PRINCETON PLASMA PHYSICS LABORATORY

ENG - MEMO

ON THE NEED FOR REDUNDANCY FOR THE SHORTED TURN PROTECTION SYSTEM

RCP_191119_SPG_1

Work Planning #:
Effective Date: **11/20/2019**
Prepared By: **Stefan Gerhardt**

Approved By	Stefan Gerhardt, Preparer	11/20/2019 10:36:00 AM

PRINCETON PLASMA PHYSICS LABORATORY
P.O. BOX 451 PRINCETON, N.J. 08543

National Spherical Torus eXperiment Upgrade

RCP-191119-SPG-01

TO: DISTRIBUTION
FROM: S. GERHARDT Stefan Gerhardt
Digitally signed by Stefan Gerhardt
DN: cn=Stefan Gerhardt, o=Physics, ou=PPPL, email=sgerhard@pppl.gov, c=US
Date: 2019.11.19 15:41:42 -05'00'
SUBJECT: ON THE NEED FOR REDUNDANCY FOR THE SHORTED TURN PROTECTION SYSTEM

NSTX-U Acceptable Risk

The NSTX-U FMECA plan defines acceptable risk for the project. In particular, the following table can be found.

***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

It can be seen that high severity events, defined as those which i) will incur more than a year of downtime, ii) cost >$5M to repair, or iii) may cause death, must be either “Extremely Unlikely” or “Incredible”.

The definitions of those probability phrases are provided here:

***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

Note that these probability thresholds are derived from an extensive study of DoE and DoE contractor documentation, and are consistent with long standing PPPL practice as described in the 1997 NSTX-U GRD and the NSTX-U Structural Design Criteria. See the FMECA plan for further elaboration.

Probabilities of Events Based on NSTX(-U) Experience

The shorted turn protection system is designed to isolate electrical faults of coils. There have been four such events of this type in the history of NSTX(-U), as shown in Table 1.

***Table 1**: Coil electrical failures in the history of NSTX-U*

Event	Year	STP could have mitigated damage
TF Failure	2002	potentially, arc was in exposed bus work
TF Failure	2011	No; internal failure[1]
OH Braid	2015	Yes, arc was on exposed water feeds
PF-1aU Failure	2016	No; internal failure

[1] Internal failures of a coil may be detected in advance of melting large quantities of Cu, but there is typically no remedial action that can be taken to eliminate the issue and return the coil to operations. Configurations that result in arcs on bus work and water feeds, however, can be corrected if detected before there is large-scale damage.

In that period, NSTX-U took >10000 magnet pulses. It can be grossly inferred that the rate per pulse of these failures where Shorted Turn Protection system (STP) can rationally be expected to help the machine is 2/10000 = 0.0002.

DCPS was only in operation for only the 2016 run campaign. During that time, there were many (>10) DCPS trips, including some days where multiple shots in a row experienced trips. Note that in 2016, the machine ran to only 1 MA of plasma current, whereas the ultimate goal is to run to 2 MA (2-4x higher forces in the future, i.e. routine operations much closer to the margins of the device). For this reason, the probability per pulse of excessive loads in the unmitigated case can be taken to 10%-100%. The 10% value will be taken below, with the understanding that it may not be conservative.

The reason for this disparity in frequency can be understood as follows. The coils are designed for the full output voltage of the rectifiers. This includes assessments of (theoretical) insulation safety factors (which are very high), and conservative assessments of creep distances in coil lead areas. Hence, arcs of the types designed to be detected by STP are rare failures.

On the other hand, the DCPS was built because excessive forces on coils and their supports would be normal events in the absence of protection (normal in the sense that excessive forces would occur many times per campaign). The coils and supports are designed for a specific set of plasma equilibrium conditions, with some control headroom applied to the PF coil currents (see the Design Point Spreadsheet). Both equilibria outside that design-basis set, and large transients to the design basis set, may create excessive forces on the coils. Equilibria outside the design basis set are fully expected (for instance, the design basis is all reasonably high elongation H-modes), and tokamak plasma are notorious for large control transients. Note that the project GRD explicitly acknowledges this condition.

Furthermore, the power supplies themselves, if not constrained to current combinations which support a plasma equilibrium, may create dramatically larger loads than the design basis. This could happen in the case of errant programming by an operator during test shots, or any number of control failures in the realtime system or the protection systems. These control failures cannot, however, exceed the design-basis power supply voltages.

Risk Analysis

An example risk analysis for excessive loads and for electrical arcs is shown below. It is assumed that each failure causes levels of damage in the “high severity” category, such that the protection system must reduce the probability to “extremely unlikely”.

The rows are as follows:

Row 1: The target probability for these catastrophic events
Row 2: The probability of these events, in the absence of a protection system.
Row 3: The postulated probability that the first realtime computer itself will fail dangerous. A fail-safe design philosophy is assumed, i.e. the unsafe state is the energized state.
Row 4: The postulated probability that the assumed WDT on the first WDT monitor fails in its function (detect the heartbeat, generate a fault if heartbeat is not present)
Rows 5 & 6: Same for the 2nd protection system. The unity values for the 2nd STP system imply that it was not deployed, i.e. guaranteed to not work.
Rows 7 & 8: The shots per day, and days per campaign, as taken from the FMECA plan.
Row 9: The probability of the unmitigated event, defined simply as the product of the numbers above.

Note that any one instance of the STP and DCPS are assumed to have the same failure probability.

Table 2: *Model risk analysis for STP and DCPS*

1	Target probability for catastrophic damage to device (1/yr)	1.00E-04	
		DCPS	STP
2	Unmitigated probability per shot of event (excessive loads for DCPS, and some coil arc for STP)	0.1	0.0002
3	Probably per shot that protection system #1 computer fails dangerous	0.01	0.01
4	Probably per shot that protection system #1 WDT fails dangerous	0.01	0.01
5	Probably per shot that protection system #2 computer fails dangerous	0.01	1
6	Probably per shot that protection system #2 WDT fails dangerous	0.01	1
7	Shots per day	22	22
8	Run days per campaign	100	100
9	Probability of unmitigated event	2.20E-06	4.40E-05

Note that “fail dangerous” with regard to STP should be understood as a failure of the technical infrastructure of the system, e.g. software lockup, cable failure, power loss, data stream failure, etc. There are inherent limitations on the STP system based on using FCPC rectifiers as test voltage sources. High impedance faults, or faults between individual turns of coils, are not expected to be detectable with a method such as this. These failures, based upon the technical limitation of the method, are addressed in this table or memo.

On this basis of Table 2, a few observations can be made:

- The DCPS-mitigate events are “normal” in the context of the FMECA classifications, while the STP-mitigated events are “anticipated”.
- For the hypothesized (and very high) failure rates (1% per shot), both the DCPS and the STP meet the project risk requirements, albeit with two layers for DCPS.
- In the absence of the 2nd layer, the DCPS would not meet the risk threshold (would be $2x10^{-2}$/yr)
- There are some components of the STP system that are not assessed by the watchdog timer, for instance physical connections at the interface to the HUI. These components must have a fail-dangerous rate <~10^{-4} /pulse.
- For the postulated rate of arcs and electrical failures, the project risk threshold would be met if the STP failure rates in rows 3 and 4 were increased to 1.5 failures per 100 pulses. It is expected at these rates of dangerous failures can be readily avoided.

Note that DCPS has its own set of formal reliability requirements (link), and the statements above regarding DCPS are made only for comparison.

Conclusion

The target risk level for failures mitigated by the shorted turn protection system can be achieved with only a single instance of the STP.

Distribution
G. Tchilinguirian
R. Ellis
M. Boyer
F. Hoffmann
J. Landi
T. Stevenson
T. Jernigan