

*If you are using a printed copy of this procedure, and not the on-screen version, then you **MUST** make sure the dates at the bottom of the printed copy and the on-screen version match. The on-screen version of the Collider-Accelerator Department Procedure is the Official Version. Hard copies of all signed, official, C-A Operating Procedures are kept on file in the C-A ESHQ Training Office, Bldg. 911A.*

C-A OPERATIONS PROCEDURES MANUAL

ATTACHMENT

9.6.1.a Cryogenic Safety Analysis

Text Page 2 through 7

C-A-OPM Procedures in which this Attachment is used.		
9.6.1		

Hand Processed Changes

<u>HPC No.</u>	<u>Date</u>	<u>Page Nos.</u>	<u>Initials</u>
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

Approved: _____ *Signature on File* _____
 Collider-Accelerator Department Chairman Date

A. Etkin

CRYOGENIC SAFETY ANALYSIS

1. **System Design Documents**

- 1.1 A written system purpose and equipment parameters with operation description, shall be prepared to serve as an overview of the system for the Cryogenic Safety Committee (CSC) and as an introduction for cryogenic facility trainees.
- 1.2 Complete and accurate Process and Instrumentation Drawing (P&ID)s shall be prepared and approved in accordance with [C-A-OPM 13.6.1.](#)
- 1.3 An active component list (instrument and valve summary), labeling requirements, and a description of all active devices of the system shall be prepared. These devices would normally include valves, gages, transducers, brakes, pressure and temperature switches, and rupture disks. In the system, all of these devices shall be identified with permanent tags.
- 1.4 A list of the system control loops, alarms, interlocks and a description of normal operations of each loop or interlock. This shall include, as appropriate, the Oxygen Deficiency Hazard (ODH) controls for personnel protection.

2. **System Operating Documents**

- 2.1 Operations procedures that describes normal operational scenarios shall be prepared for the system, in accordance with the Department Policy for the Conduct of Operations. All revisions to the operating procedures, which could present a hazard to personnel, shall be submitted to the CSC as determined by the head of the Cryogenic Systems Group or the Chief Mechanical Engineer.
- 2.2 Any checklists required for startup, shutdown, or normal operation of the system, shall be included in the operating procedures.
- 2.3 The qualification and training requirements of cryogenic personnel, beyond those required in this Document, shall be defined and documented by the System Manager. See also [SBMS Training and Qualification](#)

3. **Safety Analysis and Documentation**

- 3.1 A System Hazard Analysis shall be performed for all cryogenic engineered systems. The System Hazard Analysis shall be performed to identify hazards associated with component failure modes and functional relationships of components and equipment comprising the system. Such analyses should identify all components and equipment whose performance, performance degradation, functional failure, or inadvertent functioning could result in a hazard. The analysis should include a determination of the modes of failure including all single point failures and credible multiple failures, and the effects on safety when failures occur in system components and equipment. The analysis also shall

verify compliance with applicable safety requirements. Techniques that may be used to complete the System Hazard Analysis include Failure Modes and Effects Analysis ([C-A-OPM-ATT 9.6.1.b](#)), Fault Tree Analysis ([C-A-OPM-ATT 9.6.1.c](#)), and What-If Analysis ([C-A-OPM-ATT 9.6.1d](#)).

3.2 All safety analyses shall be documented. Safety analysis documentation shall address the following elements:

3.2.1 System Description

This section is a summary description of the physical and functional characteristics of the system and its components. Reference to more detailed system and component descriptions, including specifications and detailed review documentation shall be supplied when such documentation is necessary. The capabilities, limitations and interdependence of these components shall be expressed in terms relevant to personnel and equipment safety. The system and components shall be addressed in relation to its mission and its operational environment. System block diagrams or functional flow diagrams may be used to clarify system descriptions.

3.2.2 Data

This section shall summarize the data and assumptions, if any, used to determine the safety aspects of design features.

3.2.3 Safety Analysis Results

This section shall be a summary or a total listing of the results of safety analyses. Contents and formats may vary according to the individual requirements of the program. The following are the content and format requirements for Safety Analysis Results:

- a. A summary of the results.
- b. A listing of identified hazards, in narrative or matrix format, to include the following information:
 - (1) System/Subsystem/Unit. Enter the particular part of the system that this analysis is concerned with. For example; cryogenic pump, to distinguish from a vacuum pump.
 - (2) Component(s) Failure Mode(s). All component failure modes which can result in a hazard. Failure modes generally answer the question of “how” it fails.

- (3) Subsystem Failure Mode(s). The subsystem failure mode descriptions are similar to the component descriptions, however, the emphasis is now placed on failures affecting interfacing subsystem operations
- (4) System Component/Phase. The particular phase/component that the analysis is addressing. This could be a system, subsystem, component, operating/maintenance procedure or environmental condition.
- (5) System Event(s) Phase. The configuration, or phase of operation, of the system when the hazard could be encountered, such as, maintenance, operation, interlock testing, etc.
- (6) System Operation Description. A description of what is normally expected to occur as the result of component/system operation or performance of an operating/maintenance action.
- (7) Hazard Description. A brief description of the hazard, such as “Cryogen leak from power lead can.” Also, a complete description of the potential/actual hazards inherent in the item being analyzed, or resulting from normal actions or equipment failure.
- (8) Hazard Identification/Indication. A description of operator indications which include all means of identifying the hazard to operational and maintenance personnel.
- (9) Effect on System. A description of the detrimental effects which could be inflicted upon the system or personnel, as a result of the hazard. Possible upstream and downstream effects also shall be described.
- (10) Risk Assessment. A risk assessment for each hazard. This is the classification of hazard severity and probability of occurrence, as defined in ESH Standard 1.3.3, Safety Analysis Reports / Safety Assessment Documents.
- (11) Recommended Action. The recommended action required to eliminate or control the hazard. Sufficient technical detail is required in order to permit the design engineers and the customer to adequately develop and assess design criteria resulting from the analysis. Include alternate designs and life cycle cost impact where appropriate.

- (12) Effect of Recommended Action. The effect of the recommended action on the assigned risk assessment. Cost/schedule/performance penalties also shall be addressed.
- (13) Remarks. Any information relating to the hazard not covered in other blocks.
- (14) Status. The status of actions to implement the recommended, or other, hazard controls.
- (15) Caution and Warning Notes. A complete list of warnings, cautions, and procedures required in operating and maintenance manuals and for training courses.

3.2.4 Attach FMEA, Fault Tree, and/or "What-If" analyses used to determine the hazards in the system.

4. Engineering Documents

- 4.1 Calculations and/or test results demonstrating the adequacy of the relief system shall be documented.
- 4.2 Calculations and/or test results shall be prepared to verify that stress levels in materials comply with the requirements of the ASME Code and DOE Order 420.1. For designs that are not explicitly covered by the ASME Code, the safety analysis shall show compliance with the intent of the Code and good engineering practice.
- 4.3 Material certifications, test data, or data sheets, shall be obtained and/or documented for any unusual materials used in the system.
- 4.4 Other calculations required by good engineering practice shall be prepared and documented.

5. Maintaining Safe Operation

- 5.1 Documentation of the system shall be kept current.
- 5.2 Plans for maintenance and operations shall be prepared and approved before operations begin.
- 5.3 Operator training and qualification records shall be maintained by the Department.

6. Inspections

- 6.1 Inspections by the CSC may be performed during the review in order to further acquaint the Committee with the system and to clarify safety features of the system.
- 6.2 Inspections by the CSC may be performed as required during operations to verify continued system safety.