WASTE MANAGEMENT FRAMEWORK
TO MITIGATE TERRORIST INTRUSION ACTIVITIES

Kenneth S. Redus
Redus and Associates LLC
189 Lafayette Drive, Suite C
Oak Ridge, TN 37830 USA

ABSTRACT
A policy-directed framework is developed to support US Department of Energy (DOE) counterterrorism efforts, specifically terrorist intrusion activities that affect of Environmental Management (EM) programs. The framework is called the Security Effectiveness and Resource Allocation Definition Forecasting and Control System (SERAD-FACS). Use of SERAD-FACS allows trade-offs between resources, technologies, risk, and Research and Development (R&D) efforts to mitigate such intrusion attempts. Core to SERAD-FACS is (1) the understanding the perspectives and time horizons of key decision-makers and organizations, (2) a determination of site vulnerabilities and accessibilities, and (3) quantifying the measures that describe the risk associated with a compromise of EM assets. The innovative utility of SERAD-FACS is illustrated for three integrated waste management and security strategies. EM program risks, time delays, and security for effectiveness are examined to demonstrate the significant cost and schedule impact terrorist activities can have on cleanup efforts in the DOE complex.

INTRODUCTION
The Security Effectiveness and Resource Allocation Definition Forecasting and Control System (SERAD-FACS) is a policy-directed framework that supports US Department of Energy (DOE) counterterrorism efforts, specifically terrorist intrusion activities that affect of Environmental Management (EM) programs. SERAD-FACS identifies the trade-offs between resources, technologies, cost and risk, and Research and Development (R&D) efforts for integrated DOE waste management (WM) and security programs. The intended audience is decision makers at senior levels of the DOE. SERAD-FACS is designed to support the three missions of the Department of Homeland Security (DHS): (1) prevent terrorist attacks within the United States, (2) reduce America's vulnerability to terrorism, and (3) minimize the damage and recover from attacks that do occur. The SERAD-FACS framework is designed to couples DHS organizational goals with the DOE EM cleanup program missions to ensure consistent policy development for site security, emergency preparedness and response, and employment of Chemical, Biological, and Radiological (CBR) and Nuclear countermeasures [1].

SERAD-FACS is also structured to meet the requirements of DOE Integrated Safeguards and Security Management (denoted as ISSM and as prescribed in DOE Policy 470.1 and DOE Order 470.1, [2]), namely “provide an information baseline for use in integrating complex-wide safeguards and security considerations, facilitate managers' evaluation of program elements and resources for needed improvements, and establish cost-benefit bases for analyses and comparisons.”

ADDRESSING THE OVERARCHING ISSUES
SERAD-FACS creates the bridge for the integration of DOE ISSM with WM and EM cleanup programs. The rationale for creating SERAD-FACS is illustrated in the following example.
Situation: A low-level waste landfill is used by the EM program. Each fiscal year, several hundreds of million dollars are budgeted to clean-up projects and to the landfill operation. ISSM requirements are funded at thousands of dollars and are met per prescribed DOE orders.

Disruptive Event: A successful terrorist intrusion at the landfill occurs. A conventional device is detonated at the landfill operational area (for example, a shape charge is tossed over the fence at the landfill boundary and detonates). The chance of such an attack occurring is actually quite small, but the risk and the consequences may be significant. Risk is quantified by the product of the expected cost of the event and the likelihood that ISSM responses to the event fail.

Consequences: If the situation was a “classic” DOE security issue, namely, if only protection of the landfill operational area was the primary concern, the risk and consequences associated with failure is on the order of thousands of dollars. This is not, however, the situation. We are dealing with an integrated WM and security scenario:

- The fundamental integrated WM and security issue is whether the risk is thousands of dollars or hundreds of millions of dollars.
  - At one extreme, suppose the landfill re-opens immediately after the attack. DOE ISSM oversight and performance assurance would legitimately require assurance from EM project management that security controls were in place and would be successful against future events.
  - At the other extreme, if the landfill is unavailable for a significant period of time, EM projects will slip in schedule or use alternative disposition locations at a cost of millions of dollars.

- Since the EM projects are multi-year efforts, the EM life cycle budget is clearly disrupted.

Several national requirements mandated the creation of SERAD-FACS by Redus and Associates LLC.

- The newly created DHS recognizes the nation needs a more robust and unified homeland security structure, and this will necessarily include US DOE security oversight and assessment [1, 4].

- A significant body of literature, tools, and techniques exist for personnel, physical, information, nuclear safeguards, and cyber security system effectiveness analyses, but these are directed primarily at access to classified sensitive material [5].

- The DHS Directorate of Science and Technology will have an annual budget in excess of $500 million. DOE Office of Science programs at Los Alamos National Laboratory, Sandia National Laboratory, and Lawrence Livermore National Laboratory will be absorbed into this directorate [6].

- Integration of security and waste management programs to meet risk management and “graded protection” requirements is less than optimally performed in the DOE complex. While DOE routinely performs national laboratory security review and oversight, there is no single information system maintained by DOE and the labs that contains information on all the safeguards and security findings [7].
OVERVIEW OF THE SERAD-FACS FRAMEWORK

The SERAD-FACS framework is based on current independent and previous research by the author [8, 9, 10, 11, 12]. Recent products produced by RAND Corporation dealing with defense/security integration and refinement offer keen technical bases for the structure of SERAD-FACS [13, 14].

The architecture and logic of SERAD-FACS is based on systems engineering and analysis methods. Key questions are addressed for relevant themes. The controls that affect implementation of the process are identified and their effects quantified. The mechanisms used to implement the process are developed, the policy development process is articulated and implemented. Using a SERAD-FACS approach, policy outputs and results are determined. Listed below are the key questions for addressed by SERAD-FACS:

Themes: What are the WM/Security objectives and rationales?
Controls: What is the current context, and what are the capabilities of existing strategies? What are the views and perspectives of the players involved in WM/Security policy?
Mechanisms: What are the expected futures of WM and Security?
Process: What provisional paradigms should be created over selected time frames of interest?
Results: What are feasible policy portfolios and how should resources be allocated?

The SERAD-FACS Framework is presented in Figure 1. Each aspect of implementation of SERAD-FACS is discussed, and this discussion sets the stage for a specific illustrative example.

![Fig. 1 Top Level View of SERAD-FACS Framework](image-url)
Themes - Identify Integrated WM/Security Objectives and Rationales

There are many themes that form the basis for integrated WM/security policies. These themes have both a strategic (long-term) and an operational (short-term) emphasis. The themes are preferences dictated by multiple and overlapping objectives and rationales. In fact, the preferences by themselves address only particular aspects of integrated WM/security policy. Independence of the themes would be desirable. Since they overlap in context and form, a policy portfolio that addresses the themes will require multiple strategies. Three illustrative themes of an integrated WM/Security policy are:

- **Theme 1: Protection is Everything** – Security and response force structures/procedures form the environment in which each, and every, DOE EM project must operate. Under this theme, for example, if there is any risk whatsoever to an EM asset, maximum security operations are put into place.

- **Theme 2: Innovative Alternatives** – “Out of the Stadium” preferences are the rule rather than the exception. Innovative alternatives include, for example, federal acquisition and implementation of dedicated secure transportation infrastructures (roads, rail, air, etc.) that are put into place for all waste planned for disposition at the Yucca Mountain repository and the Waste Isolation Pilot Plant.

- **Theme 3: Security in Cleanup** – All EM projects, to include clean-up operations and WM activities, are closely coupled with site security on a project-by-project basis. Security in cleanup would necessitate that all EM projects take on the qualities of exclusion areas with appropriate security measures in place.

Control #1 –Identify the Current Context and Capabilities of Existing Strategies

The many current context and capabilities represent qualitative and quantitative expressions of current, in-place, WM and security objectives, rationales, and approaches. No single capability or contextual situation defines new or alternative integrated strategies. For example, existing DOE security contexts are directed toward protection of nuclear assets. Capabilities may employ unmanned reconnaissance systems; however, such capabilities are not being applied during waste management treatment and disposal operations.

Control #2 –Identify the Views and Perspectives of the Players

It is a fact of life that under the current context and the current capabilities, there are multiple views of and perspectives of the players (stakeholders) involved. Since the issue is how to integrate WM and security, this control is actually an articulation of constraints of how integration can be accomplished. Desires, independent of possible futures, are identified by the players. Consider, for example, the Innovative Alternatives theme. Part of this theme includes the notation that dedicated secure transportation infrastructures would be used for Yucca Mountain and WIPP disposition. Call this the “Radius Control” attribute of this theme. Players include, at a minimum, multiple federal agencies (Department of Transportation, DHS, etc.), tribal nations, state and local governments, and the general public. The players’ views and perspectives may actually not even be formulated for the notion of an integrated WM and security policy.

Understanding the views of the players can lead to an initial identification of binding constraints, flexible constraints, or constraints that require legislation in order to adequately address the theme of interest. A simple example is federal acquisition of all transportation routes within a 100 mile radius of Yucca Mountain, WIPP, and within a similar radius of all potential DOE generator sites. At the least, DOE
ISSM policies and orders, regulatory agency statutes, and tribal and local concerns clearly are needed to understand the views and perspectives of affected players in this case.

**Mechanism – Identify Future Security and WM Environments**

Several future environments act as mechanisms affecting the creation of provisional paradigms that describe integrated WM and security portfolios. Scenarios are developed and modeling or simulation requirements for various integrated WM and security environments are identified. Environments may include economic, stakeholder, operational, or organizational systems. These serve as the basis to test the provisional paradigms against the drivers of the future security environment, the future WM environment, or both. The result is the relevance and feasibility of each provisional paradigm. Based on those tests, they can then be refined. For example, unique scenarios would be developed for the “Radius Control” attribute of the Innovative Alternative theme.

**Process – Create Provisional Paradigms over Multiple Time Frames**

Key to SERAD-FACS is the identification of: (1) paradigms for which strategies or resources do not currently exist (conceptual or embryonic), (2) paradigms for which ill-defined strategies exist with many resources (inefficiencies), (3) paradigms for which well-defined strategies exist and with no resources (scarcities), (3) paradigms for which well-defined strategies exist and with resources in-place (Research, Development, or Testing), or (5) paradigms for which well-defined strategies exist with resources in-place (operations). For example, the gap in the “Radius Control” attribute of the Innovative Alternative theme is that the physical infrastructures do not exist on a national scale, and such an operational and social public infrastructure is not in-place.

**Result #1 – Create Feasible Strategy Portfolios**

Groupings of provisional paradigms allow us to create candidate portfolios. These portfolios may require resource management including “where to invest resources, where to divest resources, and where to maintain existing capabilities” [14]. Portfolios may overlap; for example, a set of feasible strategies may be created using thematic elements from Innovative Alternatives and Security in Cleanup. This is illustrated as regional security forces attached to transportation infrastructures with hand-off similar to interstate trucking operations.

**Result #2 – Allocate Resources, Technologies, R&D Efforts, Cost, and Risk**

Given feasible strategy portfolios, a variety of resource allocation technical approaches may be employed to balance, as required, resources, technologies, R&D efforts, cost, and risk. Included are: Six-Sigma tools [15], applicable regulations and regulatory guidance [3, 16, 17], and econometric and operations research approaches [18, 19].

**AN EXAMPLE OF FORECASTING AND CONTROL IN SERAD-FACS**

Central to SERAD-FACS is its forecasting and control function. US Environmental Protection Agency (EPA) Data Quality Objectives (DQO) process and Data Quality Assessment (DQA) approaches are employed as applicable [16, 17], and these processes/approaches are defensible for DOE audits and reviews.

All outputs of SERAD-FACS meet proven logical requirements (identify qualitative and quantitative statements that clarify study objectives, define types of data to be collected, specify decision rules, specify
the tolerable levels of decision risk (α-error and β-error), and define defensible testing or sampling design to support data collection to meet forecasting and control objectives).

Unique to the SERAD-FACS forecasting and control function is the explicit inclusion of DOE ISSM requirements [2] and Six-Sigma approaches [14]. Coupling these requirements with DQO/DQA quality management ensures the highest probability of correct forecasting and control definition and implementation. Figure 2 illustrates the generic structure and also the detailed approach employed.

Fig. 2 Generic Structure of Forecasting and Control in SERAD-FACS Including Detailed Approach

An illustrative example, Figure 3, is presented to illustrate one significant aspect of forecasting and control: the evaluation of a set of provisional paradigms (Protection is Everything, Innovative Alternatives, and Security in Cleanup). The context of the example presented earlier is used in this discussion. The example was developed using @Risk [20] and is planned to be finalized using GoldSim [21].

- For ease in discussing the example, consider each provisional paradigm as well-defined in an integrated security and WM universe.

- The future security and WM environments are based the plausible event associated with protecting the landfill from land or air attack using physical security systems (PSS) and air defense interdiction perspectives. PSS system reliability ranges from 99.99% reliable to 100% reliable for all paradigms. Air defense system reliability uniformly ranges from 50% reliable to 100% reliable for Security in Cleanup and uniformly from 95% reliable to 100% reliable for the other two paradigms.
Integrated security and air defense perspectives form the basis to examine (1) leakage (intrusion success), (2) fratricide (security force attrition due to mistakenly identifying security personnel as intruders), and (3) the integrated security and WM system reliability to succeed in meeting the paradigm.

Blue force size is 100 for Protection is Everything and 30 for the other two paradigms. Red force size is 30 in Security in Cleanup and 7 for the other two paradigms. Force sizes follow uniform probability distributions.

Three log-Poisson stochastic events disrupt each paradigm conditioned on the timeframe in which the paradigm is defined, specifically, the landfill operational life-cycle. There are three time periods for each paradigm: recovery, increased security funding, and decreased clean-up funding. The cost of disruption is proportional to (1) the probability of successful PSS and air defense performance, (2) the current time period of the paradigm, and (3) the log-Poisson disruptive event.

Three outputs are calculated:

- Risk is the product of the expected cost of the event and the likelihood that responses to the event fail.
- Duration is the total time associated with all disruptive events occurring.
- Fratricide is the number of friendly kills per 100 engagements, and leakage is the number of intruders surviving to accomplish the intrusion.

The marginal contribution of key variables that influence each of the outcomes are determined.
The results of the simple example are presented in Figure 4 with the following observations:

- The ordered risks (maximum to minimum) are Protection is Everything, Security in Cleanup, and Innovative Alternatives. Risk is increased by 3% to 5% for every 1-standard deviation decrease in the combined security and WM system success probability during the time period (recovery, increased security funding, and decreased clean-up funding) of intrusion.

- All time periods in which the disruptions occur are statistically significant in terms of effect on risk. The percentage increase of risk ranges from 18% to 30%. Since the Protection is Everything paradigm emphasizes security at the expense of cleanup, we easily see how the cost of not performing EM projects is added to the risk. Suppose a risk greater than $1000K constitutes infeasibility; then all paradigms are feasible. If, however, risk feasibility is less than $500K, then Protection is Everything is no longer a feasible paradigm.

- The ordered durations (maximum to minimum) are Protection is Everything, Innovative Alternatives, and Security in Cleanup. Since we are operating in an integrated environment, the duration of the EM cleanup continues to decrease as the paradigms tend to integrate security and WM activities and are significantly affected by the time period of intrusion. Suppose duration greater than 20 years constitutes infeasibility; then all paradigms are feasible. If, however, duration feasibility is less than 10 years, then Protection is Everything is no longer a feasible paradigm.

- Finally, fratricide and leakage tend to decrease in the order of Protection is Everything, Innovative Alternatives, and Security in Cleanup. This is reflected since the paradigms are integrating security and WM activities. Suppose a fratricide greater than 10 kills per 100 engagements constitutes infeasibility; then all paradigms are no longer feasible. If, however, fratricide feasibility is less than 20 kills per 100 engagements, then all paradigms are feasible.

![Figure 4 Output of Illustrative Example](image)

We can conclude:

- The greatest risk, impact on EM cleanup duration, and fratricide and leakage rates are with the Protection is Everything paradigm.

- Innovative Alternatives is preferred to Security in Cleanup for duration and fratricide and leakage, but it is has greater risk than Security in Cleanup.
SUMMARY

A policy-directed framework such as SERAD-FACS as developed by Redus and Associates LLC is needed by the DOE to identify the trade-offs between resources, technologies, risk, and R&D efforts for integrated security and waste management. We have provided the overall framework of SERAD-FACS and an example that demonstrates the impact on EM cleanup when security is not integrated with WM.

Using the SERAD-FACS framework allows DOE to support the DHS missions: prevent terrorist attacks within the United States, reduce America’s vulnerability to terrorism, and minimize the damage and recover from attacks that do occur. Equally as important, SERAD-FACS offers DOE the opportunity to identify and understand whether future integrated security and WM policies will put millions or hundreds of millions of dollars at risk, and armed with this information, manage and understand the subsequent dramatic slippages in EM schedules.

REFERENCES


