C-A OPERATIONS PROCEDURES MANUAL

ATTACHMENT

9.6.1.d What-Ifs Analysis

Text Pages 2 through 3

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

Hand Processed Changes

HPC No.	Date	Page Nos.	Initials

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

Date

WHAT-IFS ANALYSIS

Introduction

This analysis technique examines the consequences of system failures and upsets, as well as procedural errors. This method of analysis examines subsystem rather than components and looks at the effects of external influences on the system. The purpose of this analysis is to reveal any hidden flaws in the design or procedure errors which could present a hazard to personnel and/or equipment.

Procedures using the Process and Instrumentation Drawing (P&ID)s and procedures, "What-if" type questions are asked about each unique mode in the system. These questions are categorized as follows:

a. Each component shall be viewed for unsafe conditions arising from loss of electrical power, loss of instrument air, loss of cooling water, and loss of cryogen, as appropriate.

b. Each system shall be reviewed to uncover safety problems arising from contamination in the process stream.

c. Every cold subsystem in the system shall be reviewed for safety hazards involving loss of insulating vacuum. Particular attention here shall be paid not only to the loss of vacuum, but also damage occurring during a subsequent warmup as cryo-pumped gas evolves, pressurizing the vacuum space.

d. Cryogenic systems should be reviewed to demonstrate that a system will remain safe after refrigeration is lost due to loss of compressors, engines, heat exchangers, vacuum, or power.

e. Each system shall be analyzed for the effects of nature (rain, wind, fire, etc.) which have some reasonable chance of occurring.

f. Each system shall have its assumptions subjected to the scrutiny of a What-If Analysis; i.e., what if the air system fails.

g. Where the failure of equipment poses a hazard, "What-If" questions shall be asked regarding equipment reliability; i.e., what if the drive shaft fails on an expansion engine.

h. Where there is an operator interacting with the system, "What-If" questions shall be asked. (In general, if the FMEA has been completed, the operator should be able to position any single element (valve) without a hazard.)

i. Each subsystem shall be examined for credible multiple failure. (This section may be done in the format of a system Hazards Analysis in Attachment 1.)

Procedures

1. Work with P&IDs and system procedures (operating, repair, etc.).

2. Go through each step of the procedure and examine the consequence of each action specified.

3. Questions of multiple failures shall also be asked (i.e., what if step n of a procedure is initiated and there is a failure of device m?) These questions shall be restricted to credible failures.

4. Evaluate the consequences of each "What-If" situation.

5. Determine the risk for each hazard. This is the classification of hazard severity and probability of occurrence, as defined in ES&H Standard 1.3.3.

6. Decisions shall be made concerning the adequacy of safety. The design shall be approved for safety, or unacceptable risks must be corrected prior to approval.

Documentation

All "What-If" situations analyzed shall be documented using a "What-If" worksheet. Each description shall completely and unambiguously describe each element. Design changes shall be noted by drawing and/or change number. Procedural changes shall be defined by step number.

Component______________________________
____
Location______________________________
Date______________________________
By______________________________

WHAT-IF WORKSHEET

WHAT-IF	CONSEQUENCE/HAZARD	RISK ASSESSMENT	CONCLUSION/RECOMMENDATIONS