National Spherical Torus eXperiment Upgrade

NSTX-U Recovery Project FMECA and Hazard Analysis Plan

NSTX-U-PLAN-037-00

6/13/19

Stefan Gerhardt

Digitally signed by Stefan Gerhardt
DN: cn=Stefan Gerhardt, o=Physics, ou=PPPL, email=sgerhard@pppl.gov, c=US
Date: 2019.06.13 20:39:26 -04'00'

Written By: Stefan Gerhardt, Systems Integration

Peter Dugan

Digitally signed by Peter Dugan
Date: 2019.06.14 09:08:16 -04'00'

Reviewed By: Peter Dugan, Systems Engineering

Jessica Malo

Digitally signed by Jessica Malo
Date: 2019.06.14 10:48:10 -04'00'

Reviewed By: Jessica Malo, Accelerator Safety Specialist

Yuhu Zhai

Digitally signed by Yuhu Zhai
Date: 2019.06.14 12:00:51 -04'00'

Reviewed by: Yuhu Zhai, NSTX-U Recovery Project Engineer

Timothy N. Stevenson

Digitally signed by Timothy N. Stevenson
Date: 2019.06.14 13:52:46 -04'00'

Reviewed By: Tim Stevenson, NSTX-U Engineering Operations Head

Jerry D. Levine

Digitally signed by Jerry D. Levine
DN: cn=Jerry D. Levine, o=Princeton Plasma Physics Laboratory, ou=ESH&S Department, email=jlevine@pppl.gov, c=US
Date: 2019.06.14 17:01:01 -04'00'

Reviewed By: Jerry Levine, Head of ES&H

Andres Castaneda

Digitally signed by Andres Castaneda
Date: 2019.06.17 07:50:17 -04'00'

Reviewed By: Andres Castaneda, NSTX-U QA Representative

Richard J. Hawryluk

Digitally signed by Richard J. Hawryluk
Date: 2019.06.17 08:38:26 -04'00'

Approved By: Rich Hawryluk, NSTX-U Recovery Project Director

Revision Log

Date	Rev	Change
6/13/19	0	Initial Release

References: 3

Definitions 4

1: Scope 5

2: Consequence, Severity, and Risk 6

2.1 Consequence, Severity and Detectability Tables 6

2.2 Risk Table for Safety Analysis 8

2.3 Risk Table and Analysis for FMECA 9

3: Recovery Project FMECA Format 11

4: Hazard Analysis Format 14

5: Assumptions on Mitigation and Detection Systems 14

5.1 Unmitigated Safety Analysis 14

5.2 FMECA Assumptions on Detection/Mitigation Systems 14

6: Calculations of Failure Rates and Failure Probabilities 15

7: Example Failure Modes 16

8: Standard Downtime Assumptions 18

References:

[1] ASO-180529_SPG-01, *PRELIMINARY CONCLUSIONS REGARDING THE PROCESS AND FORMAT OF RISK ANALYSIS IN THE NSTX-U SAD*
[2] NSTX-U-DOC-123, *NSTX-U Recovery Project Hazard Analysis Report*
[3] Dependability_190120.xls (presentation by C. Neumeyer)
[4] DOE O 420.2C, *Safety of Accelerator Facilities*
[5] ENG-008, *Failure Modes and Effects Analysis*
[6] MIL-STD-1629A, *Procedure for Performing a Failure Mode, Effects, and Criticality Analysis*
[7] DOE-STD-6003-96, Safety of Magnetic Fusion Facilities: Guidance
[8] DOE-STD-3009-2014, *PREPARATION OF NONREACTOR NUCLEAR FACILITY DOCUMENTED SAFETY ANALYSIS*
[9] NSTX-CRIT-0001-02 *NSTX Structural Design Criteria*
[10] NSTX-U-RQMT-GRD-001, *General Requirements Document*

Definitions

Acronym	Definition	Explanation
AOE	Accelerator Operations Envelope	The set of systems and controls that must be in place during operations in order to protect the investment in NSTX-U. The AOE includes both the systems, and some information regarding limit values of those systems. The AOE also may include limits of similar nature to those in the ASE, but more restrictive.
ASE	Accelerator Safety Envelope	The ASE defines the credited controls necessary to protect workers, the public, and the environment from accelerator specific hazards. Violations of the limit set in the ASE result in a USI. The ASE is a fundamental requirement for the ASO, and is approved by the DOE-PSO.
ASO	Accelerator Safety Order	The DOE Order DOE O 420.2c, *Safety of Accelerator Facilities* was added to the PPPL contract in 2016.
	Accelerator Specific Hazard	Any hazard to workers, the environment, or public, whose nature is uniquely defined by the configuration of NSTX-U systems and not fully mitigated by PPPL standard safety management programs (ESHD-5008).
	Analyst	Per ENG-008, the analyst is the person completing the FMEA/FMECA for a specific component or system.
	Credited Control	A system or control, either engineered or administrative in nature, that reduces the risk of an accelerator specific hazard from unacceptable to the acceptable range. The credited controls are included in the Accelerator Safety Envelope.
CMPS	Critical Machine Protection System	An engineered system that reduces the risk of a machine failure from the unacceptable range to the acceptable range. The CMPSs are included in the Accelerator Operations Envelope.
FMECA	Failure Modes, Effects, and Criticality Analysis	A formal process to document failure modes, including their probability, consequences, detectability, and risks (criticality).
M&S	Materials and Supplies	Costs associated with procured components and services, as opposed to the costs of PPPL labor.
RPN	Risk Priority Number	The RPN is the product of probability, severity, and detectability. The most significant risks are those with large RPN values.
SAD	Safety Assessment Document	The Safety Assessment Document contains the comprehensive safety analysis for NSTX-U. A comprehensive SAD is a requirement of the Accelerator Safety Order

USI	Unreviewed Safety Issue	The process mandated by DOE O 420.2c for examining proposed changes and as-found conditions to determine if they impact the documented safety analysis. See procedures ESH-025 and D-NSTXU-OP-AD-131
	Validated	A detection method is considered validated when there is a testing and maintenance program associated with it.

Note: Further acronyms can be found in the appendix to the General Requirements Document (NSTX-U-RQMT-GRD-001) [10].

1: Scope

This document describes an integrated plan for both Safety Analysis and FMECA for the NSTX-U Recovery Project. These are related processes, in that:

- Both FMECA and Safety Analysis rely on assessments of failure/event probability and consequence in order to develop an understanding of failure/event risk, and

- Both FMECA and Safety Analysis will be used to develop an understanding of the required mitigating administrative and engineered controls.

There are also important differences between safety analysis and FMECA:

- The FMECA process will be used for developing an understanding of the failure modes of NSTX-U components and systems, and for identifying the systems that need to be in place to protect the investment in NSTX-U. Engineered controls required for this investment protection will be known as “critical machine protection systems” (CMPSs) and will be included in the Accelerator Operations Envelope. Some findings of the FMECA analysis will inevitably feed the safety analysis.

- The safety analysis process is used to analyze risks to workers, the public and the environment. This process will be used to identify the required hazard controls. For those hazards that are “accelerator specific” (see definitions), the controls will be known as “credited controls” and will be included in the Accelerator Safety Envelope [1,2,4].

The NSTX-U FMECA will predominantly consider failure modes of components in, or affecting, the machine core (i.e. inside the TF boundary). Failure modes outside this core scope may be included, but are not the key focus except in cases where those failures impact the machine core. For some systems (the PSS for instance), more sophisticated fault tree analysis may be used in lieu of FMECA analysis.

The NSTX-U safety analysis, which will be included as a central component of the SAD, will cover the totality of NSTX-U hazards, including those outside the NSTX-U test cell. See references [1] and [2] for more information regarding the hazard analysis method described here.

Note that this plan builds on the guidance found in procedure ENG-008, *Failure Modes and Effects Analysis* [5] and MIL-STD-1629A, *Procedure for Performing a Failure Mode, Effects, and Criticality Analysis* [6]. Those documents are recommended for further guidance in developing the FMECA. Ref. [1] provides a comprehensive comparison of the method presented here to the safety analysis which is commonly used in the accelerator community.

2: Consequence, Severity, and Risk

2.1 Consequence, Severity and Detectability Tables

The probability (P) categorization will be as in Table 2.1-1. The quantitative guidance should be used when possible, but it is also acceptable to use the qualitative guidance[1]. These categories are the same as in Refs [1] and [2], but include the category of "incredible events"[2].

***Table 2.1-1**: Probability categories*

P	Category	Qualitative Description	Quantitative Description
0	Incredible Events	Events of extremely low probability of occurrence or of non-mechanistic origin	$P<10^{-6}$/yr
1	Extremely Unlikely Events	Events that are not expected to occur during the lifetime of the facility but may be used to define limiting faults or incidents to be considered in the design	10^{-6}/yr<=P<10^{-4}/yr
2	Unlikely Events	Events that are not anticipated but may occur during the lifetime of a facility	10^{-4}/yr<=P<10^{-2}/yr
3	Anticipated Events	Events of moderate frequency that may occur once or more in the lifetime of a facility	10^{-2}/yr<=P<1/yr
4	Normal Events	Events that are planned to occur regularly in the course of facility operation	P>=1/yr

The severity (S) categories will be as in Table 2.1-2. For any given failure mode, the criterion that leads to the largest value of S shall be selected. Note that the first two columns are relevant

[1] Per Section 5.5.1 of Ref. [7], a qualitative risk analysis is acceptable for below Hazard Category 3 facilities. While NSTX-U is formally classified as an accelerator, it would be called a below Hazard Category 3 facility in the absence of that classification.
[2] While Ref. [8] is not a requirement for NSTX-U, it is of note that the quantitative ranges exactly match those suggested in Table 2 of that reference.

to the FMECA alone, while the last three may be relevant to either the FMECA or safety analysis. These final three columns mimic those that can be found in Refs. [1] and [2].

***Table 2.1-2**: Severity categories*

	FMECA Alone		FMECA or SAD		
S	**Downtime (DT)**	**Cost Impact (C)**	**Personnel Safety**	**Radiological Impact (R)**	**Environmental Impact**
0	No Downtime	no cost impact	no safety impact of any form	No radiological impact of any form	No environmental impact of any form
1	< 1 week	< $10K	Will not result in any discernible impact to any worker	< 0.1 rem to public, < 1 rem to worker	Will not result in any discernible impact to environment
2	1 week <= D < 1 month	$10K <= C < $100K	May cause minor lost-time injury or illness	0.1 rem <= R < 0.5 rem to public, 1 rem <= R < 5 rem to worker	Minor release of pollutants, localized and containable
3	1 month <= D < 1 year	$100K <= C < $5M	May cause serious injury or illness	0.5 rem <= R < 2.5 rem to public, 5 rem <= R < 25 rem to worker	Major release of non-toxic, biodegradable pollutants to air, water, or soil, not contained
4	>= 1 year	>= $5M	May cause death	>= 2.5 rem to public, >= 25 rem to worker	Major release of toxic, non-biodegradable pollutants to air, water, or soil, not contained

In interpreting this table, the following rules should be applied:

- The downtime estimate should include only the time to make the repair or replacement. This may include time for design work, but should not include estimates for programmatic decision-making delays.

- The cost impact should include only the cost to implement the repair or replacement, including both labor and M&S. It should not include any estimate of the cost of the lost operations time.

- For failures of NSTX-U components within the test cell during magnet energization or plasma operations, it should be assumed that access control systems are functioning properly and all personnel are outside the shield walls.[3]

[3] Simultaneous failure of the machine system and the access control system is not considered.

In evaluating the consequences in Table 2.1-2, consequences for both the system under consideration and interfacing systems should be considered. The interface tables in the SRDs or specific Interface Control Documents are appropriate places to determine key lists of interfaces.

If a compensatory action, such as switching to an on-line spare, is used in the assessment of the severity S or probability P, then the compensatory action shall be documented. See Section 3 for additional guidance on compensatory actions.

Detectability (D) is defined as in Table 2.1-3. Here, detectability is defined as the ability to detect and prevent the incipient failure before the full consequence described in Table 2.1-2 has occurred. Detection with no ability to avoid or reduce the impact of the failure should be rated as *remote*.

Note: detectability is only used for the FMECA and not safety analysis.

***Table 2.1-3**: Detectability categories*

D	Category	Description
1	High	A. Validated automatic detection that is a direct measure of failure, or, B. Two or more validated manual detection methods and provides near real-time feedback
2	Moderately High	A. Single validated manual detection methods that are a direct measure of failure and provide near real-time feedback
3	Moderate	A. Single validated manual detection methods that are an indirect measure of failure and do not provide near real-time feedback
4	Low	A. Non Validated detection e.g., Visual, Audible or Tactile inspections
5	Very Low	A. No or remote ability to detect the failure

2.2 Risk Table for Safety Analysis

Safety analysis is related to the protection of workers, the public, and the environment. It is documented in the Safety Analysis Document (SAD). For safety analysis purposes, the risk definitions in Table 2.2-1 and Table 2.2-2 are used, assuming that no mitigations are present.

***Table 2.2-1**: Risk definitions for safety analysis*

High risk	Unacceptable
Medium risk	Unacceptable
Low risk	Acceptable
Extremely low risk	Desirable

***Table 2.2-2**: Mapping of severity and consequence to risk for safety analysis*

	P	0	1	2	3	4
S		Incredible Events	Extremely Unlikely Events	Unlikely Events	Anticipated Events	Normal Events
0	No Impact	0	0	0	0	0
1	Negligible Severity	0	1	2	3	4
2	Low Severity	0	2	4	6	8
3	Medium Severity	0	3	6	9	12
4	High Severity	0	4	8	12	16

When any event or hazard leads to an unacceptable risk in an unmitigated analysis (see Section 5), a control that brings the risk down to an acceptable or desirable level must be implemented. If the event, or hazard, is an accelerator specific hazard, then the control becomes a Credited Control in the ASE. See Ref. [1] for more information on the accelerator community definitions for accelerator specific hazards.

2.3 Risk Table and Analysis for FMECA

For FMECA purposes, the criticality definitions in Table 2.3-1 are used.

***Table 2.3-1**: Criticality definitions*

Concept	Formula	Description
Risk without Detection	$R = P \cdot S$	This value parameterizes the criticality of the failure mode in the absence of any detection or mitigation scheme.
Residual Risk Following Detection	$R_R = P_D \cdot S_R$	This value parameterizes the residual criticality of the failure mode after the detection/mitigation have occured.

Risk Priority Number	$RPN = P \cdot S \cdot D$	This value is the most commonly used parameter in standard FMECA for ranking failure modes by criticality.

Here, these symbols are defined as:

P: Probability of the event/consequence occuring in the absence of any detection/mitigation system, as defined in the first column of Table 2.1-1.

S: Severity if undetected and unmitigated, as defined in the first column of Table 2.1-2.

P_D: Probability of the full consequence if the detection/mitigation scheme is utilized

S_R: Severity after detection/mitigation (R is for "residual")

D: Detectability, as defined in the first column of Table 2.1-3

The definitions of risk alone are provided in Table 2.3-2, and the risk matrix is shown in Table 2.3-3.

***Table 2.3-2**: Risk definitions for FMECA*

High risk	Unacceptable
Medium risk	Unacceptable
Low risk	Acceptable risk if the cost of risk reduction would exceed the improvement gained
Extremely low risk	Negligible risk (desirable)

***Table 2.3-3**: Mapping of severity and consequence to risk for FMECA*[4]

	P	0	1	2	3	4
S		Incredible Events	Extremely Unlikely Events	Unlikely Events	Anticipated Events	Normal Events
1	Negligible Severity	0	1	2	3	4
2	Low Severity	0	2	4	6	8
3	Medium Severity	0	3	6	9	12
4	High Severity	0	4	8	12	16

[4] Note that Tables 2.3-3 and 2.2-2 are the same in this revision to the Plan. However, they are presented differently in case the Project risk tolerance for one area changes.

The following rules shall be utilized in defining the Critical Machine Protection Systems (CMPSs):

1. No failure mode may have an RPN >24.[5] If an RPN>24 is identified, then either the design must change so that one of P, S, or D is reduced, or an appropriate compensatory action specified.

2. If any failure mode presents a risk R≥8, then there must be a mechanism to detect and prevent the failure mode, or an appropriate compensatory action should be specified. See Section 3 for additional guidance on compensatory action. The engineered protection systems that detect and prevent the failures are critical machine protection systems (CMPSs).

3. The residual risk following detection and mitigation (R_R=$P_D S_R$) should be less than 8. If it is not, then either the detection and mitigation systems need to be revisited in order to reduce the residual risk, or an appropriate compensatory action needs to be specified.

Note: In rare cases it may not be possible to reduce the RPN to less than 24, or to reduce R_R to less than 8. In those cases, senior laboratory management must be made aware of the failure mode.

3: Recovery Project FMECA Format

The NSTX-U Recovery Project FMECA will be a spreadsheet, with the fields described below. An example FMECA spreadsheet can be found at this link:

https://docs.google.com/spreadsheets/d/1QJGs8egWZaFJWBznm3fAfSLMANQQ3L7-bqjALy2YR0g/edit#gid=834083317

SBS #: Indenture levels [6] at level 4 or 5 of the SBS will be used to indicate systems. This is consistent with the Project interface definitions, which are also maintained at L4 and L5 of the SBS.

System: The system name based on the SBS (*automatically determined*).

[5] The RPN threshold of 24 is semi-arbitrary, but is based on the observation that the “Low risk” band, corresponding to $P{\cdot}S$ of 4-6, may be unacceptable if the chance of observing the failure is sufficiently small. For $P{\cdot}S$ in the range of 4-6 and remote detectability, the RPN range of 20-30 straddles the proposed threshold of 24. This threshold also ensures that the medium risk failures, with $P{\cdot}S$ of 8-9, trigger the RPN threshold if their detectability is moderate or worse.

Responsible Engineer: The Responsible Engineer responsible for the system (*automatically determined*).

Failure Mode: The specific means by which the function of the component has failed.

Example: Plasma facing component fracture, or magnet overheating

Operations Phase: A value selected from the pull-down list, which may include the following

- All
- Coil Testing and Plasma Operations
- Neutral Beam Operations
- Glow Discharge Cleaning
- LITER Operations
- Bakeout
- Maintenance/Outage

Failure Cause(s): A terse description of the failure cause. Consider cases where the failure cause is driven by an interfacing component. See Section 6 for more descriptions of failure causes.

Example: Excessive magnet I^2t heating, excessive load due to halo currents

Failure Effect(s): A terse description of the failure effect; consider the impact on the higher-level elements of the SBS, or other SBS elements. The interface tables in the SRD and Interface Control Documents should be examined to determine the impact on interfacing elements, which may be more severe than on the element itself.

Example: Magnet unable to provide confining field, needs replaced; exposure of underlying metal structure requires vessel entry to repair.

Probability (P): The probability of the consequence in the absence of detection is taken from a pulldown menu with the values in Table 2.1-1.

Example: The probability of coil damage from overcurrent or overheating, without the DCPS present.

Probability (P_D): The probability of the consequence with detection is taken from a pulldown menu with the values in Table 2.1-1.

Example: The probability of coil damage from overcurrent or overheating, with the DCPS present and functioning correctly.

Severity (S): There are five columns associated with the severity, which are taken from a pull-down menu of items in Table 2.1-2.

Detectability (D): The detectability is taken from a pull-down menu of items in Table 2.1-3.

Risk (R): The risk is given by $P \cdot S$ (*automatically determined*).

Risk Priority Number (RPN): The risk priority number is given by $P_D \cdot S \cdot D$ (*automatically determined*).

Detection/Mitigation System SBS #: For $R \geq 8$, a detection system needs to be selected from the pull-down menu of SBS #s. Note that columns exist for up to three detection methods.

Detection/Mitigation System: Name of the Detection/Mitigation system based on the selected SBS # (*automatically determined*).

Detection/Mitigation Elaboration: Short text that describes the detection and/or mitigation method. This is most important if there are no automatic detection/mitigation systems identified.

Rely on Inspections: a yes/no field about whether inspections are part of detecting the failure before it manifests the full stated consequence.

Residual Severity (S_R): Severity following detection/mitigation, chosen from pull-down menus which are taken from items in Table 2.1-2.

Residual Risk (R_R): Risk following detection is given by $S_R \cdot P_D$

Redundancy: Simple yes/no field if a redundant feature/component is present in the design. The redundant feature/component must have equivalent capability to the primary device, and should be invokable in less than 1 week.

Compensatory Action: Any short-term compensatory action to take in response to the failure having occurred. The net effect of invoking the compensatory action should be of modest impact, i.e. switching to an on-line redundant water pump is likely an acceptable compensatory action, while fabricating a new PF coil is not. In general, compensatory actions are actions to be taken in lieu of the explicit repair of the failed component, and the time to invoke the compensatory action should not exceed 1 week. The invocation of the compensatory action may be used in reducing the severity of a failure only if it is documented in this cell.[6]

[6] This restricted definition of compensatory action serves two functions:
- It clearly separates the invocation of programmatically impactful repairs (those with large probability and severity) from short-term work-arounds.

Reference: Any reference materials (memos, calculations, etc) used to substantiate the information on the failure mode.

4: Hazard Analysis Format

The hazard analysis will be included in the SAD. The specific format will be determined there.

5: Assumptions on Mitigation and Detection Systems

5.1 Unmitigated Safety Analysis

Following the scheme in Ref [1] and indicated in Section 2.2, the safety analysis should first be done assuming that hazards are not mitigated. Practically speaking, this implies that the safety analysis should start with the following assumptions:

- Active controls (e.g. access control systems) are not in place.
- Administrative controls for operations (e.g. search and secure procedures, hazardous inventory limit procedures, etc.) are not in place.
- Basic architectural features of the test cell are in place (walls, ceiling, permanent features of labyrinths), but mobile and non-permanent elements of the shielding are not under configuration control.

5.2 FMECA Assumptions on Detection/Mitigation Systems

This section elaborates on the guidance in Section 2.3 and Section 3. The initial analysis of the severity S and probability P are done assuming that detection/mitigation systems are not in place. The results of this analysis are then used to determine the required detection/mitigation systems. Examples of this include the following:

- The probability and severity of coil overheating events should be considered without the presence of the Digital Coil Protection System (DCPS).

- It prevents the impact of failures from being masked by the presence the on-line spares. This allows the criticality of the function to be assessed independent of any designed-in spares.

- The probability and severity of coil ground faults should be considered without the FCPC ground fault detectors present.

6: Calculations of Failure Rates and Failure Probabilities

As noted in Section 2, failure probabilities are provided with both quantitative and qualitative ranges. When possible, the quantitative ranges should be used. These may be determined from sources such as i) historical failure rates in NSTX service, ii) manufacturer's stated failure rates, or iii) databases of failure rates. Where this is not possible, engineering judgement and the qualitative ranges may be used.

Where calculations are made, the assumptions in Table 6-1 may be used:

***Table 6-1**: Assumptions supporting the quantitative evaluation of failure rates.*

Quantity	Units	Value
Run weeks per year[7]	wks/year	20
Operations days per run week	days/wk	5
Hours with FCPC and Coil Cooling water systems on during operations day	hrs/day	11
# of machine pulses per day[8]	pulses/day	22
# of neutral beam pulses per day[9]	pulses/day	216
Duration per pulse	sec/pulse	5
Weeks under Vacuum Each Year	wks/year	27
Weeks with NB Cryogenic Systems Operating	wks/year	30
Weeks with NB Systems In Operations	wks/year	22
# of bakeout periods per year	bakeouts/year	1
# of weeks per bakeout	wks/bakeout	3

In the absence of other information or calculations, it should be assumed that NSTX-U structural components that have been qualified using the NSTX-U Structural Design Criteria [9] against the shot spectrum in the General Requirements Document [10], and fabricated using the laboratory's quality assurance program, have a failure probability in the range titled "Extremely Unlikely Events".

[7] Time not spent during a run week may be considered dedicated to maintenance
[8] Based on Operations from 8:00 AM to 5:00 PM, with 2.5 minutes between pulses
[9] Based on Operations from 8:00 AM to 5:00 PM, with 2.5 minutes between pulses

7: Example Failure Modes

Tables of example failures modes can be found in various print and online references. These lists may be consulted in order to better understand failure modes of the system under consideration. The lists and tables below provide some example failure modes to consider.

Per Ref. [7], general classes of failure modes may include:

- Premature operations
- Failure to operate at a prescribed time
- Intermittent operation
- Failure to cease operation at a prescribed time
- Loss of output or failure during operation
- Degraded output of operational capability
- Improper alignment of valves or other control settings.
- Other unique failure conditions, as application, based upon system characteristics and operational requirements of constraints

Specific failures of a given part or system may include those in Tables 7-1 through 7-4. These lists are not all inclusive, but may be used in conjunction with a block diagram or other system description [5] to initiate the development of a FMECA.

***Table 7-1**: Failure modes for mechanical components*

1	Development of cracks/fractures
2	Parts that were intended to move becoming “stuck”
3	Parts becoming deformed under load
4	Parts that are otherwise fastened becoming loose
5	Parts that experience excessive wear or corrosion
6	Parts being exposed to excessive heat, or to excessive cooling

***Table 7-2**: Failure modes for thermal-hydraulic components*

1	*LOCA - Loss of coolant accident*
2	*ICE - Ingress of Coolant Event*
3	*LOFA - Loss of Flow Accident*
4	*LOVA - Loss of Vacuum Accident*

***Table 7-3**: Failure modes for electrical components*

1	Electrical components developing short circuits
2	Out of range (high or low) or null outputs
3	Failure of input stage electronics
4	Electrical connections or cabling failing

Note that potential electrical failure causes include insulation failure or contamination, overvoltage or overcurrent conditions, excessive temperature, radiation exposure, contact corrosion, and connector fatigue or mechanical damage.

***Table 7-4**: Failure modes for vacuum and pressure systems*

1	Leaks developing
2	Failure of valves to open, or to close; this can include partial closures
3	Operation of valves at inappropriate times
4	Failure or inaccurate output of sensors (pressure, flow, temperature, etc…)
5	Failure of pumps
6	Failure of windows and viewports

8: Standard Downtime Assumptions

While failure consequences are to be selected by the analyst from the menu items in Table 2.1-2, a number of project-wide assumptions should be respected by all analysts. These are provided in Table 8-1.

Table 8-1: Project-wide failure consequence assumption

Failure	Consequence
Any failure that requires manned vessel-entry to repair.	The minimum downtime impact is 3 months[10]. The time to enact the repair should be added to this baseline.
Any failure that vents the NSTX-U vacuum to air, but does not require manned vessel-entry.	The minimum downtime impact is 2 months[11]. The time to enact the repair should be added to this baseline.
Any failure that results in the extraction of the CS assembly from the machine to complete the repair.	The minimum downtime impact is 8 months.[12] The time to enact the repair, including any disassembly and reassembly of the CS assembly in the South High Bay, should be added to this baseline.
Any failure that results in the required replacement of a magnet, including a single TF outer leg.	The downtime should be listed as > 1 year.

[10] The 3 months = 12 weeks is derived from 3 weeks to enter the vessel, 1 week to close the vessel, 1 week to leak check, 4 weeks to conduct a bakeout and follow-on leak check, and 3 weeks to recover plasma operations.
[11] The 2 months ≈ 7 weeks is derived from 4 weeks to conduct a bakeout and follow-on leak check, and 3 weeks to recover plasma operations.
[12] The 8 months is derived from 1 month to prepare for the CS extraction, 1 month to reinstall umbrella components, 1 month to install TF flexible leads, 2 months to close the vessel and do leak checking, and 3 months to repeat the magnet ISTP and recover plasma operations.