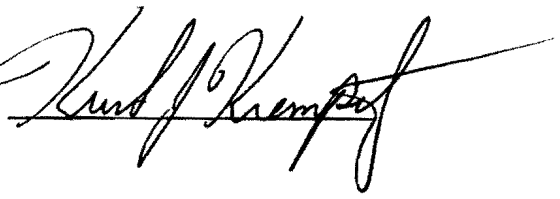
ECN, ECS Safety Documentation, Analysis, Etc. per ESH 5032TA

3740.224-EN-327

K. Dixon
November 21, 1991

Checked by 

1.0 Documentation Requirements

1.1.1 Introduction

At DAB is a large liquid argon HEP calorimeter designed to function in the P-Pbar collider at the D0 section of the Tevatron Accelerator. It contains 5200 gallons of LAr in the CC cryostat, and approximately 3000 gallons in each of two, a north and south, end cryostats (ECN and ECS).

These low pressure vessels are filled with detector modules built of stainless steel, copper and depleted uranium. The LAr functions as the ionization medium, and the spatial and temporal collection of the charge of charged electrons identifies the passage of charged particles. The collection of these charges in 4 pi is related to the energy of the particles and their measurement is called calorimetry.

The contained LAr is isolated from the ambient temperature in specially designed, vacuum jacketed and superinsulated vessels (cryostats) which are provided with liquid nitrogen cooling to the ullage spaces.

1.1.2 Flow Sheets

System flow sheets, 3740-ME-222394, sheets 1 and 2, Revision W, were provided to the Cryosafety Panel in November of 1991.

1.1.3 Operating Procedures

Operating procedures for all cryostats and ancillary systems have been provided to the Panel. These procedures are updated continuously as the system is updated and more experience is gained.

1.1.4 Personnel Qualification and Training

The personnel qualification and training was performed during the CC and ECN cooldown/fill operations which is supplemented by extensive cryogenic operating experience by most of the lead operators (see paragraph 4.3 for more detail). The recent experiences of operating the CC

and ECN cryostats led to modifications of the operating procedure which will now be a more valuable tool to operate the ECS vessel. In the second and subsequent fills, these operators will carefully and fully train others using fully tried and tested procedures (see 4.2).

1.1.5 Particular Documentation

These requirements are addressed in 3740.224-EN-323, -329, the "ECN(ECS) Pressure and Vacuum Vessel Engineering Notes".

1.1.6 Piping Components List

The list is in the D0 Piping Components, 3740.510-EN-193, D. Clark et. al. delivered to the Panel along with the updated flow schematic.

2.0 Analysis Requirements

2.1 Failure Mode and Effects Analysis

The FMEA is appended to this document

2.2 "What If" Analysis

The "What If ...?" is appended to this document

2.3 Hazard Analysis

The hazard analysis is in the form of an ODH analysis, 3740.510-EN-258, D. Clark and J. Michael. Modifications are now underway to take into account the entire detector moving into the Collision Hall and the increased flow to and volumes of the Muon Chambers.

3.0 Engineering Calculations

3.1 Relief Device Adequacy

The adequacy of the relief devices is addressed in 1.1.5 above.

3.2 Stress Levels

Flexibility and stress calculations for the cryostat piping is addressed in D0 Engineering Note 3740.510-EN-312.

3.3 Other Calculations

The only warn structural components having safety implications are the carriages which support the cryostats on the center beam of the platform. Each carriage is a welded structure designed in accordance with the rules of the AISC Specification for Structural Steel for Buildings (by hand calculations). The design was then analyzed for deflections using finite element methods, which also served to verify the stress levels in the structural members. Upon delivery, the carriage was load-tested to 125% of its design loading and the deflections were measured at the design load. The design and the finite element analysis are contained in Engineering Note 3740.215-EN-285, and the measured deflections are documented in Engineering Note 3740.214-EN-282. These Notes were submitted for review to the Cryosafety Review Panel as part of the standard documentation procedure. These notes were also submitted to the Mechanical Safety Review Panel.

4.0 Maintaining Safe Operation

4.1 Documents

The D0 cryo group has one of the most extensive Engineering Note, Drawing, and Operating Procedure files at the Laboratory. It will be maintained and augmented as required to continue this high level of support documentation.

4.2 Plans

The D0 Cryosystem is monitored and controlled by a TI565, Programmable Logic Controller. All of the sensor and control work has been designed to

support unmanned steady state (exclusive of cooldown) LAr operation. The system is monitored by a link to: the main D0 Control Room, the CDF Cryogenics area, the Laboratory FIRUS system, and a D0 cryoexpert autodialing system. Experienced D0 personnel will conduct training and qualification classes for a broader group of operators from the RD/Cryogenics Department during subsequent detector cooldown and fills. Long term running would be attended only as required by this group. The Cryoexperts would continue their role for the foreseeable future.

4.3 Training

The operators have now trained themselves from the initial CC and ECN operations. Formal training classes have been to some operators and will be given to all potential ones. Only those operators that have successfully completed the formal operations classes and successfully passed an examination related to their training will be added to the "qualified operator" list. Cryoexperts will be trained as necessary to keep a ready supply on hand for each running period.

The Cryoexperts and "qualified operators" are listed below:

Cryoexperts

NAME	EXPERIENCE
Dixon, Kelly	11 years
Krempetz, Kurt	13 years
Markley, Dan	11 years
Rucinski, Russ	3 years

Qualified Operators

NAME
Cross, Pete
Drennan, Craig
Durando, Dave
Gordon, Steve
Lambin, Bruce

5.0 Inspections

The D0 Cryo personnel will provide any walk through inspections and answer safety related questions that the D0 Cryosafety Panel may have on a schedule of their choosing.

November 21, 1991

ECN, ECS FMEA and "What If" Analyses

Both analyses are done in accordance with Fermilab ES&H Manual 5032TA and address situations, components related to the ECN cryostat. These analyses are exactly the same for the ECS cryostat when identical ECS components are substituted for ECN ones; eg, PV301N is the same as PV101N. Source dewar and transfer line process components are included in the FMEA analysis, but ancillary processes such as air and water are not included.

FMEA Hazard Class Definitions

Safe No mechanical damage or personnel injury

ODH Releases of argon or nitrogen to the atmosphere, possibly threatening personnel. This possibility is taken into account in the ODH analysis.

Mech. Damage Possible damage to equipment, most likely due to overpressurization. Personnel injury is considered sufficiently unlikely and as such, constitutes and acceptable risk.

Unsafe More than negligible possibility of personnel injury even if standard ODH procedures are followed.

COMPONENT			FAILURE OR ERROR MODE	HAZARD OR EFFECT	HAZARD CLASS	REMARKS OR RECOMMENDATIONS
PV	101	N	Fails to open	Lose Ln2 to cooldown condenser	Safe	
			close unexpect.	Lose Ln2 to cooldown condenser	Safe	
			Fails to close	Lower pressure in the ECN	Safe	Low ECN pressure would alarm. Could use PV513N to limit LN2 flow.
			open unexpect.	Lower pressure in the ECN	Safe	Low ECN pressure would alarm. Could use PV513N to limit LN2 flow.
PV	102	N	Fails to open	Lose Ln2 to S.S. operating condenser	Safe	
			close unexpect.	Lose Ln2 to S.S. operating condenser	Safe	
			Fails to close	Lower pressure in the ECN	Safe	Low ECN pressure would alarm. Could use PV513N to limit LN2 flow.
			open unexpect.	Lower pressure in the ECN	Safe	Low ECN pressure would alarm. Could use PV513N to limit LN2 flow.
MV	103	A	Open	Normal	Safe	
			Closed	PT104A blocked	Safe	ECN pressure is indicated by PT130A also.
PT	104	A	fails	Lose ECN pressure indication	Safe	ECN pressure is indicated by PT130A also.
MV	105	A	Open	Capped after outlet	ODH	ECN gas sample port. No safety hazard involved even without cap.
			Closed	Normal	Safe	
HX	106	N	Rupture	Cause ECN to relieve	Safe	Relief capacity of ECN is adequate to handle this case. See EN323
HX	107	N	Rupture	Cause ECN to relieve	Safe	Relief capacity of ECN is adequate to handle this case. See EN323
PV	108	V	Fails to open	Unable to establish ECN vacuum	Safe	Would be discovered before anything was put in the ECN.
			close unexpect.	Unable to establish ECN vacuum	Safe	Would be discovered before anything was put in the ECN.
			Fails to close	Will not be able to use VP146V	Safe	Would be discovered before anything was put in the ECN.
			open unexpect.	ECN insulating vacuum gets soft	Safe	Insulating vacuum would be on order 10E4 torr instead 10E6 torr
PSV	109	V	Fails to relieve	Pressure in the ECN Vacuum Vessel	Safe	Lift plate. Relief on vacuum piping would open. [2 level failure case]
			open unexpect.	Lose ECN insulating vacuum	Safe	Relief capacity of ECN is adequate to handle this case. See EN263
PT	110	N	fails	Lose indication of condenser pressure	Safe	Affects PV110N, see PV110N failure mode effect analysis
PV	110	N	Fails to open	Raise ECN condenser temperature	Safe	PSV111N would relieve. ECN pressure would build very slowly.
			close unexpect.	Raise ECN condenser temperature	Safe	PSV111N would relieve. ECN pressure would build very slowly.
			Fails to close	condensers can make LAr rain	Safe	ECN pressure would decrease.
			open unexpect.	condensers can make LAr rain	Safe	ECN pressure would decrease.
PSV	111	N	Fails to relieve	Overpressure condensing coils	Mech. Damage	Failure rate: Fail to open 1 in 100,000 demands. [2 level failure case]
			open unexpect.	Vents nitrogen	ODH	Vents inside building
RD	112	A	Fails to rupture	Will not back up a PSV113A failure	Safe	RD112A is not needed for any probable relief case. [3 level failure case]
			Rupture	Will vent ECN outside	Safe	
PSV	113	A	Fails to relieve	ECN pressure will raise to 18 psig	Safe	RD112A will backup this failure mode. [2 level failure case]
			open unexpect.	Will vent ECN outside	Safe	
PV	114	A	Fails to open	Block direct GAr line from Ar dewar	Safe	It would be possible to use the UV piping for GAr feed.
			close unexpect.	Block direct GAr line from Ar dewar	Safe	It would be possible to use the UV piping for GAr feed.
			Fails to close	Allows GAr from Ar dewar	Safe	Can stop GAr supply by closing PV611A or MV648A.
			open unexpect.	Allows GAr from Ar dewar	Safe	Can stop GAr supply by closing PV611A or MV648A.

COMPONENT			FAILURE OR ERROR MODE	HAZARD OR EFFECT	HAZARD CLASS	REMARKS OR RECOMMENDATIONS
PV	115	A	Fails to open	Block vac. pumps from ECN pres. vess	Safe	Can evacuate ECN press. vessel thru drain line.
			close unexpect.	Block vac. pumps from ECN pres. vess	Safe	Can evacuate ECN press. vessel thru drain line.
			Fails to close	ECN press. vess. tied into UV piping	Safe	Can isolate UV piping with MV454UV.
			open unexpect.	Vac. pumps tied into ECN's cold GAr	Safe	PV115A is interlocked, can't open with ECN positive pressure.
mv	116	N	Open	Normal	Safe	
			Closed	Blocks PT110N	Safe	PV110N will not control correctly.
mv	117	N	Open	Capped after outlet	CDH	Nitrogen sample port from ECN condensers
			Closed	Normal	Safe	
PV	118	A	Fails to open	Will not be able to fill ECN with LAr	Safe	Will have to fix problem to fill-might be safety related toggle switch.
			close unexpect.	Stops LAr fill of ECN	Safe	Will have to fix problem to fill ECN with LAr.
			Fails to close	ECN LAr is not doubly isolated.	Safe	Would need 2 additional failures for any problem to occur from this
			open unexpect.	ECN LAr is not doubly isolated.	Safe	Would need 3 additional failures for any problem to occur from this
CV	119	H	Sticks closed	Blocks He bottles from PV119A	Safe	Gas bottle GB119H has helium to operate PV119A for some time.
			Sticks open	GB119H can bleed down	Safe	During a cryostat move could cause PV119A to open but bayonet is capped.
PV	119	A	Fails to open	Will not be able to fill ECN with LAr	Safe	Will have to fix problem to fill ECN with LAr.
			close unexpect.	Stops LAr fill of ECN	Safe	Will have to fix problem to fill ECN with LAr.
			Fails to close	ECN LAr is not doubly isolated.	Safe	Would need 2 additional failures for any problem to occur from this
			open unexpect.	ECN LAr is not doubly isolated.	Safe	Would need 2 additional failures for any problem to occur from this
PSV	119	H	Fails to relieve	PV119A would not work	Safe	PRV119H would have to fail for this failure to occur [2 level failure]
			Opens unexpect.	Vents helium	CDH	Would increase frequency of changing helium bottles
PRV	119	H	close unexpect.	Lose low pressure He in PV119A	Safe	PV119A would still work
			open unexpect.	Causes PSV119H to relieve	Safe	PV119A would still work. Would go thru more He bottles.
PS	119	H	fails	Lose indication of PV119A position	Safe	PS119H redundantly shows position of PV119A
EV	119	H	fails	Lose control of PV119A	Safe	Can use PV118A in place of PV119A
EH	120	A	fails	Can't warm up ECN contents	Safe	Alternative methods would be possible.
PV	121	V	Fails to open	Would not have VP146V on line	Safe	Insulating vacuum would be on order 10E4 torr instead 10E6 torr
			close unexpect.	Turns off VP146V	Safe	Interlocked, insul. vac. d.p. turns off when PV121V is closed.
			Fails to close	Backstreaming into insu. vac. poss.	Safe	PV125A upstream protects the insul. vac. from backstreaming.
			open unexpect.	Backstreaming into insu. vac. poss.	Safe	PV125A upstream protects the insul. vac. from backstreaming.
DPT	122	A	fails	Lose indication of LAr level	Safe	Other devices give LAr level in ECN.
EI	123	A	fails	Lose indication of LAr level	Safe	Other devices give LAr level in ECN.
mv	124	A	Open	Bypasses DPT122A	Safe	See DPT122A fails
			Closed	Normal	Safe	
PV	125	V	Fails to open	Isolates VP146V	Safe	Insulating vacuum would be on order 10E4 torr instead 10E6 torr
			close unexpect.	Isolates VP146V	Safe	Insulating vacuum would be on order 10E4 torr instead 10E6 torr
			Fails to close	Backstreaming into insu. vac. poss.	Safe	No danger involved [2 level failure case]
			open unexpect.	Backstreaming into insu. vac. poss.	Safe	No danger involved [2 level failure case]

COMPONENT			FAILURE OR ERROR MODE	HAZARD OR EFFECT	HAZARD CLASS	REMARKS OR RECOMMENDATIONS
TG	126	V	fails	Lose indication of D.P. inlet pressure	Safe	
CC	127	V	fails	Lose indication of D.P. inlet pressure	Safe	
PV	128	A	Fails to open	Isolates the venting of PSV113A	Safe	If PV128A doesn't open by operating procedures we will not fill the ECN.
			close unexpect.	Isolates the venting of PSV113A	Safe	PV128A will be mechanically locked open. [2 level failure case]
			Fails to close	Leak thru relief in ECN P&P sequence	Safe	
			open unexpect.	Leak thru relief in ECN P&P sequence	Safe	
EV	128	I	fails	Lose control of PV128A	Safe	See PV128A failure mode effect analysis
EI	129	E	fails	Lose indication of RD112A leakage	Safe	Large leakages can be determined through other means
PT	130	A	fails	Lose ECN pressure indication	Safe	
CC	131	V	fails	Lose ECN insul. vac. pressure ind.	Safe	
TS	132	E	fails	No sensing of LN2 in vent manifold	Safe	Both condenser inlet valves are interlocked closed if this device fails
PT	133	A	fails	Lose VPT pressure indication	Safe	
PT	134	A	fails	Lose VPT pressure indication	Safe	
DPT	135	A	fails	Lose LAr temp. gradient information	Safe	
RO	136	N	gets clogged	Lose exhaust purge flow	Safe	Will have possibility of Ar freezing in exhaust line.
MV	137	A	Open	Bypasses DPS138A	Safe	Lose ind. of LAr flowrate at ECN. FM671A indicates flowrate at LAr dewar.
			Closed	Normal	Safe	
DPS	138	A	fails	Lose ECN LAr flow rate information	Safe	FM671A indicates flowrate at LAr dewar
FM	139	A	fails	Lose ECN LAr flow rate information	Safe	FM671A indicates flowrate at LAr dewar
PT	140	A	fails	Lose VPT pressure indication	Safe	
mv	141	A	Open	A cap looks at ECN GAr	ODH	
			Closed	Normal	Safe	
TG	142	V	fails	Lose D.P. inlet press. indication	Safe	Some vacuum valves will close on interlocks from TG142V signal.
mv	143	A	Open	A cap looks at ECN LAr	ODH	Due to heat leak, LAr can't be delivered thru this 1/4" tube.
			Closed	Normal	Safe	
mv	144	A	Open	A cap looks at ECN GAr	ODH	
			Closed	Normal	Safe	
mv	145	A	Open	Normal	Safe	
			Closed	PT130A blocked	Safe	ECN pressure is indicated by PT104A also.
VP	146	V	fails	Lose D.P. on ECN insul. vacuum	Safe	PV125V and PV121V close by interlock to isolate VP146V.

COMPONENT			FAILURE OR ERROR MODE	HAZARD OR EFFECT	HAZARD CLASS	REMARKS OR RECOMMENDATIONS
MV	491	N	Open	Normal	Safe	Permits LN2 to condensers
			Closed	Stops LN2 to condensers	Safe	Loss of liquid nitrogen, see "What if" analysis
PSV	492	N	Fails to relieve	Overpressure piping	Mech. damage	Failure rate: Fail to open 1 in 100,000 demands
			open unexpect.	Vents nitrogen	CDH	Vents inside building.
mv	493	N	Open	Capped after outlet	CDH	
			Closed	Normal	Safe	
mv	494	A	Open	Capped after outlet	CDH	
			Closed	Normal	Safe	
PV	1403	N	Fails to open	No subcooling of LN2 to condensers	Safe	Lower LN2 quality to cryostat condensers.
			close unexpect.	Lose subcooling of LN2 to condensers	Safe	Lower LN2 quality to cryostat condensers.
			Fails to close	LN2 flows into exhaust pipe	Safe	Will waste some LN2, little or no effect on cryostat condensers.
			open unexpect.	LN2 flows into exhaust pipe	Safe	Will waste some LN2, little or no effect on cryostat condensers.
CV	1404	N	Sticks open	Allow backflow	Safe	Exhaust line purged by N2 gas under normal operation.
			Sticks closed	Lose LN2 manifold subcooling	Safe	See PV1403N closed.
MV	801	H	Open	Normal	Safe	
			Closed	Lose GB814H as He gas source	Safe	GB815H, GB816H, and GB119H backup GB814H.
MV	802	H	Open	Normal	Safe	
			Closed	Lose GB815H as He gas source	Safe	GB814H, GB816H, and GB119H backup GB815H.
MV	803	H	Open	Normal	Safe	
			Closed	Lose GB816H as He gas source	Safe	GB814H, GB815H, and GB119H backup GB816H.
MV	804	H	Open	Normal	Safe	
			Closed	Isolates GB814H and GB815H	Safe	GB816H and GB119H provide He gas to PV119A.
MV	805	H	Open	Normal	Safe	
			Closed	Isolates GB816H	Safe	GB814H, GB815H, and GB119H provide He gas to PV119A.
PSV	807	H	Fails to relieve	Overpressure piping	Mech. damage	Failure rate: Fail to open 1 in 100,000 demands
			open unexpect.	Vents gaseous helium	CDH	Vents inside building.
PRV	808	H	Set too high	PSV807H on GHe line relieves	Safe	
			Closed	Isolates GB814H and GB815H	Safe	GB816H and GB119H provide He gas to PV119A.
PRV	809	H	Set too high	PSV807H on GHe line relieves	Safe	
			Closed	Isolates GB816H	Safe	GB814H, GB815H, and GB119H provide He gas to PV119A.
PI	810	H	fails	Wrong ind. of He gas bottle press,	Safe	Valves of gas bottles will be closed prior to disconnecting them.
PI	811	H	fails	Wrong ind. of He gas bottle press,	Safe	Valves of GB816H will be closed prior to disconnecting it.
PS	812	H	fails	False indication of low GHe press.	Safe	Can use PI810H to check GHe pressure.
PS	813	H	fails	False indication of low GHe press.	Safe	Can use PI811H to check GHe pressure.
PS	826	H	fails	Lose alarm signal to control system	Safe	Will lose one of the two cold valve helium supply alarms.
mv	825	H	Open	Normal	Safe	
			Closed	Isolates PS813H	Safe	See PS813H fails

ECN/ECS "What-If"

"WHAT IF"	CONSEQUENCE/HAZARD	CONCLUSION/RECOMMENDATIONS
Leaks occur?	Oxygen Deficiency Hazard may occur due to cryogens leaking into the building.	Leaks of reasonable size have been anticipated by the ODH analysis and appropriate provisions made so they present no personnel or equipment danger (i.e. the ODH class is 0).
The vacuum of the ECN is spoiled?	Loss of vacuum.	The loss of vacuum of the cryostat is a relief case looked at in D0 engineering note 6. A heat leak of approx. 2.7 KW will occur causing an additional loading of the nitrogen condensers. The required relief capacity for LOV is 114 scfm. The relief system on the EC vessels has a capacity of at least1600 scfm
There is a loss of vacuum on a transfer line?	Increased heat load, lower quality of transferred liquid, would frost up the effected piping.	There is no safety hazard if this occurred. The problem would be discovered by either a visual inspection of frost and/or questionable operational behavior.
There is a fire under or around the ECN?	The ECN could relieve and possible loss of signal or valve operators could occur.	Fire exposure of the ECN is looked at in D0 Engineering Note 6. The required relief capacity for fire is 450 scfm. The relieving system on the EC vessels has a capacity of at least1600 scfm. See also the "What If" there is a loss of signals or valve operators occurs?
There is a fire in the cryocorner?	Could lose electrical signals to and from the ECN. Some of the o-rings on bayonets could fail.	See the "What if" there is a loss of signals or valve operators occurs? and "What if" a leak occurs?
There is a fire in the Ar dewar room?	Could lose electrical signals to and from the ECN. Some of the o-rings on bayonets could fail.	See the "What if" there is a loss of signals or valve operators occurs? and "What if" a leak occurs?
There is a loss of signals or valve operators?	We would lose the ability to control valves.	All control valves fail in the closed positions. All reliefs and rupture discs remain operational. After some time trapped volume reliefs could relieve. The ECN could relieve also after a long period of time.
A cap on an EC rotating bayonet is missing or is not clamped on?	Would not be able to successfully pass pump and purge part of the ECN procedures.	It is written into the ECN procedures pump and purge section 8.3.0 that the caps are to be installed. If a cap is missing we would not successfully be able to pull a vacuum on that line. If a cap was in place but not clamped, then it would become unseated after the first backfill to positive pressure and the subsequent pumpdown would fail. In either case, the problem would be discovered before cryogens entered the line.
There is an earthquake?	Damage to the piping system could occur.	The ANSI B31.1-1986 piping code under par. 101.5.3 states that "The effect of earthquakes, where applicable, shall be considered in the design of piping, piping supports..." The effect of earthquakes are not applicable to the region of Illinois where Fermilab is located. The Uniform Building Code shows that Fermilab is in a Class 0 seismic zone which means no design provisions for earthquakes are required.
There is a loss of electrical power?	Backup power will be required to maintain operation of the system.	Sustained loss of electrical power will result in critical equipment running on the Emergency Power Generator. The instrument air, vacuum pumps and controls are (will) all be EPG powered. Should the EPG fail before the return of commercial power the equipment is lost, see below.

"WHAT IF"	CONSEQUENCE/HAZARD	CONCLUSION/RECOMMENDATIONS
There is a loss of instrument air?	Valves will close.	Safe. The primary system is backed up for several hours with a tube trailer. All valves are failsafe, i.e. they close on the loss of instrument air. Reference the failure mode and effects analysis.
There is a loss of cooling water?	The main cooling water supply might be in jeopardy if a system was not designed properly.	The vacuum and instrument air equipment have a primary, emergency powered, immediate start, closed loop, fan blown radiator, redundant pump, glycol stream to put the heat load on the building system and provide lower summertime coolant temperatures. Loss of the secondary system, or commercial power if the emergency generator functions, does not effect the cooling provided to the rotary equipment.
There is a loss of Liquid nitrogen?	Cooling will be lost and will cause the Vessels to warm, boil off, and vent.	The loss of liquid nitrogen denies the detector its necessary cooling and it will pressurize and vent. The rate of loss is calculated to be only 0.45 gpm of liquid argon on average, which is very slow. The loss of liquid nitrogen does not provide a personnel or equipment danger.
Some kind of contamination occurs?	The contamination could restrict flows.	Continued or serious one-time contamination of the coolant stream with frozen solids will result in a loss of liquid nitrogen, see above.
There is some kind of equipment failure?	A piece of equipment will stop working.	100% redundancy in mechanical forepumps provide for vacuum equipment failure in the operating mode. The insulating vacuum can stay at a "good vacuum" provided there are no large leaks and the cryostat stays cold. Instrument air is backed up by 8 or more hours of high pressure gaseous nitrogen. All valves close on air failure. Expected equipment modes do not provide a personnel or equipment danger.
An operator makes a procedural error?	Upset of the system may occur.	Any one operator procedural or console error can cause any one component to act improperly which is comparable to a component failure. Failure of equipment is covered above and failure of valves was covered in the FMEA. A single operator error cannot cause a safety problem.
Any of the other cryostats drain into ECN by error.	Possible contamination could spread, ECN can get pressurized and the relieving capacity can be overwhelmed.	Redundant fill/drain valves are in place to minimize any communication between vessels. A locked switch independent of the PLC coupled with good operating procedures will reduce an error of this type when the modules within the cryostat are warm and high vaporization rates may occur.
The storage dewar fills the ECN when the modules are warm.	ECN can get over pressurized and the relieving capacity can be overwhelmed.	Redundant fill/drain valves are in place to minimize the effects of any valve opening done in error. A locked switch independent of the PLC coupled with good operating procedures will reduce an error of this type when the modules within the cryostat are warm and high vaporization rates may occur.