National Spherical Torus Experiment-Upgrade

NSTX-U

REQUIREMENTS DOCUMENT

Real Time Control And Protection - Shorted Turn Protection

NSTXU_1-7-3-6-9_RD-100

Revision 0

November 19th, 2019

Frank Hoffmann
Digitally signed by Frank Hoffmann
Date: 2019.11.19 16:11:30 -05'00'

Prepared by: Frank Hoffmann, Real-time Protection and Control RE

PAUL SICHTA
Digitally signed by PAUL SICHTA
Date: 2019.11.20 09:05:30 -05'00'

Reviewed by: Paul Sichta, Control and Data Technical Authority

Dan Boyer
Digitally signed by Dan Boyer
Date: 2019.11.20 10:06:08 -05'00'

Reviewed by: Dan Boyer, Physics

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 16:07:23 -05'00'

Reviewed by: Stefan Gerhardt

Yuhu Zhai
Digitally signed by Yuhu Zhai
Date: 2019.11.20 10:13:23 -05'00'

Approved by: Yuhu Zhai, NSTX-U Project Engineer

Change Record

Revision	Date	Description of Change
0	11/19/2019	Initial Release*

*Some draft versions posted for PDR.

Table of Contents

1 References

[1] NSTX-U-RQMT-GRD-001, *NSTX-U General Requirements Document*
[2] NSTX-U-RQMT-SRD-008, Realtime Control & Protection SRD
[3] ENG-010 "*Control of Drawings*"
[4] ENG-023 "*Electrical Equipment Approval* "
[5] ANSI/VITA 17-1998 "*American National Standard for Front Panel Data Port Specifications*"
[6] QA-028 "*Software Quality Assurance*"
[7] RCP-191119-SPG-01 "*On the need for redundancy for the Shorted Turn Protection System*"

2 Scope

This document defines the requirements for the Shorted-Turn-Protection System (STP).

The STP is part of the NSTX-U machine protection scheme. It monitors coil voltages and currents and evaluates those with the goal to detect shorted turns inside the coils, as well as arcing at the coil terminals for each of the coils.

The format of this document, including interface specifications, is provided in the General Requirements Document [1].

3 Functions

The functions of the STP are:

a. The Shorted Turn Protection system shall track the NSTX-U timing events and the reception of these in the correct sequence. The timing events are:
   i. SoP: Start of Pulse
   ii. EoP: End of Pulse
   iii. T-60: 60 seconds before SoP
   iv. T-30: 30 seconds before SoP
   v. T-n: n seconds before SoP (n is configured for NSTX-U as part of the timing systems)
   vi. Abort: Event generated if COE aborts a shot

b. While the system is activated and a shot is active (i.e. between detection of the SoP and EoP events):
   i. continuously monitor NSTX-U coil voltages and coil currents.
   ii. continuously model the expected electrical behaviour of the coil systems, including effects from coupled inductances with other coils, the vessel components, and plasma current to a sufficient granularity.
   iii. compare the measured coil voltages and currents with the respective values expected from the model.
   iv. issue a STP Level-1 fault if there is a discrepancy larger than a predetermined and configurable threshold between any of the measured coil voltages and currents and the respective modeled coil voltages and currents.
   v. issue a STP Level-1 fault if the EoP timing event is not detected within a configurable time period (tracked with an internal timer) after detection of the SoP event

c. Continuously provide a fail-safe status signal that indicates a fault in case the STP system stops operating unexpectedly.

4 Materials and Design Requirements

a. The System shall be designed to conform to electrical isolation requirements as defined in the GRD [1] Section 4.2.3 parts b and c.

b. Where practical, equipment, communication protocols, and software will be utilized that is commercially available and supported by vendors or open source software communities.

c. When equipment must be designed in-house for a specific purpose, it shall conform to industry and PPPL engineering procedures defined for electronics (ENG-023 [3]) .

d. The use of material in the construction of this system shall conform to industry standards wherever practical following Reduction of Hazardous Substances (RoHS) directive.

e. The computing hardware platform for executing the STP algorithms shall use an operating system (OS) that supports deterministic real-time execution of the algorithm.

f. The computing hardware platform for executing the STP algorithm shall include redundancy for critical components, in particular a) power supplies and b) data storage.

g. The software code shall be developed and maintained following the Software Quality Assurance Procedure [6].

h. The software code shall only use library functions that are considered real-time safe.

i. Changes to the Shorted Turn Protection software shall only be carried out by I&C group personnel in collaboration with the main stakeholders from NSTX-U operations and Physics operations.

5 Configuration Requirements and Essential Features

5.1 Mechanical Requirements

a. The computing hardware platform for executing the STP algorithm shall be suitable to be mounted in standard computing racks.

b. Associated realtime computing platforms shall be installed in an area with restricted access such as the FCC or caged area in the Junction Area.

c. Where possible, existing data acquisition equipment shall be used (for example FPDP hardware modules or analog input devices). Newly developed data acquisition equipment shall conform to the mechanical and electrical requirements of existing equipment as much as possible.

5.2 Input Data

a. The system shall have as input data redundant measurements of the following:
    a. TF coil current and voltage
    b. OH coil current and voltage
    c. Currents and voltages of all PF coils
    d. Plasma current data, from the plasma current Rogowski coils after compensation for vessel and linked-coil pick-up

b. Positions of ground switches and line switches for all PF, TF, and OH coils shall be measured

c. The system shall sample all inputs using the system-wide FPDP clock.

d. The system shall evaluate the voltage measurement by ensuring the matching measurements for a coil voltage are identical to within a configurable measurement difference. Measurements that are dissimilar by more than the specified difference shall result in triggering a STP Level-1 fault.

e. The system shall evaluate the current measurement by ensuring the matching measurements for all coil currents are identical to within a configurable measurement difference. Measurements that are dissimilar by more than the specified difference shall result in triggering a STP Level-1 fault.

f. The system shall convert the input data stream to the physics and engineering representation required by the algorithms.

g. The system shall adjust the input data measurements for sensor specific compensation, for characteristics such as DC offsets and integrator drift.

h. The sensor specific compensations shall be determined for each shot during the shot cycle at a configurable time before the shot

5.3 Configuration & Operation

a. The system shall be operated only by trained personnel as departmental training matrices.

b. Logging into the associated realtime computing platform and software execution on the computing platform shall be restricted to a group of trained and qualified I&C engineers.

c. Only a maximum of one instance of the system shall be active on a Shorted Turn Protection computing platform at any time.

d. Each STP system shall provide a user interface (UI) on a computer screen / terminal in the PPPL control room.

e. The system shall be started by executing a command line command.

f. The UI shall at a minimum provide functionality to:
   i. Configure the system to adapt its functionality for the setup of the NSTX-U machine.
   ii. Load and save configurations from/to a dedicated and secure data archiving system such as an MDS+[1] tree.
   iii. Change the operating state the system is in.
   iv. Provide status of all important status items, including Shorted Turn Level-1 fault status.
   v. Provide operating state, and status of key operating parameters.
   vi. Provide a summary view of the operation during the last shot.
   vii. Clear a detected STP Level-1 fault

[1] MDS+ = Modular Data System Plus. MDS+ is used to archive nearly all NSTX-U shot data, as well as many operations parameters and metadata.

g. Configuration and/or selection of operating modes shall be done by accessing suitable parameters from a dedicated and secure NSTX-U MDS+ tree.

h. The system shall be designed to accommodate changes in position of the SDS cabinet bus links

5.4 Status Indication

a. For the operator, status indication and events during operation shall be done using the provided UI.

b. A detected harmful condition shall be indicated by raising a STP Level-1 fault through a dedicated signal sent to the Hardware User Interface in the Junction Area.

c. A dedicated signal changing its state at a suitable frequency shall be emitted. The signal shall be monitored and passed on to the Hardware User Interface in the Junction Area to indicate the continuous operation of the system. Non-reception of this signal by the Hardware User Interface shall trigger a STP Level-1 fault.

6 Baseline Performance and Operational Requirements

6.1 Operating States

a. The Shorted Turn Protection algorithm shall be executed as part of a deterministic finite state machine (FSM).

b. The FSM shall track NSTX-U timing events (T-30, T-n, SoP, EoP, Abort) to:
   i. Determine the protection phase (from SoP to EoP) in which the protection algorithm is active
   ii. Issue an STP Level-1 fault if any of the tracked timing events are received out of sequence

c. The FSM shall have dedicated states to distinguish between operation phases to prevent parameter changes during the protection phase in the following manner:
   i. A setup phase in which the operator is allowed to change system parameters. During this phase UI activity is allowed.
   ii. A ready phase in which the system is waiting for the timing event indicating that the next shot is imminent (T-60). In this phase the only allowed operator activity is to change the system phase back to the setup phase. During this phase UI activity is allowed.
   iii. A parameter access and calibration phase (between T-60 and SoP) in which modified parameters are stored, required parameters system parameters are read, and measurements to account for sensor specific calibrations. During this phase UI activity is NOT allowed.

iv. An active protection phase (between SoP and EoP) in which the STP algorithm is being executed. During this phase UI activity is NOT allowed.
v. A data storage phase (after EoP) in which all logged pulse data is being stored. During this phase UI activity is NOT allowed.

d. The FSM shall have dedicated states for all failure states. Leaving any of the failure states, shall
   i. be triggered by operator UI interaction, and
   ii. shall only be possible after all available data has been written to MDS+ data storage.

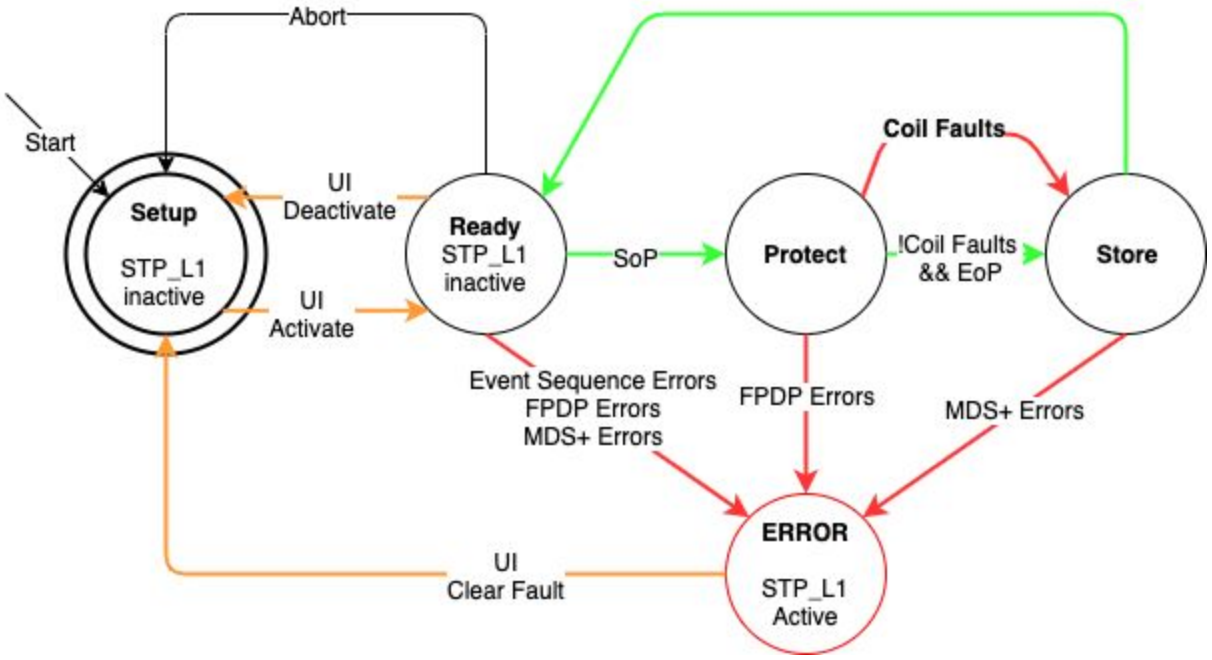

Fig. 1: State Machine Diagram (The states shown may include sub-states.)

6.2 Timing Requirements

a. The system shall operate with a cycle time of 200us, based on the 5kHz data sampling frequency for the control and protection systems.

b. The system shall receive and process a new set of measured data every 200us.

c. The system shall update the STP Level-1 fault output signal once every 200us.

d. The execution of the algorithm shall be no more than 1000us.

e. If the algorithm execution time is longer than 200us, the algorithm shall be structured in a way ensuring that no input data sample is lost.

f. After detecting an error condition the Shorted

g. The system shall toggle the output signal to indicate that the system is alive once every 200us, generating an active pulse of 25% - 50% duty cycle.

6.3 Input Data Requirements

a. The system shall receive its input data as an FPDP data stream in the same format used for the other control and protection systems.

b. The system shall verify the timely reception of FPDP data packets.

c. The system shall verify the integrity of the received FPDP data packets, checking the order of the received data words and - if available - using other in-stream data integrity features like CRC-32.

d. The system shall verify the consistency of pairs of data values expected to be identical within FPDP data packets.

e. The system shall verify and maintain read access to the MDS+ system for reading parameters.

6.4 Algorithm Requirements

a. The STP shall accommodate stepping a replaceable, modular short detection algorithm that is active between the start of the pulse (SoP) to the end of the pulse (EoP).

b. Commonly used languages and coding methods for real-time system development, e.g., C/C++ code generated from a Simulink model shall be accommodated.

c. The detection algorithm shall use an approximate model of the NSTX-U conducting structures, measured voltages applied to coils, and estimates of the interaction of the conductors with the measured plasma current to predict the conductor currents at each step.

d. The algorithm shall compare the predictions to measured currents and compare the errors to predefined thresholds.

e. The algorithm shall declare a fault for a coil if the error threshold for that coil is exceeded. A fault on any coil shall cause a latching STP Level 1 fault to be declared.

f. Algorithm parameters (e.g., thresholds, model parameters, and parameters needed for the calculation of estimation uncertainty) shall be configuration controlled and the parameters used shall be archived with each shot.

g. Measurements, as well as calculated currents, uncertainties, and faults for each coil shall be archived to enable post-shot analysis.

6.5 Output Data Requirements

a. The system shall verify and maintain write access to the MDS+ system for writing system results and state changes in a suitable format.

b. The system shall store all relevant output data in memory during the active operation period and write the output data to the MDS+ system after the end-of-pulse event.

c. The system shall log (and later commit to the MDS+ system) all relevant events detected by and occurred in the system, including suitable event details and time stamp.
   Relevant events shall include:
   i. detected faults,
   ii. detected loss of input data stream,
   iii. changes of the internal system state.

d. If logged data cannot be committed to the MDS+ system for storage, the system shall remain in the current state that is attempting to write the data. Abandoning the data storage process shall require operator action using the UI.

6.6 Output Fault Signal Requirements

a. The signal to indicate that the system is alive shall be fail-safe: a broken signal path must be detected as a system no longer in operation.

b. The STP Level-1 fault signal shall be fail-safe: a broken signal path must be detected as a STP Level-1 fault.

c. The emitted STP Level-1 fault signal shall be implemented so that it can be combined with other existing faults signals inside the Hardware User Interface.

6.7 Testing Requirements

a. The system shall have the ability to test in the final configuration, either in concert or individually, the following aspects:
   i. Input interconnections (e.g. currents, voltages, timing signals, etc.)
   ii. Software, including both IO, framework, and algorithms
   iii. Output interconnections (e.g. to DCPS HUI and the HCS)

(Note: voltage and current transducers themselves may be tested as separate coordinated test)

6.8 Reliability

a. The components of the shorted-turn protection system which are not monitored by the WDT shall have a fail dangerous[2] rate of $<10^{-4}$ /pulse [7].

b. The software components of the Shorted Turn Protection system, which are monitored by the WDT, shall be designed to have a fail-dangerous rate of less than 0.5% per pulse[3] [7].

c. The WDT circuitry which monitors the operating state of the STP shall have a fail-dangerous rate of <0.5% per pulse [7].

d. The voltage and current sensors shall have less than 2 critical failures per 10,000 pulse or 0.0002/pulse.

7 Upgrade Performance and Operational Requirements

a. The input data for the Shorted Turn Protection Systems may be augmented to include other measurements, such as :
    i. Feedback of the voltage commands as executed by the FCPC rectifiers

8 Interfaces

Interfaces are defined in the associated SRD [2] and ICDs.

[2] In this context, fail dangerous refers to any configuration of the system where the pulse is allowed to proceed without the protection afforded by the system or sub-system.
[3] Ref. [7] postulates a 1% fail-dangerous rate per pulse; this requirement is ½ that for additional conservatism.