# Savannah River Site Levels of Control Implementation

Robert R. Lowrie and Edward Murphy (WSMS)
Andrew M. Vincent, III (WSRC)

**Abstract**

The Savannah River Site (SRS) established a prescriptive approach to defining and protecting major contributors to defense in depth in the mid '90s. This approach came in partial response to DNFSB criticism at the time of inconsistent classifications between similar facilities at the site. This basic approach of a rigorous and prescriptive minimum definition of levels of control has been in place since that time. Recently SRS has changed its policy of defining major contributors to defense in depth to be a more qualitative approach, with no prescribed minimum number of levels of control. However, to assure that consistency is maintained, guidance has been developed to identify areas of attention when identifying the major contributors to defense in depth that receive the Safety Significant functional classification label or that are protected within the TSRs. This paper discusses this guidance and its implementation within the overall hazard analysis and functional classification process.

## Why an initial prescriptive process?

To understand the background behind the guidance provided for control selection, it is important to understand the drivers that lead to the initial prescriptive process used at SRS. In response to two competing and mutually exclusive conditions and criticism from the DNFSB, a single and consistent set of rules was required. First, in the early 1990s DOE was tying to establish a set of rules associated with control selection. These were based on proposed DOE standards 3005 and 3009, both of which were in development. Several Savannah River Site facilities were trying to start or restart under a revised Authorization Basis that needed a standard from which to select controls. With the lack of specific DOE direction as to how safety controls should be selected and the added issue of the DNFSB pointing out inconsistencies in the controls selected for similar hazards and event scenarios at different facilities on the same site, SRS adopted two concepts. First, was the concept of identifying safety functions and both specifying applicable requirements and classifying the SSCs that perform those functions (i.e., Functional Classification). Second, was the concept of Levels of Control (LOCs). An LOC included all SSCs and Administrative Controls that were required to demonstrate that the proposed event scenario would either be prevented or mitigated based on a prescriptive set of rules. These two concepts provided assurance that the controls set described in the facility safety basis documentation would appropriately cover the safety basis accidents and with the prescriptive selection process that the solutions for similar types of hazards would have a similar level of protection provided. SRS then used this process to successfully start or restart a large number of hazardous facilities.

## What changed?

The primary changes that drove change in this program were associated with improved (more clear) direction from DOE as to the appropriate control selection processes and experience with working with the prescriptive control selection process for 10 years. The DOE standards and guides have recently provided a more complete statement of the expectations for major contributors to defense in depth and the separation between major contributors to defense in depth and SSCs and ACs that provide defense in depth but are not classified as SS. A second factor is that over the last 10 years of starting or restarting facilities at SRS significant experience has been gained in the expectations for the controls required for facilities of various types and risks. That experience provides a solid basis from which to move to a more qualitative process for selecting major contributors to defense in depth.

## What now?

The basic premise of the control selection process at SRS (i.e., the concepts of first identifying needed safety function and then assuring completeness of the control by identifying a Level of Control) remains unchanged. The selection process first identifies the needed safety functions and then identifies the most advantageous method to provide that safety function, which allows clear definition of applicable requirements and identification of the appropriate set of SSCs and administrative controls for protection within the TSRs and of SSCs that will be functionally classified. This second clear definition of the administrative controls and SSCs required to perform the needed safety function as a significant contributor to defense in depth is captured within the level of control (LOC) approach. However, the previous prescriptive nature of the control selection process has significantly changed. Prescribed LOCs for worker protection and defense in depth have been replaced by an informed qualitative approach to selecting these controls.

The primary driver for the initial prescriptive process remains unchanged at SRS and is likely the same at most large DOE sites with multiple facilities of various hazard types and risks. That driver is the need for a process that facilitates consistency in control selection. The DOE direction in this selection process is essentially limited to guidance in DOE-STD-3009:

> *Distinguish safety-significant SSCs from among those structures, systems, and components contributing to defense in depth. To effectively use the graded approach concept, focus on the most important items of defense in depth whose failure could result in the most adverse uncontrolled releases of hazardous material. This Standard maintains that all SSCs with a safety function do not require classification as equipment requiring detailed description in the DSA (i.e., safety-class SSCs and safety-significant SSCs).*
>
> *The major features of defense in depth typically comprise the outer or predominant means of mitigating uncontrolled release of hazardous materials…*

Implementation of this guidance has primarily been based on an expert team approach to determining the correct answer. As long as the same group of people make the selections in all cases, there is better than a 50/50 chance of getting similar answers for different facilities.

However, for large sites with large staffs and many teams making the selections, this is not possible or even desirable. Therefore, SRS has chosen to guide the selection process by providing guidance to the team as to what a "significant exposure" is and what constitutes a "major contributor to defense in depth". This guidance does not (as in the past) prescriptively drive control selection, but it is provided to the selection team to help in the selection of controls. This guidance is the key element of the new functional classification methodology and procedure for SRS and the salient point of this paper.

## How can we identify major contributors to defense in depth?

The selection process for safety significant major contributors to defense in depth naturally builds on the hazard analysis process and the selection of safety class and safety significant controls for specific receptors (public or workers). A key element of the SRS process is the use of an integrated hazard analysis process (IHA). During the IHA, event by event evaluations are performed with the identification of all SSCs and ACs that could be selected as controls to either mitigate or prevent the event. This listing of possible controls provides the starting point for selecting major contributors to defense in depth.

A second key to making an informed selection process for those SSCs or ACs that provide a major contribution to defense in depth is the event by event evaluation process. Unless the SSCs and ACs are judged against a specific event, then it is difficult to assure that the process identifies all SSCs and ACs that contribute to risk reduction in a significant way.

A third element required to understand the basis for selection of major contributors to DID is the definition of a significant exposure used at SRS to implement the 3009 guidance. Obviously the public criteria based on the 25 rem EG is well defined. However, the definition of a significant worker exposure has not been defined and is thus open to wide interpretation. These interpretations can vary from LD-50 down to any exposure above allowable normal worker exposure levels. Therefore, SRS has established a 100 rem exposure as a conservative threshold for defining a significant exposure (with ERPG-3 used for chemicals). These thresholds are then used to inform the qualitative control selection process for workers and as will be described later in this paper as guidance for selecting major contributors to defense in depth.

An important underlying aspect behind the values identified as a guidance threshold for significance is that the 1$^{st}$ LOC provides adequate protection for the hazard. The 1$^{st}$ LOC is complete and assures that the control set will assure that the receptor will not be exposed to hazardous material at a level above that assumed in the hazard and accident analysis process. However, following on to the selection of an adequate set of controls to assure protection for the identified receptor is the evaluation of major contributors to DID implementing the DOE-STD-3009 concept of multiple layers of protection against the most significant hazards.

Key in understanding the process of selecting major contributors to defense in depth is to address the "Major" portion of that criterion, as it relates to the likelihood of identifying a major contributor to defense in depth associated with the safety of workers or the public for these postulated events. Events that are more frequent and have a very large potential consequence fall into the category of likely having or requiring a "Major Contributor" to defense in depth. This

recognizes that there is already a built in risk reduction associated with low frequency events. For example events that are not likely to occur, yet are required to be evaluated for control selection, are not as likely to have (or warrant) SSCs or ACs that provide a major contributor to defense in depth for the workers or the public. In addition to the frequency element of risk, the impact on risk for postulated significance of the consequences are also addressed. Therefore, events that expose workers or the public to consequences that are not significantly higher than the 25 rem or "significant exposure" guidelines for the public or workers respectively also do not fall into the category of likely having or requiring a "Major Contributor" to defense in depth. It is important at this point to emphasize that the first LOC and the remainder of the safety programs already in place in the facility assure that adequate protection is provided for these receptors. This starting point for selecting major contributors to defense in depth assures that exposures are much less than these values and in effect assure that exposures to the various receptors remain at the normal operational level. Therefore, only those events with relatively high frequencies and significant exposures are likely to warrant having a control provide a major contribution to defense in depth for that event.

With the above understanding the SRS process focuses on events that pose the most risk to workers and the public. Thus, events that can cause death to any receptor or that require a SC or SS control to protect the public or workers per the control selection process warrant consideration for the pubic and worker group 3 (collocated workers) are selected for further control evaluation and possible identification of a major contributor to defense in depth.

A fourth element of this evaluation is to carry the SRS concept of a level of control (LOC) into this selection process. By identifying the major SSCs and/or ACs and all other SSCs or ACs required to perform the identified safety function, then the process truly captures the set of items required to provide a major contribution to defense in depth. DOE-STD-3009 refers to these additional SSCs as support systems.

With these elements to the process defined, then the process for selecting major contributors to defense in depth can be initiated. There is a slight difference in process between the DID evaluation process for an existing facility and for a project. An existing facility performs this evaluation process based on the available set of controls. In the greenfield project environment, the facility does not exist and therefore, the appropriate question is whether a major contribution to DID already exists or should be included in the design.

## Methodology for Selecting Major Contributors to Defense in Depth

The approach to selecting the major contributors to defense in depth that are identified as SS is based on an informed qualitative team approach within the IHA. The process outlined in this section is intended to guide the selection of controls and is not intended to prescribe the result. However, the result must be technically defensible and consistent with the intent of the selection criteria provided herein.

The process of identifying potential major contributors to defense in depth is a natural extension of the hazard evaluation process. Events that have the potential for significant consequences to

the public or workers are scrutinized more closely using this process. The SRS process is described below. Events that are:

1. more frequent than BEU and have an unmitigated consequence to any receptor that would result in death or serious injury within one year based on an exposure for the event duration (exposures up to 2 hours), or

2. identified in hazard or accident analysis as requiring a LOC for Worker Group 3 or the public.

shall be evaluated for major contributors to Defense in Depth. Projects shall evaluate the need for including a SS major contributor to DID. Existing facilities shall evaluate identified preventors and mitigators providing DID for those that provide a major contribution to DID, and thus should be identified as SS. For each event, alternate complete LOCs that were not selected as the event's primary LOC (i.e., already classified as SC or SS for the event) are identified as candidates for selection as Major Contributors to Defense-in-Depth.

Major Contributors to DID are identified from this list of candidate controls and designated as SS SSCs or administrative controls, based on consideration of the following criteria. When selected, these Major Contributors to DID are credited with providing additional LOCs for the affected events. The following criteria shall be considered when identifying candidates as major contributors to DID.

a) The control has already been credited as a first LOC for any receptor for another event. As these controls have already been credited as SC or SS, they may also provide a cost effective major contribution to DID, and be selected as a second LOC.
b) The first LOC is a complex electromechanical device, particularly if it must function rapidly.
c) The first LOC is directly dependent on human performance (An additional LOC reducing the risk of reliance on human performance may be appropriate in this case.).
d) The control is identified as a candidate LOC for multiple events.
e) The first LOC does not satisfy its design requirements without additional analysis (i.e., required backfit analysis).
f) The control substantially reduces the risk of events subjecting the public to consequences which are much greater than the 25 rem EG or exceed ERPG-3, particularly if the frequency of the event as determined by hazard analysis is determined to be Anticipated or Unlikely.
g) The control reduces the risk of events subjecting workers to much greater than 100 rem evaluated at one year EDE, to death within one year, or which exceed ERPG-3, particularly if the frequency of the event as determined by hazard analysis is determined to be Anticipated or Unlikely.
h) The control provides an additional significant and robust protective component for the identified receptor beyond the credited controls.
i) The control appreciably reduces the risk of significant energetic events that potentially threaten multiple levels of control. As required by DOE-STD-3009, a major contributor to DID must be identified for significant energetic events (e.g., deflagration, detonation, or energetic and catastrophic rupture).

j) The control reduces the risk of a significant and uncontrolled release of hazardous chemicals (e.g., valves or physical barriers to prevent potentially reactive chemicals from mixing in an uncontrolled manner) where the consequences to any receptor could exceed ERPG-3.
k) The control provides a significant prevention of a criticality (e.g., geometry of nuclear material maintained to prevent critical mass) when the credited controls are not as robust as desired.

Selection of major contributors to DID must consider the degree of risk reduction provided by the control under consideration. Note that a singular occurrence of a control associated with one event may provide a greater amount of overall facility risk reduction than a control repeatedly mentioned for various events, that provides minimal risk reduction. Risk reduction also varies with the affected population. A balance must be established between a high dose to a limited population versus a lower dose to a larger population.

In those cases where there are many ways to detect and prevent or mitigate the event it is typically not necessary to select more than one LOC to be classified as SC or SS (Note specific exceptions in "i" and "j" above). There is no pre-defined number of LOCs to ensure adequate DID and all SSCs providing DID do not need to be classified as SS. However, as a general rule, events that could result in the most severe uncontrolled releases of hazardous material [e.g., events which (a) significantly exceed the offsite or onsite (receptor 3) criteria or (b) which are energetic, could damage multiple facility DID features, and significantly exceed the offsite or onsite (receptor 3) criteria] generally would have more LOCs with the potential to provide a major contributor to DID, than those events that do not have the same severe release potential. This decision must be based on documented sound engineering judgment. The assumptions made must be protected programmatically. For internal event cases, where a robust passive SSC is credited as the first LOC and that SSC makes it BEU that a release could occur that challenges the EGs or criteria, it is not necessary to select the additional LOCs.

## Summary

Based on the experience with selecting safety SSCs and Administrative Controls, the Savannah River Site has moved from a prescriptive process of control selection based on numbers of LOCs and moved to an informed qualitative process. The guidance within the SRS procedure that governs control selection should permit consistency of application yet be true to the direction in DOE-STD-3009 CN2 in having these controls selected qualitatively with no prescribed minimum or maximum numbers of safety related controls.

## Status

This revision to the SRS functional classification procedure and methodology manual has been conceptually approved by the SRS Authorization Basis Steering Committee responsible for the procedure. However based on feedback from the procedure review process DOE-SR requested that they be provided examples of the implementation of this procedure so that the full impact of the changes was clear. As of the preparation of this paper, these examples are being prepared and

the meeting with DOE-SR is being scheduled. An update will be provided at the EFCOG meeting.