S01030100-ES0001, R00

Second Target Station (STS) Project

Policy for Selection of Safety Related Credited Controls

January 2021

OAK RIDGE NATIONAL LABORATORY
MANAGED BY UT-BATTELLE FOR THE US DEPARTMENT OF ENERGY

Second Target Station (STS) Project

Policy for Selection of Safety Related Credited Controls

Approved by: Steven M. Trotter Digitally signed by Steven M. Trotter Date: 2021.01.28 11:58:57 -05'00'

Steven M. Trotter, STS Environment, Safety, Health, and Quality

Approved by: Graeme Murdoch Digitally signed by Graeme Murdoch Date: 2021.02.08 12:22:44 -05'00'

Graeme Murdoch, STS Project Manager

Approved by: John Haines Digitally signed by John Haines Date: 2021.02.08 16:59:39 -05'00'

John Haines, STS Project Director

January 2021

Prepared by
OAK RIDGE NATIONAL LABORATORY
Oak Ridge, TN 37831-6283
managed by
UT-BATTELLE, LLC
for the
US DEPARTMENT OF ENERGY
under contract DE-AC05-00OR22725

CONTENTS

1. INTRODUCTION AND BACKGROUND

1.1 INTRODUCTION

This document establishes the policy to be used to designate controls essential to safety as "Credited Controls" for the Second Target Station (STS) Project. The policy is based on hazard/safety analysis documented in the SNS Final Safety Assessment Document for Proton Facilities (FSAD-PF), the Final Safety Assessment Document for Neutron Facilities (FSAD-NF), and hazard and safety analysis supporting the Second Target Station (STS) project. This policy implements the requirements of DOE Order 420.2C[1], *Safety of Accelerator Facilities* (referred to as the Accelerator Safety Order) related to the selection of safety related engineered and administrative controls designated as Credited Controls.

DOE Order 420.2C[1] requires the Safety Assessment Document (SAD) to "…provide detailed documentation of engineered controls (e.g., interlocks and physical barriers) and administrative measures (e.g., training) taken to eliminate, control, or mitigate hazards from operation..." The DOE Implementation Guide for DOE O 420.2C[2] discusses identifying certain controls as "Credited Controls" and defines a Credited Control as "…controls determined through safety analysis to be essential for safe operation directly related to the protection of personnel or the environment." Credited Controls are a limited subset of the total number of controls used for overall facility operation. This policy specifically addresses controls required to protect the public and on-site personnel. Furthermore, the policy addresses both the primary Credited Control and Credited Controls that provide an additional significant reduction in risk to the public or worker.

The criteria presented in this policy are primarily based on radiation dose and airborne toxic chemical concentrations. These criteria also serve to protect the environment, as the Credited Controls prevent or mitigate radioactive material and/or toxic chemical releases. Therefore, the criteria requiring Credited Controls in Section 2 inherently provide appropriate protection for the environment.

Standard industrial hazards are not intended to be addressed in detail in the hazard analysis and SAD[2] and are not addressed in this policy. Standard industrial hazards are those that are routinely encountered and accepted in general industry and for which national consensus codes and/or standards exist to guide safe design and operation. However, standard industrial hazards are evaluated for their potential to serve as initiators for accidents related to specific accelerator processes. At STS, the potential exists for a unique Oxygen Deficiency Hazard (ODH) that potentially falls outside the scope of national consensus codes/standards. For this reason, a criterion requiring Credited Controls for significant ODH hazards due to significant quantities of cryogenic material is included in this policy.

The criteria presented here are applied to postulated off-normal/accident event consequences analyzed in the Hazard Analysis and the SAD. The hazard analysis and SAD evaluate a broad and encompassing range of postulated off-normal events and their potential consequences to workers and the public. Section 2 of this document presents criteria for determining when Credited Controls are required to prevent or mitigate a postulated off-normal event, based on the unmitigated consequence potential of the event. Section 3 presents guidance to aid in the proper selection of a Credited Control when more than one control is available to prevent or mitigate a postulated event. Appendix A defines terms used throughout this document.

1.2 BACKGROUND

The purpose of the Safety Assessment Document (SAD) is to describe in sufficient detail all significant hazards presented by the facility and its operations, and the controls by which these hazards will be

managed to an acceptable level of risk[2]. Figure 1 illustrates the overall safety analysis process to be followed by STS in designating Credited Controls. Since Credited Controls are important to safety, they are typically addressed in the Accelerator Safety Envelope (ASE) with requirements for operability, testing, and surveillance, as needed to ensure they can reliably perform their designated safety function. Credited Controls are included in the highest quality assurance category (Level 1), as described in the applicable quality assurance plan for the project or existing facility (*Second Target Station Quality Assurance Plan*[8]).

The process that drives the determination of public and worker protection requirements evaluates the following event types:

Internal events: This includes credible internally initiated operational accidents such as process upsets, spills, equipment failures, fires, and explosions. Credibility must be conservatively determined based on consensus of professional opinion, while assuring that all types of event scenarios are evaluated, and the events excluded can easily be justified as clearly not credible based on physics or other bounding logic. Examples of credible internal events include events resulting from equipment failures and human errors:

- A single independent failure of equipment or system
- Two independent operator errors (Note: An operator error associated with the event that can go undetected for a significant period of time would be counted as one of the two independent operator errors.)
- Common Cause, i.e. multiple failures occurring with or following a single initiating event

Natural phenomena events for the site (e.g., earthquakes, extreme straight-line wind, tornadoes, lightning, precipitation, etc.) that could affect the facility are defined by DOE-STD-1020-2016[4]. Evaluations of postulated impacts (for both the public and workers) require determining the appropriate natural phenomena design category for each of the natural phenomena hazard (NPH) events. Note that for postulated earthquake impacts, Seismic Design Categories (SDC) and Limit States (LS) for each credited safety system will be defined to assure that the safety function is appropriate for the identified risk.

Man-made externally initiated events such as airplane, train, or truck crashes, or adjacent facility events that can either cause releases or have a major impact on facility operations. The frequency for considering these events in the design and safety basis is 10^{-6} per year if conservatively calculated or 10^{-7} per year if realistically calculated.

In evaluating all three event types, additional failures are considered in event scenario development if they could be caused by the event being investigated (i.e., failure(s) dependent upon the accident initiator).

The hazard evaluation assesses consequences to at least two on-site groups of workers: workers inside the process building being evaluated and workers outside the building. The approach used to evaluate the potential impacts to workers in these groups depends on the hazard involved and location of the workers. All credible worker locations are considered to assure appropriate controls are provided. An informed qualitative approach (one that combines expert opinion, conservative assumptions and calculations, as needed to get a conservative understanding of the hazard) to Credited Control selection for worker protection is typically applied. For release of radioactive material outside the building, plume transport methods are typically used to guide the selection.

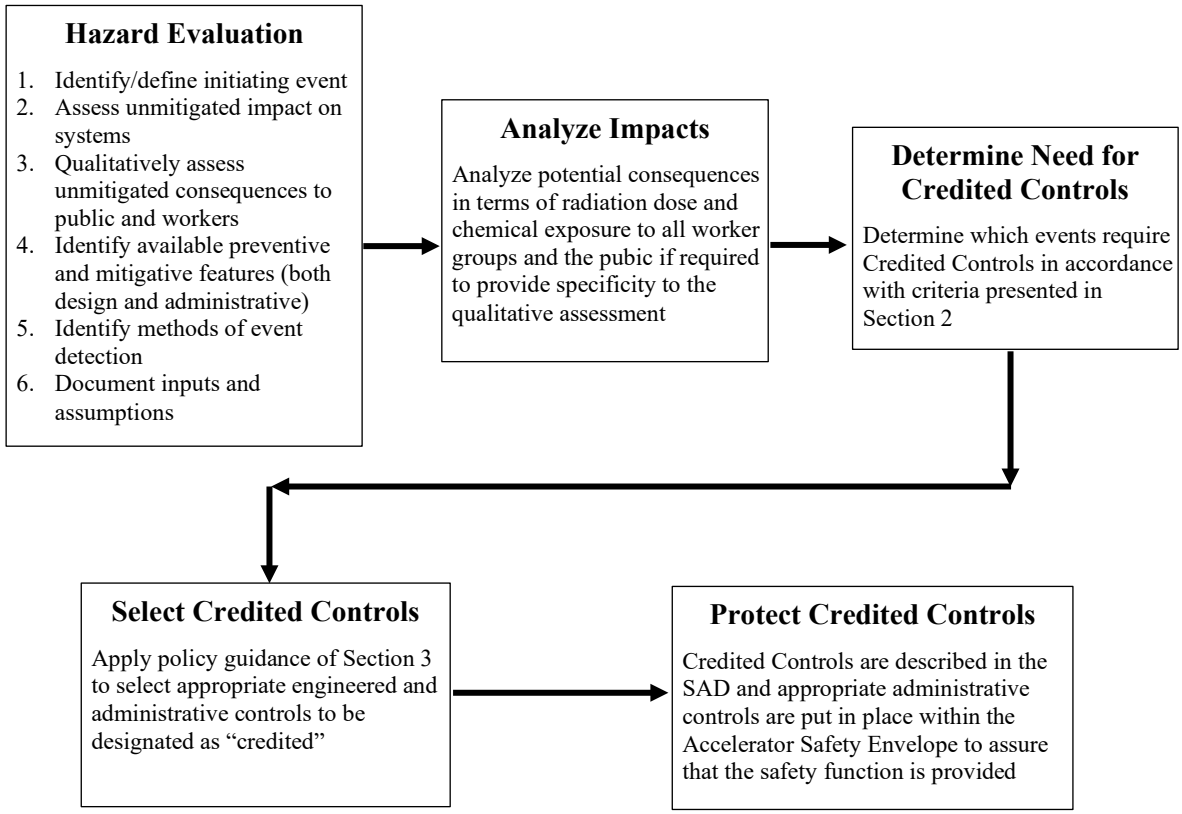

Figure 1. Hazard Based Process for Determining Safety Related Credited Controls.

2. CRITERIA FOR DETERMINING THE NEED FOR CREDITED CONTROLS

The criteria below are to be applied to determine when safety related Credited Controls are required. The criteria are written in terms of "levels of control" for two reasons: (1) a level of control may need to consist of more than one equipment item (e.g., system or component) or administrative controls that work in concert to accomplish the required safety function, and (2) in certain instances, more than one level of control is warranted to minimize the risk associated with a significant hazard. For the following criteria, it is understood that a level of control shall be complete in that it consists of the credited control items whose function is necessary and sufficient to prevent or mitigate significant exposure to workers or the public.[*] A level of control, as used below, shall consist of Credited Engineered Control(s) and/or Credited Administrative Control(s) unless otherwise specified.

The following assumptions apply to the criteria listed below:

- Radiation dose criteria are for the total effective dose equivalent (TEDE), which includes both internal and external exposures resulting from the accident.

[*] The values used to identify Credited Controls within this policy are not intended to constitute "acceptable exposures" to the identified receptors, but only the need for Credited Controls. Selection of Credited Controls builds on the robust safety management programs included in the Integrated Safety Management System and SBMS and thus is part of an overall program to assure that the workers, the public, and the environment are not exposed to hazardous materials beyond that which would be considered ALARA.

- Toxic chemical hazards are evaluated against the appropriate Protective Action Criteria (PAC) criteria associated with the chemical of concern. Chemical vapor concentration criteria are for the highest 15-minute average or one hour depending on the worst case, during the accident period at the location of interest.

- Accident consequences are to be evaluated over a maximum 8-hour period.

- When determining unmitigated consequences, equipment required to act in response to an event (i.e., an active control) is assumed to fail.

- Passive controls, such as a seismically qualified wall, can be assumed to function unless a credible failure is postulated.

- The dose criteria for onsite workers located outside the building during atmospheric releases are to be applied at a 100 m distance downwind from the point of release. The distance of 100 m was selected because the accuracy of typical dispersion models is limited at closer distances.

The following criteria apply to the unmitigated consequences determined conservatively to be associated with each off-normal/accident event evaluated in the SAD:

1. If the unmitigated dose exceeds 25 rem to an off-site receptor, two levels of control are required:
   a. A primary level of control shall be identified to prevent or mitigate the accident.
   b. A second level of control shall be credited as a back-up.

2. If the unmitigated dose is between 5 rem and 25 rem to an offsite receptor and with an estimated frequency above 10^{-4}/year, at least one level of control shall be identified.

3. If the unmitigated offsite airborne toxic chemical vapor concentrations exceed PAC-2[5,6], then a level of control shall be identified.

   Note: Either of the two levels of control required by criterion 1 above may be used to satisfy requirements for criteria 2 and 3. The level of control required by criterion 2 may be used to satisfy the criterion 3, and vice versa.

4. If the unmitigated radiation dose to a worker exceeds 25 rem or exposure to airborne chemical concentrations above the defined PAC-3 level, then a level of control shall be identified.

5. If the unmitigated radiation dose to a worker outside the building exceeds 25 rem and occurs at an estimated frequency exceeding 10^{-4}/year, at least two separate levels of control shall be identified.

6. For each unmitigated event that could cause a worker to experience breathing air with oxygen concentration below 12.5 volume percent and for which existing SBMS do not provide adequate design or operational requirements adequate to assure worker safety; a level of control shall be identified.

For credible events that require designation of a level of control for protection of personnel or the public, consideration should be given as to whether designating an additional level of control could provide significant additional risk mitigation to help ensure that worker risk is minimal. The process used, discussed in Section 4.1.1 of Reference 7, satisfies the Accelerator Safety Order (ASO) requirement to ensure that all marginal and unacceptable risks have been mitigated to acceptable levels through controls and/or limits on the operation of the facility. The process for identifying the possible additional level of

control requires a careful evaluation of the overall situation and possible credited and non-credited controls that could be applied. Part of the evaluation is whether the additional level of control should be credited, and this must be considered on a case-by-case basis. The following would be examples of when an additional level of control should be considered:

- The credited level(s) of control for an event initiated by or involving an explosion or large fire that could breach confinement barrier(s) is not a preventive feature (e.g., one that prevents an H_2 release that could cause an H_2 explosion event, or a fire suppression system that prevents a large fire).

- A credited level of control is dependent on human performance within a limited period.

- A credited level of control is dependent on a complex device for which a documented reliability analysis is not available.

If Credited Engineered Controls (CECs) are selected per Criterion 1, their public protection role shall be documented in the section of the FSAD that describes CECs. This FSAD section shall also describe standards applied to a CEC that is the primary control per Criterion 1(a), including DOE Order 420.1C, Chg. 3[3] seismic and fire protection requirements for safety systems that protect the public per Reference 4.

3. GUIDANCE FOR SELECTING CREDITED CONTROLS AFTER NEED FOR CREDITED CONTROL IS ESTABLISHED

This section provides guidance for selecting equipment items to accomplish the safety related functions identified per the criteria of Section 2. The basic purpose of Section 2 is to determine when a safety related credited "level of control" is needed. Once the need for a level of control is established, it is necessary to follow a disciplined process of selecting the set of equipment items (Credited Engineered Controls) and/or administrative controls (Credited Administrative Controls) needed to accomplish the required safety function. The selection of Credited Controls often involves choices between multiple controls that could function to control an identified event. The criteria below provide guidance that will help the designer attain the greatest degree of efficiency and reliability. It is realized that there will be situations where some of the criteria may not be appropriate for a given situation. Engineering judgment must be applied in these cases to determine the best items for selection.

When selecting CECs, it is necessary to identify any dependencies for each system being considered. For example, if a given system is a CEC but it depends on another system to enable it to function as required, then at least some aspect of that other system becomes a part of the CEC to assure that the safety function can be performed. Structures, systems, and components that directly support the function of Credited Engineered Controls (or Credited Administrative Controls) need to be identified and their safety functions defined in the SAD.

The selection preferences listed below should be followed to the extent practical when designating Credited Controls:

1. When either an active or passive device can be credited to ensure the safety function, the passive device should be selected. This is because of the inherently higher reliability of passive devices.

2. If either engineered control(s) or administrative control(s) could perform the needed safety function, the engineered control should be selected. This is because of the generally higher reliability of engineered controls versus human actions.

3. When a choice exists between controls that would prevent an event and controls that could mitigate the consequences of the event, the preventive controls should be selected. This is because of the inherent value of preventing accidents as opposed to mitigating their effects.

4. Only those items essential for safe operation directly related to the protection of workers, the public, and the environment should be selected as Credited Controls. The number of Credited Controls should, in general, be minimized and include only a limited subset of the total number of controls employed for overall facility operation. This guidance allows a high degree of operational attention (e.g., monitoring, surveillance, maintenance, control of documentation, etc.) to be devoted to the Credited Controls. To support this selection criterion, Credited Controls that protect against multiple events or receptors are preferred.

5. Where two levels of control are required, the controls are to be independent such that the failure of one level of control does not cause failure of the other. This criterion ensures that multiple levels of control are not compromised by a single failure.

4. REFERENCES

1. DOE Order 420.2C, *Safety of Accelerator Facilities*, July 2011.
2. DOE Guide G 420.2C-1A, *Accelerator Facility Safety Implementation Guide for DOE O 420.2C, Safety of Accelerator Facilities*, August 2014.
3. DOE O 420.1C, Chg. 3, *Facility Safety*, November 2019.
4. DOE-STD-1020-2016, *Natural Phenomena Hazards Design and Evaluation Criteria for Department of Energy Facilities*, December 2016.
5. EPA 550-B-99-009, *Risk Management Program Guidance for Offsite Consequence Analysis*, March 2009.
6. *Protective Action Criteria (PAC): Chemicals with AEGLs, ERPGs, & TEELs*, Rev 29A, February 2012. Available at: Protective Action Criteria (PAC) with AEGLs, ERPGs, & TEELs | Department of Energy
7. *SNS Final Safety Assessment Document for Proton Facilities*, SNS102030103- ES0018-R02, December 2010.
8. *Second Target Station Quality Assurance Plan,* Document No. S010300000-QA0001, R0, March 2020.

APPENDIX A. DEFINITIONS AND ACRONYMS

Acute Exposure Guideline Levels (AEGLs)**: Provide the basis for the Protective Action Criteria (PAC, see below)**. They represent threshold exposure limits for the general public and are applicable to emergency exposures ranging from 10 minutes to 8 hours. Three levels—AEGL-1, AEGL-2, AEGL-3—are developed for each of five exposure periods (10 minutes, 30 minutes, 1 hour, 4 hours, and 8 hours) and are distinguished by varying degrees of severity of toxic effects. DOE guidance is to use the 1-hour AEGL values, which appear in this database. The three AEGLs are defined as follows:

AEGL-1 is the airborne concentration (expressed as ppm [parts per million] or mg/m3 [milligrams per cubic meter]) of a substance above which it is predicted that the general population, including susceptible individuals, could experience notable discomfort, irritation, or certain asymptomatic, nonsensory effects. However, these effects are not disabling and are transient and reversible upon cessation of exposure.

AEGL-2 is the airborne concentration (expressed as ppm or mg/m3) of a substance above which it is predicted that the general population, including susceptible individuals, could experience irreversible or other serious, long-lasting, adverse health effects or an impaired ability to escape.

AEGL-3 is the airborne concentration (expressed as ppm or mg/m3) of a substance above which it is predicted that the general population, including susceptible individuals, could experience life-threatening adverse health effects or death.

Credited Control: An equipment item or administrative action that has been formally designated through hazard analysis to be essential for protection of workers or the public. A Credited Control may be a Credited Engineered Control (CEC) or a Credited Administrative Control (CAC).

Credited Administrative Control: A procedure or other requirement that specifies certain human action(s) take place which ensure the safe operation of the facility for workers and the public.

Credited Engineered Control: Hardware or structural items (structures, systems, and/or components) that accomplish a required safety function.

Chemical Evaluation Criteria: Where a potential accident release involves a potential injury threat due to its chemical properties, a criterion is needed to evaluate the need for Credited Controls or to judge adequacy of controls selected based on radiation dose related criteria. Criteria involving concentration are typically used. Non-radiological chemical toxicity of accident releases is judged based on PAC-3 for workers and PAC-2 for the public.

Dose: For the purposes of assessing accident consequences to a receptor, dose is defined as the total effective dose equivalent (TEDE) received from the single event.

Evaluation Guideline: The public evaluation guideline of 25 rem is specified by the DOE for use in deciding whether Credited Controls are needed to prevent or mitigate accidents. Although this is a quantitative criterion, it is not considered to be an "acceptable" dose. Analysis is used to determine if the Evaluation Guideline could be challenged by the identified event scenario.

Informed Qualitative Approach: The informed qualitative approach assumes that the integrated team charged with implementing this procedure makes use of expert input and quantitative analysis as needed to inform the inherently qualitative control selection process for workers and defense in depth. This input is not a "go-no-go" input but part of the control selection process.

Level of Control: One or more structures, systems, components, administrative controls, or inherent features (e.g., chemical properties, gravity, physical constants, underground location) that can be readily expected to act to prevent an accident or to mitigate its consequences substantially. For example, in the cryogenic moderator system, the hydrogen boundary, the hydrogen rupture disc, and the rupture disc discharge path perform (together) as a single level of control against the inadvertent release of hydrogen inside the core vessel.

Offsite: Within the context of this policy, offsite refers to the public, and includes receptors along or beyond the Oak Ridge Reservation boundary and along Bethel Valley Road. The inclusion of Bethel Valley Road inside the reservation boundary came about because the SNS PSAR was completed and approved before most of Bethel Valley Road was closed to the public after September 2001. The Bethel Valley Road locus of potential receptors has been retained for conservatism. It can be noted, however, that the ridge top location of SNS places the limiting dispersion paths to members of the public between the SNS site and other ridge top locations at or beyond the boundary instead of down to Bethel Valley Road.

Protective Action Criteria (PAC): DOE's Protective Action Criteria are defined by Advanced Technologies and Laboratories International, Inc in "Protective Action Criteria (PAC): Chemicals with AEGLs, ERPGs, & TEELs," Rev 27, February 2012. This is available at: Chemical Safety Program: PACs for Chemicals of Concern - Definition of PACs (AEGLs, ERPGs or TEELs) (energy.gov). EPA 550-B-99-009, Risk Management Program Guidance for Offsite Consequence Analysis, March 2009. The PACs are applied, based on the following hierarchy: 1) AEGLs if available then, 2) ERPGs if available, 3) then TEELs.

PAC-2: Irreversible or other serious, long-lasting, adverse health effects or an impaired ability to escape.

PAC-3: Life threatening health effects.

Total Effective Dose Equivalent (TEDE): The TEDE referred to in this policy is the sum of the effective dose equivalent for external exposures and the committed effective dose equivalent (CEDE) for internal exposures (e.g., from inhalation of airborne radioactive material) received over the course of a postulated accident.

Unmitigated Consequences: A defined concept used to provide structure to the identification of these items that are important to safety. The unmitigated consequences of an event are generally taken to be the consequences without the benefit of human actions and without the benefit of structures, systems, or components that would prevent or mitigate the event. An unmitigated hazard scenario is evaluated for each initiating event by assuming the absence of preventive and mitigative controls. Unmitigated likelihood and consequence estimates assume that active engineered and administrative controls are not available to reduce either the consequence or likelihood of the hazard scenario. However, the unmitigated analysis does assume that passive design features exist and provide their safety function if these features are not affected by the accident scenario, or these features are affected by the accident scenario and a separate assessment determines that they will survive accident conditions.