exportable.
- Identification of the security system essential elements and appropriate controls required for testing of these essential elements in the facility.

For this process to work effectively, it should be applicable to all facilities and have implementation feedback as an integral part of the overall process. Accordingly, this process requires input and participation from both safety and

security professionals and the associated decision makers at each participating site.

The expectation for the solution reached for each site recognizes that assuring adequate safety and security is the goal and that risk of an accident or security breach will never be zero. Therefore, the focus is on providing adequate and appropriate protection in these areas with consideration of other project elements. Thus, the final solution balances each of these parameters to reach the appropriate solution for the facility under consideration.

3. Establish Terminology/Concept Crosswalk

To effectively integrate the safety and security processes, there is a need for a common understanding of the requirements, concepts, and terms on which each group relies. This report is intended to inform and familiarize security professionals and safety professionals with the regulations, requirements, and issues governing the functions of their counterparts. It is not the intent of this section to complete this familiarization process, but to highlight some of the differences that may exist between the two disciplines.

The inherent differences in requirements and expectations result in two different sets of terms, regulations, and goals for success that if understood, allow success in both venues and satisfy all acceptance criteria. At the top level, the acceptance criteria for a facility or project requires that both safety and security requirements be satisfied. Neither set of regulations takes precedence over the other within the scope of the applicable regulatory requirements. However, there are conditions for which individual regulations do not apply. For example, DOE-STD-3009, CN3 excludes sabotage and terrorism from the scope of the hazard and accident analysis performed in support of the facility nuclear safety basis. Although acts of sabotage and terrorism are excluded from the hazard and accident analysis scope, this does not preclude the need to analyze and describe security systems and associated accident conditions in the safety basis for the facility. On the other side, a threat (perceived or real) in which security personnel are alerted changes the relative significance of the criteria. In this case the environment, safety & health (ES&H) requirements are not applicable if they are in conflict with the security response. Protection of the material is the highest priority and provides the greatest safety for all.

There are three key differences that need to be addressed to provide an appropriate platform within which security and safety issues can be integrated: (1) Definition of success (goals), (2) Regulations and expectations (3) Terms and definitions.

The definition of success within the ES&H discipline is to assure that the complete spectrum of potential accidents that could expose members of the public, onsite workers, facility workers, and the environment to hazardous materials has been evaluated and appropriate protection provided. The definition of success within the security discipline is to develop protection strategies for threat level 1 through 4 facilities that achieve acceptable protection system levels. These two definitions of success often lead to conflicts, the most obvious being personnel evacuation in the event of an off-normal condition. A key factor in successful resolution of this conflict is the integration achieved through the alternative analysis.

4. Awareness Training on Project Approach, Selection of Tools, and Terminology

To effectively transport the selected security concepts among the various sites, a consistent approach to training and terminology is needed. As this consistency should be developed along with the security system, the purpose of this section is to establish the overall approach to developing the training and consistent terminology for the system. This discussion focuses on ideas and concepts that would enhance the portability of training procedures and programs for the various proposed security systems to multiple DOE sites.

Integrated Safety Management System principles should be incorporated in project execution planning and in establishing scope and technical requirements for the security system using a tailored approach. A needs and impact analysis should be conducted to determine the basis for the design and development of the training program. Additionally, it is recommended that training procedures associated with the security systems be developed in time to support all associated internal and external reviews.

Project interfaces need to be established, implemented, and maintained among the organizations and disciplines participating in the design and implementation process. Interface controls include communications, identification of responsibilities, and written procedures. The vendor may be required to provide design review/support personnel to

interface with facility system engineers and facility safety personnel to answer questions about the equipment and its possible affects on facility personnel and the safety basis. Consideration should be given to having the security system vendors observe and monitor (where permissible) the final installation and onsite shakedown testing of these systems.

Procedures should incorporate appropriate and pertinent information from source documents, such as facility design documents, safety basis documents, and vendor technical manuals. Prior to approval for the first deployment of any selected security system, all associated facility operational and maintenance procedures should be completed and available to accompany future deployments at other sites. Modifications to these procedures should be made at each site prior to approval for deployment, incorporating installation-specific revisions to the base procedures.

5. Integrated Project Approach to Safely Deploy Security Systems

Prior to selection of new or upgraded security systems to meet the DBT, an integrated evaluation of available alternatives should be performed. The integrated evaluation is to ensure integration of safety, security, operations, and governmental policy. The integrated evaluation involves establishing a project management team structure with participation from appropriate security, safety, and operations representatives. Figure 1 provides a process flowchart to effectively deploy new or upgraded security systems to meet the DBT, while ensuring compliance with applicable safety requirements. The process begins with recognition of a change in security protection requirements, such as a change in the DBT or with the results of an ongoing SSSP review. Security personnel then perform a vulnerability analysis (VA) of the DBT changes.

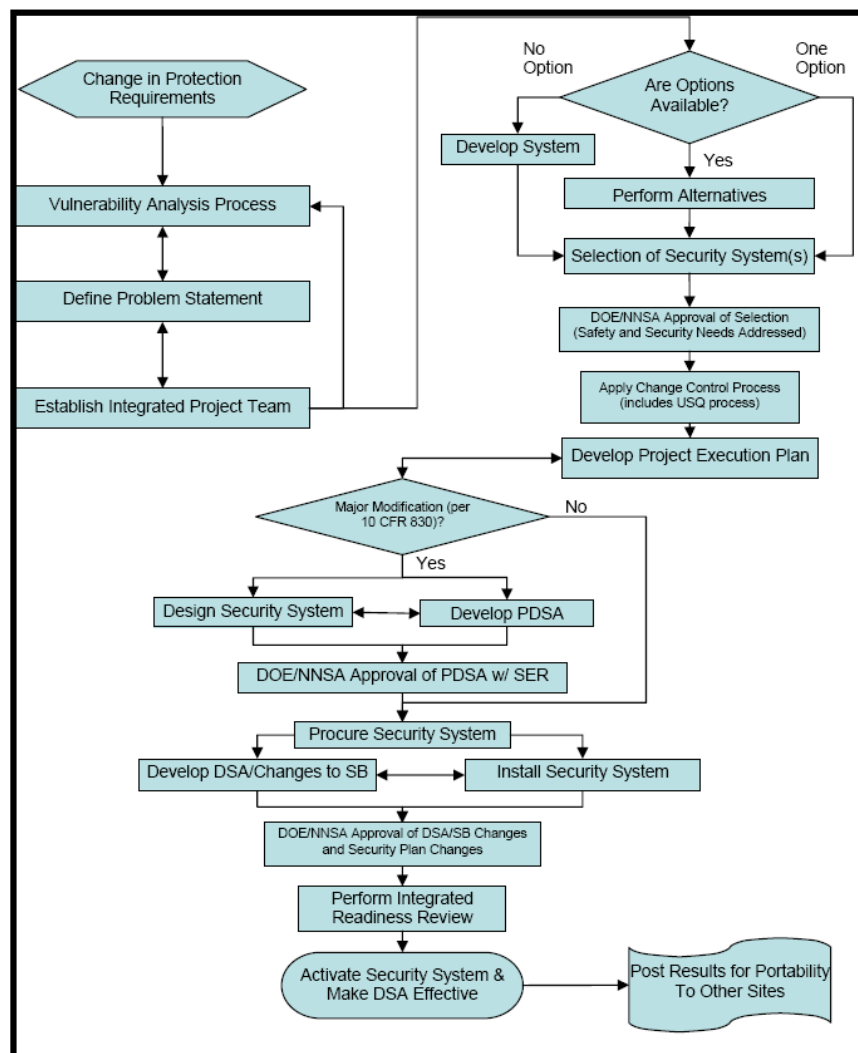


Figure 1 Security System Deployment Process Diagram

DOE M 470.4-1¹⁰ chg 1, Part 1, Section E – “Vulnerability Assessment Program,” outlines the general requirements to conduct a VA and contains information about planning assumptions, threats, targets, modeling, performance testing, results, quality assurance, figures of merit, critical system elements, VA reports, system effectiveness, training and certification. Additional VA Program requirements are contained in:

- DOE O 470.3A,¹ “Design Basis Threat Policy”
- Adversary Capabilities List⁸
- VA Process Guide⁹
- Salient Considerations Memorandum³
- DOE Manuals 470.4-2,¹¹ “Physical Protection”; 470.4-3,¹² “Protective Force”; and 470.4-6,¹³ “Nuclear Material Control and Accountability”
- “Consolidated Guidance Concerning the Required Format and Content for the Design Basis Threat Implementation Plans and Quarterly Updates”¹⁴
- “2004 Design Basis Threat Implementation Plan Vulnerability Assessment Requirements”¹⁵
- “Modified Probability of Hit/Kill Tables”¹⁶
- “Establishment of Force-on-Force Performance Test Working Group.”¹⁷

The VA Process Guide provides the VA analyst with the minimum process requirements/expectations (at the macro level). When the VA identifies a shortfall in protection measures, an analysis of possible upgrades to the security system is required. The upgrade may require deployment of new or upgraded security systems. To ensure that safety considerations of the upgrade are properly analyzed, a project team approach is applied. The shortfall in the protection measures is defined by the VA process in the form of a “problem statement” that the project team uses as the basis for identifying the most effective (from both a safety and security perspective) option for satisfying the problem statement. The security representatives on the integrated project team provide a briefing of the problem statement at the site and the known list of available technologies to the integrated project team (IPT).

If no known options are available a market search is conducted for technologies that may address the shortfall. If no options are identified to meet the objective, a development effort is required. The IPT would bring in the appropriate system development subject matter experts (SMEs) to design a concept that would meet the DBT for the application under consideration. Since no other alternative is defined in the initial assessment, once developed, the solution becomes the single solution, and the IPT can proceed to the “Selection of Security Systems” block in Figure 1. If there is only one option available to address the shortfall, the IPT can proceed to the “Selection of Security System(s)” block in Figure 1 and then submit the selection to DOE for approval of the selected security system. If multiple options are available, a formal alternatives analysis may be performed using a formal method, such as Kepner Tregoe and/or pairwise comparison (ref. Section 6). The alternatives analysis should result in a recommended security system or upgrade. DOE approval of the recommendation should be documented through a formal security evaluation report as noted in Section 8 of this report.

After selection of the system upgrade, a project execution plan should be developed (or refined if one was generated earlier) to procure, analyze, design, train, test, and deploy the new or upgraded security system. A change control process should be applied to the new or upgraded security system selection (ref. Section 10). Change control includes application of the USQ process to address the impact on safety and a security change control process to determine the depth of analysis required and the DOE approval requirements for the modification. It is recognized that the security change control process may need to be developed further at some sites.

In concert with the change control process, DOE and the contractor determine if the new or upgraded security system could be a 10CFR830 major modification to a nuclear facility (ref. Section 8.2). If DOE and the contractor determine that the new or upgraded security system results in a major modification to a nuclear facility, then a preliminary documented safety analysis (PDSA) is required and must be approved by DOE prior to procurement. The PDSA and its precursor document, conceptual safety design report (CSDR), are expected to be developed in concert with the design of the new or upgraded security system. The PDSA and CSDR define the safety features and the safety classification of those key features. Additionally, they establish design requirements associated with

the safety functions, such that the system is designed and procured to the appropriate standards. These documents and specific implementation requirements will be more fully described in DOE-STD-1189, Integration of Safety into the Design Process planned for RevCom in October 2006.

DOE documents approval of the PDSA through a safety evaluation report (SER), allowing procurement to proceed. DOE may approve limited procurement and construction as described in DOE-G-421.1-2, Implementation Guide for use in Developing Documented Safety Analysis to meet Subpart B of 10CFR830. As the security system is being installed, a DSA and technical safety requirements (TSR) for operation will be prepared. Prior to deployment of the security system, DOE must approve modifications to the facility DSA and TSR with an SER and any changes to security plans with a formal security evaluation report (ref. Section 8). Once the system is installed, training is complete, and the DSA and TSR changes approved, an integrated readiness review following the tenets of DOE O 425.1B, Startup and Restart of Nuclear Facilities, should be performed. The purpose of the readiness process is to ensure personnel, procedures, and equipment are ready to effectively and safely deploy the security system (ref. Section 9). The results of the security and safety evaluations should be posted within the data system toolbox to allow for portability to other sites (Section 7 provides the conceptual basis for the SIDS supporting this portability between sites).

A strong corporate culture and infrastructure supporting integration of security and safety disciplines are fundamental to a successful execution of a security project. Additionally, a clearly articulated management commitment to integration of the two disciplines is needed to ensure the easiest, quickest, and most successful implementation of the near-term DBT requirements.

Quality assurance requirements driven by the safety requirements may also be a factor in system selection and implementation. For example, security technologies that rely on software or firmware for safe/reliable implementation of the technology often have specific requirements that need to be addressed early in the technology development process. In these cases, quality assurance professionals need to be integrated into the team early in the planning process. Software verification and validation driven by the software quality assurance requirements of DOE N 203.1, Software Quality Assurance, may be a major factor in the project schedule and cost, and need to be addressed early. These software quality assurance requirements may also be a factor in the technology selected.

The standard project management process and principles should be used, but with assurances of involvement of a multi-disciplined team approach. It is important that the IPT include DOE representation from both disciplines. Key steps to ensure success include:

- Select a project manager to lead the effort
- Define clear lines of authority and responsibility
- Provide necessary resources (staff and funding)
- Use an integrated team approach, inclusive of applicable disciplines (e.g., facility operations, physical security, emergency response, protective force, risk management, legal, security and safety basis subject matter experts, and other safety and health disciplines)
- Identify and observe applicable rules, regulations, and requirements
- Use evaluative system engineering tools (e.g., alternate analysis/pair-wise comparisons) for optimizing both security and safety options
- Prepare a final report summarizing the selection process, clearly explaining the rationale, results, and conclusions
- Develop security system specifications (e.g., failure data, safety controls, capabilities, inherent hazards, and functional and operational requirements) supporting both design and safety analysis processes
- Develop and adhere to a realistic and achievable schedule with logic ties and deliverables.

As this process matures, a plan for the most effective implementation of each of these steps should be developed and documented.

The successful application of the integrated project management process is likely to result in conflicting

requirements/desires, necessitating the need to strike a rational balance between safety and security expectations. In these cases, productive communication between the stakeholders, including all applicable disciplines within the contractor and DOE organizations, is essential.

6. Alternative Analysis Process for System Selection

As described in Section 5, a key step for integration of safety and security, as well as selecting security technology, is to clearly identify the problem statement and the objective of the upgrade. This objective needs to be clearly stated and communicated among all IPT members. The objective is the compass for the IPT when evaluating potential alternatives. An alternative analysis approach is summarized below and presented graphically in Figure 2.

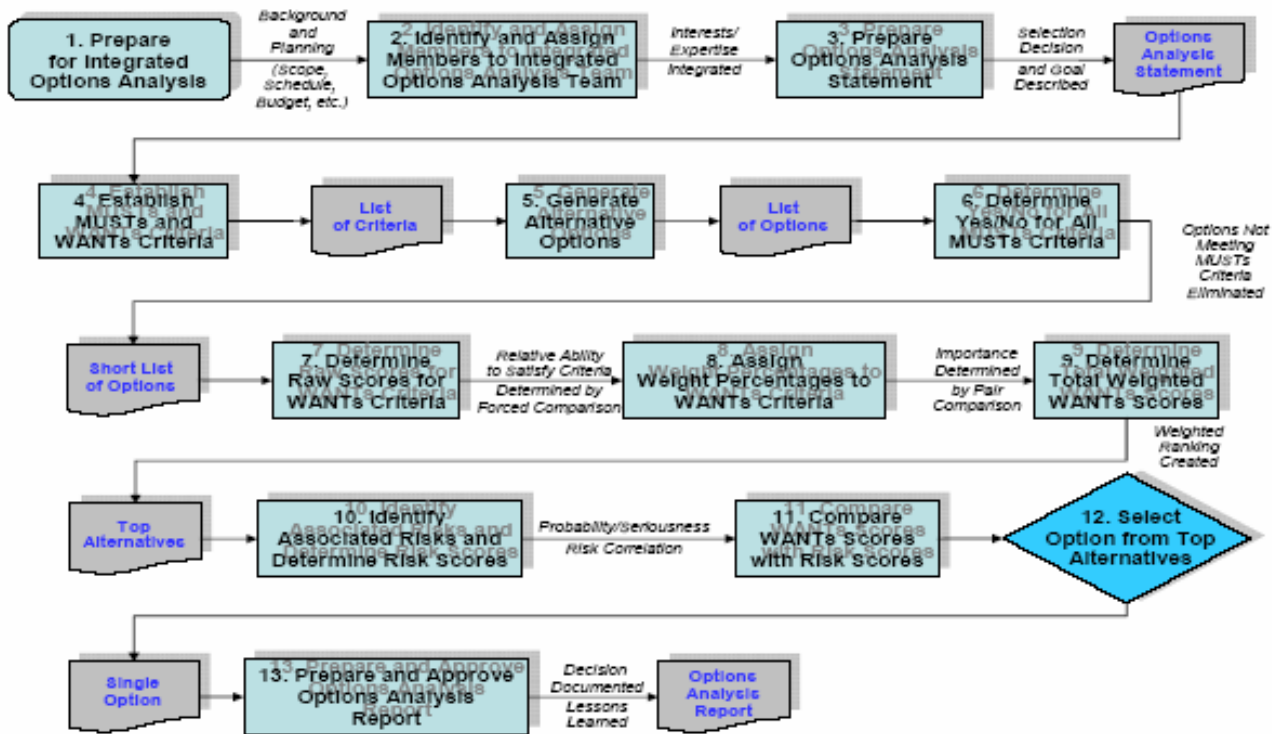


Figure 2 Integrated Options Analysis Process

Once the objective is identified, the project team establishes minimum acceptable requirements for all impacted stakeholders, requirements deemed important enough by the project team to eliminate a particular security technology from further consideration. Such requirements are referred to as “Musts” and are simple statements that when applied to a particular security technology a “Yes” or “No” answer may be obtained. The intent is to reduce the list of potential alternatives to only those that are credible as early on in the evaluation process as possible. Documentation of which specific security technologies failed to meet any of the “Must” criteria is key to developing a defensible selection process.

After the “Musts” are developed, the project team establishes desirability criteria for the security technology to meet the objective. These desired attributes are known as “Wants” and some potential alternatives will meet these better than others. As with the “Musts,” these “Wants” should include input from all stakeholders. They may be from a safety, security, or any other perspective deemed important by the project team. Rationale for the “Wants” along with creation of a “dictionary” provides a mutually agreed upon definition of the “Want” and helps to maintain consistency in terms will be valuable in making and documenting a defensible selection process.

Once the “Wants” are established, the project team develops a weighting system to determine the relative importance of each “Want.” This allows potential alternatives to be compared to one another, or “scored,” on the basis of how well they meet established “Wants.” The weighting system may be an overall comparison or a pairwise comparison of all “Wants.” Typically, an overall comparison is used for small numbers of “Wants” and a pairwise comparison for larger numbers. In the end, the project team needs to choose which system works best for their project.

After a clear objective is defined and “Musts” and “Wants” are established, a list of potential security technologies is developed. Typically, this is done by a small group of SMEs who are very conversant in the available choices. This process should be approached in a brainstorming spirit. That is, SMEs should not be allowed to immediately exclude or drop possible alternatives based on their subjective experiences or opinions. This exercise should be conducted with the attitude of, “What are all of the security technologies available, even those that have only a small potential of meeting the overall objective?”

Each of the possible alternatives is then evaluated against each of the “Must” criteria. As previously indicated, these criteria are a simple “Yes or No.” Alternatives that fail any single “Must” criteria are removed from further consideration. Documentation of the alternative and the specific criteria that failed is critical to the integrity of the selection process and later questions regarding the adequacy of the evaluation.

All alternatives passing the “Must” evaluation are scored using the weighted “Wants” criteria. All alternatives are then ranked according to their weighted score. From this, a short list of the top scoring alternatives is developed. Only those alternatives with similar scores are considered. More or fewer alternatives go onto the short list according to the similarities in scoring. Note that it may be important to look at attractive attributes of the second tier of candidates to see if modifications may be appropriate in the selected system that would have changed the outcome of the ranking process. Vendors may be willing to “improve” their design to accommodate the enhanced system configuration.

Relative risks of each alternative on the short list should be reviewed. The risks considered should include all aspects of each alternative. Examples may include impact to facilities, reliabilities, maintainability, etc. A preferred security technology can then be selected if the ranking and risk consideration reveal a single best alternative.

If the short list of the highest ranked alternatives and risks are considered similar, additional “Want” criteria should be developed. The additional criteria are weighted as necessary. However, in many cases, all additional criteria are considered equally important. Once the alternatives on the short list have been scored using the additional “Want” criteria, a final selection can be made.^a

A thorough but concise final report on the selection process should be prepared. The purpose of this document is to provide an easily understood explanation of the selection of a particular alternative from a number of viable alternatives. Professional judgment and opinions are valid justifications in the selections process so long as the logic and rationale are included to explain the thought process. The final documentation should include dictionaries or other documentation generated to build the decision making framework as appendices.

7. Security Systems Toolbox: Development, Data Capture, Data Sharing

The intent of the tool box process is to identify and provide information to sites within the complex to expedite procurement and deployment of security systems that meet applicable security and safety requirements. This process ensures that the following are accomplished:

- Identify data elements needed to develop a package of security system options
- Capture key decisions and relevant data used to approve a system
- Define information to be supplied by vendors/system developer
- Identify how DOE can pre-approve key features of security systems and make sure those features are portable to multiple sites with minimal additional evaluation
- Capture and/or update performance data for the security technology.

However, it is noted that site-specific or implementation-specific evaluations will always be required to assure that there are no interface issues at the site where the system is deployed. To develop the appropriate security system toolbox, the approach is developed in the following subsections.

^a As a side benefit, the establishment and weighting of “Wants” can also serve as a “team building” experience. This process allows team members to both be heard and see other perspectives. It emphasizes competing objectives and focuses on the importance of collective consensus decisions to achieve the best solution. An independent facilitator is important during these deliberations to guard against “group think” and to ensure that opposing views are heard and dispositioned. It is important to assure that the SMEs are solicited and heard by the team. It may be important for the independent facilitator to allow the discussion of the individual “Wants” to be in the team meeting, but have the actual weighting performed independently, with only the facilitator knowing the actual final weighting factors. This helps to assure the validity of the outcome of the evaluation. Issues that cannot be resolved should be elevated to senior management for resolution.

7.1 Develop Initial Data Sets

The initial data sets should come from reviewing the key security systems currently being implemented at various sites. Once that initial data set is captured, emphasis shifts to a team approach to identifying upcoming safety systems. For review of ongoing security systems, a lead/host site should be designated to establish security and safety analysis input information (ref. Section 7.5). Examples of analysis input information include control derivation, hazard and accident analysis basis, test and failure data, alternative analysis reports, product specifications, performance specifications, procurement specifications, design and installation packages, readiness process, etc.

A determination as to whether the system deployment would constitute a 10 CFR 830 major modification determination would be required. This would include impacts or design changes to existing facility systems to include safety significant or safety class systems, impacts to existing TSRs, safety class/safety significant control treatment, and quality requirements (including software). The initial systems to be addressed include:

- Dillon Aero, 7.62 AP, mobile and fixed platforms
- ROWS, 5.56 or 7.62 AP, mobile and fixed platforms
- MK-19, 40 mm
- Secure transport vehicles
- Inert gas systems
- Fixed foam systems
- Generic command and control system.

Additional systems and technologies are being assessed and can be added as appropriate. This includes systems and technologies that are ready for deployment and those being developed. Specificity for these elements is required as this process moves toward implementation.

In order to standardize and optimize the data capture performed by these security system review teams, a checklist should be developed as an aid. Potential ideas for the generic checklist of desired data elements include:

- Identify what data are portable
- Structural impacts and loadings, PC-2 or PC-3 design
- Accidental discharge analysis
- Hazard analysis
- White papers
- Development of positive USQ, evaluation of the safety of the situation, and addendum to DSA
- Training programs – standardized training
- Software quality assurance.

When a site hosts discussions on a particular system, the team sharing the data prepares and shares what they learned from the process in a final report, which will be used to populate the standing data base described below. Team reports and documents issued should prescribe processes and methodologies used, specify requirements, or establish design when items, services, and processes not currently used in the complex are identified.

An important aspect of maintaining the integrity of the database is independent peer review of the information placed into the database. To achieve this review and assure that the security system (and associated information) has the best portability to other DOE sites, it is recommended that entries receive an independent SME review, preferably from other sites. It is expected that this peer review may require personnel outside of DOE to achieve an appropriate level of scrutiny (e.g., Department of Defense). This peer review would require both safety and security professionals on the team. Thus, the review may have to be driven at the Central Technical Authority and Chief of Defense Nuclear Security Safety level of DOE to assure that appropriate SMEs are brought into the process.

7.2 Near-Term Systems Being Developed

As the focus is on the near-term deployment, the initial evaluation is based on anticipated security systems that can be fielded between now and 2008. This initial listing allows the team to determine any additional key security systems that may be used in meeting the current DBT, as well as driving security upgrades. A key element of this

evaluation is to determine which systems have the potential to be extended to other sites. An inventory of emerging security systems should be generated to ensure this common approach is applied early in the conceptual phase. By applying a standard approach and leveraging lessons learned from previously installed systems, it may be possible to shorten the design/approval cycle for the emergent projects. The inventory of emerging projects should be compiled from the upgrade actions defined in the various DBT Implementation Plans from the Office of Defense Nuclear Security and the Office of Energy, Science, and Environment. To ensure completeness, the effort should be coordinated with the Security Technology Deployment Programs of the Office of Security Technology and Assistance (HS-80) and the Office of Defense Nuclear Security (NA-70). When appropriate, interfaces with the Physical Security Equipment Action Group (PSEAG) and the Technical Support Working Group (TSWG) may improve collection of system performance and safety data.

As an added benefit, the database can also be used as a tool for security system developers to both review data for existing systems (including installed and available), as well as a guide for the data requirements and expectations for developing systems.

7.3 Data Sharing

Once gathered, it is important to share data with both the security and safety personnel at other sites to ensure viable options are known and options that failed are not repeated. The intent is that this information be placed on a controlled, electronically accessible platform that would allow personnel at the various sites to access the information as needed, but within the limitations driven by the security classification of the information.

To assure that the data is appropriate for use, a configuration management program needs to be implemented for the database. This should include a peer review of the information before it is available for use within the database.

It is expected that two levels of information will be provided in the database. First would be the primary data set that has the key verified information for the security technology. The second is a set of supporting or lower tier information that is available for consideration by a reviewer, but not as formal as the primary approved data set. This may include comments, test results, USQs, etc.

7.4 Standing Data Base

To be of use, data must be made available to multiple sites. This requires the creation and maintenance of an accessible data base at the classification level required to contain useful information and on an electronically accessible platform that is available to all sites. The scope of that data base should include the essential elements for key security systems currently deployed, security systems being developed (HQ point of contact), security systems being considered at various sites, and insights in development of DBT accident base case concepts that would envelop a variety of scenarios.

A targeted information checklist should be jointly developed by security, safety, and operations personnel for use in site data gathering and retrieval visits. This list can be refined as teams begin working together. Elements to be considered for this checklist include:

- Systems characteristics
- Key features for safety
- Derivation of administrative controls
- Issues found during approval process
- Options reviewed that were not of value
- System owner (i.e., host site).

Key issues that will need to be resolved include the host platform and location for the database, configuration control of the database, and classification level of the database. These issues should be jointly resolved with the safety team and security directors.

7.5 Lead Site Concept

Based on the implementation schedule and limited resources to develop needed security technology, the team proposes the use of a "Lead Site" or "Host Site" approach to deploying security technologies and developing the

information required for the safe deployment of the technology at the applicable DOE sites. The “Lead Site” would be the site that identifies the need for the technology and starts the development of the technology. Thus, a single site would be identified as the lead for a particular security technology and as host, solicit input and direct interaction from other sites with interest in the same security technology. This approach allows the combined resources of several sites to share information and build the needed security and safety information in the database that is intended to facilitate implementation of the technology at other DOE sites. This approach is expected to limit the analysis and development efforts to only that required for the specific deployment at the other sites and not force a total duplication of efforts. Key in this effort would be the joint effort in developing the procurement specification and essential elements of the technology. Additionally, the required safety controls in many cases may be directly transportable to the other sites that deploy the technology. To assure that this development effort is managed appropriately, NNSA/DOE-HQ would coordinate and manage this development effort.

8. Safety Basis and Security Documentation Integration

8.1 Discussion of Drivers and Their Implications

The selection or upgrade of a security system to meet the DBT involves identification of practical alternative systems that not only satisfy the security needs, but also consider characteristics such as operational efficiency, cost, and safety (exclusive of malevolent acts). As outlined in Section 6, this selection should be based on a disciplined documented analysis.

The security system selection process includes a security evaluation process to determine that the appropriate system is developed and deployed. Once a system selection has been made, it is necessary for DOE security offices to approve the choice. Approval may be accomplished by a security evaluation or other appropriate DOE approval mechanism. This DOE security approval mechanism is the security equivalent to the SER, providing DOE authorization (or conditional approval) to proceed with the security system procurement, installation, and deployment. Once approved by DOE, the security upgrades are identified in the SSSP and the DBT Implementation Plan.

It is also necessary to perform a USQ determination to assess the potential safety basis impacts of the proposed system. If required (i.e., positive USQ), DOE approval of changes to the facility safety basis must be sought. This is done through modifications to a facility DSA and TSRs, the approval for which is documented in a DOE-issued Safety Evaluation Report. Note that, as presented previously, if the change constitutes a 10 CFR 830 major modification, then a PDSA is required before the project can proceed with procurement and final design.

8.1.1 Safety Basis Implications

10 CFR 830 requires that facility hazards be analyzed and that hazard controls be implemented so that adequate protection is achieved for the public, workers and the environment. When a security system is put into place in a facility, accidental or unintended discharge could present a hazard to workers and/or the public.

Accidental or inadvertent discharge must be addressed for all credible scenarios. These events could be caused by human error, faulty security system design, or internal or external hazards. Examples of accident initiators that could actuate the security system and exacerbate accident consequences include facility events (e.g., fires) and natural phenomena hazards (e.g., seismic).

Moreover, accidental discharges could initiate accidents such as hazardous material releases, fires, nuclear criticality, leaks, or damage to safety SSCs or process systems. Depending on the characteristics of the security system and the facility, the installation could be considered a major modification of the facility. In that case, 10 CFR 830 would require the preparation of a PDSA and application of the nuclear safety design criteria of DOE O 420.1B.

Installation of a new system would trigger a comprehensive change control process. To address the impact on safety, the change would involve entering the USQ determination process and the modification of the facility’s safety basis to include consideration of the safety aspects of the new system. If the USQ determination is negative, DOE approval of the change would not be necessary for the safety review. If the security review is also negative, DOE approval of the change would not be necessary. However, it is recommended that a security configuration control process be employed for those systems deemed critical to the security posture (see Section 8.1.2). This

would include the essential elements of those systems.

Similarly, a security system deployed outside of a nuclear facility that had the potential of affecting facility safety as a result of unintended actuation would also trigger the USQ process. This would also require an analysis of those potential effects and the identification of safety controls that might prevent or mitigate the event.

8.1.2 Security Implications

The new or upgraded security system may also have implications in the security venue. A process involving change control, vulnerability analysis/evaluation, etc. culminating in DOE approval must be followed. It is essential that the security and safety basis processes be coordinated to ensure safe and secure operation of the proposed change without delays caused by the opposite review and documentation approval process. Implementation of the new or upgraded security system will require changes to facility specific security plans. An evaluation of impact to the existing physical security and/or administrative controls specified in the security plan must be completed. If an impact exists, then a revision to the security plan must be completed and submitted for DOE approval. DOE evaluates the acceptability of the revised control set and approve with or without conditions of approval. The basis for DOE acceptance of the physical and administrative controls should be formally documented in a formal security evaluation report. This security evaluation should document the review activities (i.e., facility walkthroughs, documents reviews, interviews, etc.), basis for recommended approval and/or basis for conditions of approval, criteria for acceptance, and the evaluation.

8.1.3 Safety Change Implications to Security

As security upgrades may impact safety authorization, any new or upgraded safety system may have implications in the security venue. A process involving change control, vulnerability analysis/evaluation, etc. culminating in DOE approval must be followed. It is essential that the security and safety basis processes be coordinated to ensure safe and secure operation of the proposed change without delays caused by the opposite review and documentation approval process. Implementation of the new or upgraded safety system may require changes to facility specific security plans. An evaluation of impact to the existing security physical and/or administrative controls specified in the security plan must be completed. If an impact exists, then a revision to the security plan is required to be submitted for DOE approval. DOE evaluates the acceptability of the revised control set and approve with or without conditions of approval.

8.2 Major Modification^b and USQ Considerations

In some cases the new or upgraded security system (i.e., change) may be considered a major modification in accordance with the Nuclear Safety Rule, 10 CFR 830. In these cases, the addition of the system potentially results in a significant change to the safety basis for the facility or facilities in which the system or upgrade will be installed. The implication of classification as a major modification is that a PDSA must be prepared and approved (through an SER) before the installation of the new system may proceed. The PDSA must show how the nuclear safety design requirements of DOE O 420.1B will be satisfied. This would include a description of the system and its installation, a hazard analysis and (if warranted) identification of safety controls, and classification of safety controls as Safety Class or Safety Significant, if appropriate according to the criteria for those designations. Upon installation, the facility safety basis would need to be modified to account for the new system and its safety controls.

Some of the issues that would need to be addressed are the controls indigenous to the security system, controls that may be required because of facility-specific conditions, design of the installation regarding seismic and fire hazards to the system that could affect inadvertent actuation, etc.

The PDSA requires DOE approval prior to procurement and installation of systems and components. Creation of the PDSA requires significant interaction among the safety basis project team and security to ensure proper integration and coordination. More definitive guidance on the treatment of major modifications is being developed as part of DOE-STD-1189 "Integration of Safety into the Design Process," which is planned for RevCom in October 2006.

The determination of whether or not a major modification is appropriate to characterize the change is typically a

^b Major modification will be clarified by DOE-STD-1189, *Integration of Safety into the Design Process*, scheduled for REVCOM in October 2006.

challenge requiring the involvement of DOE. The USQ process is helpful in answering this question. If the USQ determination is positive, then discussions with DOE should commence and a consensus reached as to whether declaration of a major modifications and preparation of a PDSA are necessary. The comprehensive change control process is then followed to ensure integration and updates to both the safety and security bases. The completed PDSA would be submitted to and approved by DOE.

If a PDSA is not necessary to properly address the proposed change, a comprehensive change control process would still be followed including updates to both the safety and security bases. In this case, since a PDSA is not necessary, procurement and design activities could proceed after DOE approval, based on a safety analysis that demonstrates adequate safety for the installation.

There is also the possibility that a USQ determination of a proposed change could be negative, that is, there is no USQ. This could be the case when there is an existing security system, and the proposed change does not present new safety issues that were not previously considered for the initial installation. In this case, the change could be made on the contractor's authority. However, both the safety and security documentation needs to be updated to reflect the changes.

8.3 Hazard and Accident Analysis Process

DOE-STD-3009, Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analysis provides appropriate guidance for hazard and accident analysis involved in assessing a security system deployment.

One of the first steps is to decide what type of safety evaluation is to be performed. The site practice for hazard analysis ("What-If", HAZOP, etc.) should be used to assess this change. Obtaining concurrence from DOE on the selected approach is suggested. It is also important to determine the extent of facility involvement in the proposed change. Prior to any meetings to discuss the impacts of the change, discussions should be held with security professionals and SMEs to accurately define the proposed change, identify any inherent safety features of the system, and identify key installation requirements.

Analysis sessions are held with the project team, including, as appropriate, nuclear criticality safety, facility safety, facility operations, fire protection, and security personnel familiar with the system. The project team would follow the selected hazard analysis approach to address the hazards and potential accident scenarios resulting from the new or upgraded security systems. There are typically several sessions with the project team to cover a comprehensive set of internal and external initiating events. Planned activities associated with the security system, both internal and external to impacted facilities, should also be considered. Inherent safety features associated with the new or upgraded security system are also considered to ensure that a comprehensive analysis/evaluation is performed. The session outcome is a formal document presenting the process, discussing the resulting hazards and accident scenarios including estimated frequencies and consequences to workers and the public. A set of recommended safety controls appropriate for preventing/mitigating event consequences is also provided and is the key result of the analysis. The specific controls provided with the security system could receive special designation in this document, if appropriate.

8.4 Derivation of Controls

With respect to the proposed change and within the context of the safety basis process, it may be necessary to designate specific controls (engineered or administrative) in the safety basis to prevent or mitigate the event of concern (e.g., accidental discharge). The controls could be specific safety SSCs consisting of passive and/or active features ensuring safe operation and preventing inadvertent actuations. Some of these controls will probably be inherent with the design and installation of the proposed security system. Acceptable controls may include safety management program elements ensuring safety during routine activities, as well as training exercises with the security system. The control set or sets would flow directly from the hazards and accident analysis process into the safety basis (i.e., the DSA and TSRs). If the controls are passive or active they would be included in the TSRs as Design Features, Limiting Conditions for Operation (LCOs), or Administrative Controls. If safety management programs suffice, then the programs would be summarized and the salient features emphasized in the TSRs.

8.5 Security Information Protection

It is very likely that some of the security system information necessary for the safety basis documents (DSA and

TSRs) would be classified with access provided on a “need to know” basis. This could be accomplished by having a classified addendum to both the DSA and the TSR documents. The DSA addendum might have the elements of the system description that need protection. The TSR addendum might have the elements of the hazard control set that would be the responsibility of the security element to implement. The list of “need to know” personnel, however, includes the Facility Manager and designees. It is ultimately the Facility Manager’s responsibility to ensure that operations are conducted according to the facility safety basis and also to be aware of any proposed changes to the safety basis, as reflected in the classified addendum.

9. Post-Installation Readiness

After installation of physical security systems, an appropriate level of review needs to be conducted to ensure that the security features will be available when needed and ready to function as designed. In addition, the review needs to ensure the safety features related to the security system are installed, ready to operate, and available when called on. The level of review can be graded based on the significance of the installation as long as the review covers these key features. Use of existing readiness review processes in place at the site is encouraged.

Essential elements associated with security systems require routine testing of the system to ensure operability. Security system testing requirements should be identified during the system selection process and documented in the project execution plan. Additionally the testing requirements are documented in the SSSP and in a formal Performance Assurance Program Plan as required by DOE security directives.

In addition to reviewing physical security systems, when the safety controls related to security are administrative in nature, the review needs to ensure appropriate procedures, training, and other activities are in place and effective.

DOE O 425.1 C,¹⁸ “Start and Restart of Nuclear Facilities,” is applicable for new nuclear facilities and modifications following shut down of a HC-1 or HC-2 nuclear facility. The requirements of this order specify a readiness review process that must, in all cases, demonstrate that it is safe to start (or restart) the applicable facility. It is also required for new HC-3 nuclear facilities. The order should be reviewed for applicability when deploying security technologies and for modifications within a nuclear facility.

10. Configuration Control

Configuration (change) control for security systems should be managed by a rigorous process that includes determination of approval authority. Over the past decade a safety basis configuration control process has matured, covering structures, systems, and components and associated technical basis documents and administrative procedures. A configuration control process to manage security approvals and changes initiated to meet the DBT are also required.

Engineered systems for security projects/changes should be treated like any other project or change, including designation of a design authority representative and/or system engineer. SME reviews are applied when necessary using a graded approach and facility operational safety reviews (or equivalent) include representatives from security.

All facility changes (including security-related changes) affecting Hazard Category 1, 2, and 3 nuclear facilities must be subject to the USQ process. Changes to security plans or facility changes that affect security should be subject to an evaluation process to determine approval authority for the change. Configuration control for security changes should be owned by the line organization with DOE providing formal approvals in a form of documents similar to the SERs used for safety basis documents. The rigor of the change control process may be linked to the security designation for the facility (Threat Level 1 - 4). A listing could be posted on a master list (possibly web-based) to identify the latest approval and effective documents.

While configuration control applies in a graded manner to aspects of change to nuclear facilities, it is the implementation procedures that actually flow down the process by triggering change packages and multi-discipline safety and technical reviews (including security and safety representatives). Figure 3 depicts application of the USQ and Security Change Evaluation processes within the configuration control program. Authority to proceed with changes is contingent on execution of both the USQ and Security Change Evaluation processes. These processes include DOE approval if the change could place a facility or activity outside its safety basis or security plan.

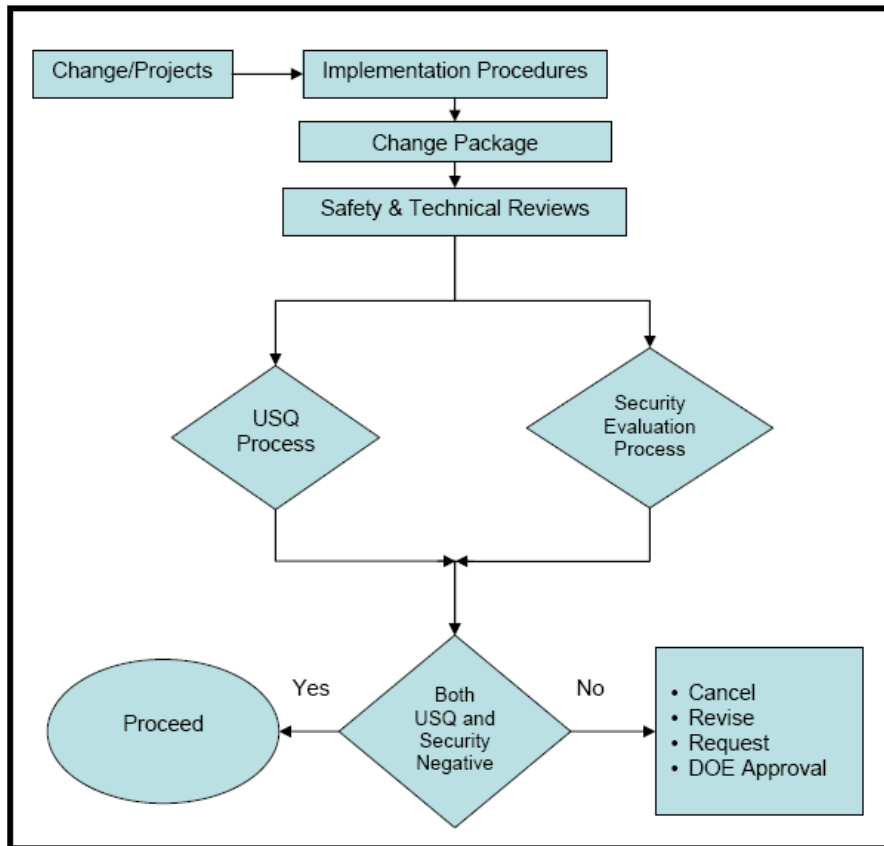


Figure 3 Security and Safety Change Process

11. Review Process for Improvements and Lessons Learned

The intent is to assess this process against the transfer of information for security system deployment between Y-12 and INL. This assessment will be used to benchmark the process presented in this report. Follow-on implementation will provide additional feedback to the process as well as populate the security system database/toolbox. The intent is that while the database is populated, the participants provide feedback that facilitates continuous improvement in the process. It is proposed that an annual integrated review be held with interested participants from security and safety to overview the current process and assure that it is providing the intended benefit to the sites. As this review depends on DOE’s implementation of these recommendations, it is suggested that the scope of the reviews be defined along with the implementation program(s).

12. Summary

A cost effective, comprehensive process has been developed to simultaneously satisfy DBT and safety basis objectives for security systems. This approach is intended to facilitate sites meeting the defined dates to satisfy the DBT. An integrated project team approach has been proposed that contains multiple interrelated elements/processes. Figure 1 lays out the overall process. A key element of this process leading to cost savings for individual facilities is the toolbox approach that makes systems and key information transportable between facilities and sites and accessible by multiple DOE sites for review and use. The toolbox will be populated with pertinent SIDS information that includes safety basis and security data for various security systems, including system evaluation and approval documentation. These data may be used as part of the information set required to obtain approval to deploy similar security systems at several sites.

For this process to be successful, safety and security professionals from around the complex and at DOE-HQ need to actively seek to understand the parameters under which their counterparts work and possess a contextual understanding of the terms of art used by their counterparts.

References

1. DOE O 470.3A, "Design Basis Threat Policy," U.S. Department of Energy, 11/29/2005.
2. DOE O 470.4 "Safegaurds and Security Program," U.S. Department of Energy, August 26, 2005.
3. "Salient Considerations of the Design Basis Threat Annex Special Evaluation Team," from William J. Desmond, Administrator for Defense Nuclear Security/Co-Chair, Annex Special Evaluation Team NNSA, and Larry D. Wilcher, Director, Security Policy Staff/Co-Chair, Annex Special Evaluation Team Office of Security, June 25, 2004.
4. 10 CFR 830, "Nuclear Safety Management," *Code of Federal Regulations*.
5. DOE O 420.1B "Facility Safety," U.S. Department of Energy, December 22, 2005.
6. DOE-STD-1189-2006, "Integration of Safety into the Design Process," U.S. Department of Energy, Draft.
7. 10 CFR 851, "Worker Safety and Health Program," *Code of Federal Regulations*.
8. "Adversary Capabilities List (ACL) - Terrorist Adversary Capabilities List," from Linton Brooks, Under Secretary for NNSA and Robert Card, Under Secretary for Energy, Science, and Environment, February 18, 2004.
9. "Vulnerability Assessment Process Guide," from Marshall Combs, Director, Office of Security, Office of Security and Safety Performance Assurance, September 30, 2004.
10. DOE O 470.4-1, Chg1, "Safeguards and Security Program Planning Management," U.S. Department of Energy, August 26, 2006.
11. DOE Manual 470.4-2, Chg1, "Physical Protection," U.S. Department of Energy, August 26, 2006.
12. DOE Manual 470.4-3, Chg1, "Protective Force," U.S. Department of Energy, August 26, 2005.
13. DOE Manual 470.4-6, Chg1, "Nuclear Material Control and Accountability," U.S. Department of Energy, August 26, 2005.
14. "Consolidated Guidance Concerning the Required Format and Content for the Design Basis Threat Implementation Plans and Quarterly Updates," from Glenn S. Podonsky, Director Office of Security and Safety Performance Assurance, February 1, 2005.
15. "2004 Design Basis Threat Implementation Plan Vulnerability Assessment Requirements," from CDR Robert F. Brese, USN, Acting Director, Office of Security Oversight, November 16, 2005.
16. "Modified Probability of Hit/Kill Tables," from the Office of the Associate Administrator for Defense Nuclear Security (NA-70), December 16, 2005.
17. "Establishment of Force-on-Force Performance Test Working Group," from Glenn S. Podonsky, Director, Office of Security and Safety Performance Assurance and William J. Desmond, Associate Administrator for Defense Nuclear Security, May 16, 2005.
18. DOE O 425.1 C, "Start and Restart of Nuclear Facilities," U.S. Department of Energy, March 13, 2003.