5. Chapter Five, Accelerator Safety Envelope (ASE)

Table of Contents

5.1.Background

The Accelerator Safety Envelope (ASE) formally establishes the set of bounding conditions or constraints on engineered and administrative systems, within which the Collider-Accelerator Department proposes to operate. These constraints are based on the safety analysis documented in Chapter 4 of the Safety Analysis Document (SAD). The ASE assures the validity of the basic set of assumptions used in the SAD safety analysis and ensures that the physical and administrative controls used to mitigate potential hazards are in place.

DOE requires adherence to the approved requirements stated in the Accelerator Safety Envelope because it is the authorization basis for all commissioning and operations activities. This chapter provides an overview of the development of the content of the ASE. The actual ASE is a separate, controlled document that must be approved by DOE. DOE approval is required for all changes to the ASE. As per BNL Subject Area requirements, a proposed draft ASE is submitted to the Laboratory's ESH Committee for review at the time the SAD is submitted for BNL approval.

Section 1 of the ASE is an introduction. The introduction indicates the method used by the Collider-Accelerator Department for change control of the ASE. It indicates how the Department is to treat a variation beyond the constraints described in Sections 2, 3, and 4 of the ASE, and it describes the use of emergency actions that may be taken when actions not consistent with the ASE are needed to protect the public, worker or the environment.

To understand the appropriate level of bounding information or constraints included in Sections 2, 3, 4 and 5 of the ASE, one must first understand the overall flow-down of information from the highest level constraints stated in BNL SBMS requirements to the lowest-level constraints stated in the Department documents such as operating procedures. This flow-down of information generally produces several levels of constraints that provide a defense-in-depth to ensure the safe and environmentally sound operations of the accelerators. The top levels of constraints are placed in the Accelerator Safety Envelope (ASE). The lower levels of constraints are established in the Collider-Accelerator Conduct of Operations document[1] and Operations Procedure Manual.[2]

The highest-level constraints, which are termed “Safety Envelope Limits,” are documented in Section 2 of the ASE. These are the absolute limits that BNL places on its operations to ensure that the regulatory limits established to protect the environment, the public and staff and visitors are met.

The next highest level constraints are the operating limits used as a basis for the Safety Analysis Document (SAD) hazard analysis. This level of constraints is termed

[1] http://www.rhichome.bnl.gov/AGS/Accel/SND/conductofops.htm C-A Conduct of Operations
[2] http://www.rhichome.bnl.gov/AGS/Accel/SND/OPM/index.htm C-A Operations Procedure Manual

"Corresponding Safety Envelope Parameters," and is documented in Section 3 of the ASE. Section 3 of the ASE identifies the critical operating parameters that ensure the accelerator and experimental operations will not exceed the corresponding Safety Envelope Limits in Section 2 of the ASE.

Although it is an accepted practice for DOE Reactor Facilities, the Accelerator Safety Order neither prescribes nor prohibits a list of alternate actions to Corresponding Safety Envelope Parameters listed in the ASE. However, BNL SBMS requirements indicate that operations procedures addressing ASE-required equipment and systems should specify the minimum necessary system components and monitoring devices to allow operation, and if these minimums are not met, then alternate actions are to be specified in the procedures. C-AD has chosen to also list these alternate actions in the ASE and has termed them "Authorized Alternatives." The equivalence of an Authorized Alternative to a Corresponding Safety Envelope Parameter was thoroughly reviewed. It is acknowledged that the use of an Authorized Alternative might pose a slight increase in risk; however, the C-AD does not consider the increase to be significant. Additionally, the number and depth of Authorized Alternatives listed in the ASE do not indicate that the affected systems are unreliable. It is noted that DOE reactor facilities can have the equivalent of authorized alternatives for all of their safety systems. Further, whenever an Authorized Alternative is used at C-AD, the Department is committed to performing a critique. Authorized Alternatives are listed in Section 3 of the ASE.

Lower levels of safety-related constraints may or may not be included in an ASE. In a large complex facility like C-AD accelerators, lower-level safety-related constraints are contained in much larger controlled documents that are reviewed and updated

frequently. As previously indicated, these documents are the Collider-Accelerator Conduct of Operations document[3] and the C-AD Operations Procedure Manual.[4]

The C-AD ASE has been developed primarily to define the important limits for operation within the assumptions of the SAD hazard analyses and to define operability requirements of safety-significant systems. The scope and content of the ASE have been limited to include only the most critical requirements in order to make the ASE operationally useful for controlling the safety of the accelerators and experiments. Because of this philosophy, the details needed to adequately describe the use of lower-level safety-related constraints only appear in operating procedures, which are initially examined by an independent review team during the Accelerator Readiness Review, and subsequently examined and updated every three years by the C-A Department.

These lower-level constraints may consist of documented or measurable limits or administrative controls necessary to establish an operational margin of safety that may be more conservative than that established in the ASE. This operating margin provides a defense-in-depth approach to ensure that the Collider-Accelerator Department will operate the accelerators and experiments well within Safety Envelope Limits and Corresponding Safety Envelope Parameters agreed to by DOE in formally approving the ASE. Lower-level constraints in the C-A OPM generally address requirements for industrial safety, environmental protection, waste management, pollution prevention, radiation protection, ALARA, workplace hazardous materials monitoring, use of personal protective equipment, and occupational health and safety.

[3] http://www.rhichome.bnl.gov/AGS/Accel/SND/conductofops.htm C-A Conduct of Operations
[4] http://www.rhichome.bnl.gov/AGS/Accel/SND/OPM/index.htm C-A Operations Procedure Manual

Compliance with lower-level constraints is achieved through training of personnel, self-assessment, periodic management review and each individual's commitment to adhere to requirements in procedures. Examples of lower-level constraints may be related to ASE parameters that are physically designed into the accelerators, such as maximum beam power, maximum beam energy or maximum beam intensity. A physical change to the accelerator would be needed to exceed these ASE parameters. Since C-AD management and staff are expected to adhere to configuration control procedures in the OPM, physical changes to accelerators or experiments would be referred by liaison physicists and liaison engineers to appropriate safety committees and internal and external approval authorities before the change occurred. These configuration control procedures are considered lower-level constraints. Safety committees examine proposed changes to accelerators and experiments and consider the impact on the ASE requirements. Other examples of lower-level constraints are authorizations such as 1) release of an effluent to the sanitary system and 2) radiation safety check-off lists that must be completed prior to start-up of an accelerator for a particular physics program.

5.2. Summary of ASE Content

The basic content of the ASE includes the following sections:

Section 1: Introduction

The following items are included:

- General actions to be taken upon discovery of a violation of the Safety Envelope, including shutdown of the facility.
- A description, or reference, to the method used by the Department for change control of the ASE.

Section 2: Safety Envelope Limits

This section contains two categories of limits: the absolute limits that BNL places on its operations to ensure the Collider-Accelerator Department meets regulatory limits established to protect the environment, public and staff/visitors; and the design/operating limits used as a basis for the SAD.

Section 3: Corresponding Safety Envelope Parameters

This section identifies the measurable limitations on critical operating parameters that, in conjunction with the specifically identified hazard control considerations established by

the facility design, construction, or experimental design constraints, ensure the accelerator or experimental operations will not exceed the Safety Envelope Limits. These parameters are derived from the safety analysis in Chapter 4 of the SAD.

Section 4: Engineered Safety Systems Requiring Calibration, Testing, Maintenance, and Inspection

This section includes the identification of the systems and requirements for calibration, testing, maintenance, accuracy or inspection necessary to ensure the continued reliability of engineered safety systems that ensure the operational integrity of parameters listed in Section 3. Requirements are consistent with established BNL Policies.

Section 5: Administrative Controls

This section includes the administrative controls necessary to ensure the operational integrity of parameters listed in Section 3. Included are minimum staffing level requirements, qualification and training requirements for operations, minimum operable equipment, work planning and control systems and environmental release mitigation measures.