National Spherical Torus eXperiment Upgrade

NSTX-U Centralized Control System Requirements

NSTX-U-RQMT-RD-025-01

November 25, 2019

Ben Smith
Digitally signed by Ben Smith
Date: 2019.11.26 08:11:24 -05'00'

Prepared by: Ben Smith, Central I&C Engineer

Peter Dugan
Digitally signed by Peter Dugan
Date: 2019.11.26 08:24:51 -05'00'

Reviewed by: Peter Dugan, Systems Engineering and Integration

Joseph R_ Petrella Jr_
Digitally signed by Joseph R_ Petrella Jr_
DN: C=US, O=PPPL, CN=Joseph R_ Petrella Jr_, E=jpetrell@pppl.gov
Reason: I have reviewed this document
Location:
Date: 2019-11-26 10:24:00

Reviewed By: Joe Petrella, Project Cognizant Engineer

John Dellas
Digitally signed by John Dellas
DN: cn=John Dellas, o=Princeton Plasma Physics Laboratory, ou=NSTX-U Recovery Project - Power Systems, email=jdellas@pppl.gov, c=US
Date: 2019.11.26 12:34:29 -05'00'

Reviewed By: John Dellas, Power Systems RE

Timothy N. Stevenson
Digitally signed by Timothy N. Stevenson
Date: 2019.11.26 14:17:14 -05'00'

Reviewed By: Tim Stevenson, Operations and Safety Systems RE, Heating Systems RE

PAUL SICHTA
Digitally signed by PAUL SICHTA
Date: 2019.11.27 12:56:21 -05'00'

Reviewed by: Paul Sichta, Control and Data TA

Yuhu Zhai
Digitally signed by Yuhu Zhai
Date: 2019.11.27 13:44:43 -05'00'

Approved By: Y. Zhai, NSTX-U Project Engineer

Record of Revisions

Date	Version	Brief Description of Changes
10/11/19	Rev 0	Initial Release
11/25/19	Rev 1	Make consistent with SRD-12 and RD-24, correct per PDR chits

References

[1] NSTX-U-RQMT-GRD-001, NSTX-U General Requirements Document
[2] NSTX-U-RQMT-SRD-012, NSTX-U SRD – Operations & Safety Systems
[3] NSTX-U-RQMT-RD-026, NSTX-U Trapped Key System Requirements
[4] NSTX-U-RQMT-RD-024, NSTX-U Personnel Safety System - Safety Instrumented Systems Requirements

1: Scope

a. This document provides implementation requirements for the NSTX-U Centralized Control System (CCS). The CCS directly receives status information from the Personnel Safety System - Safety Instrumented System (PSS-SIS) and Trapped Key System (TKS). The CSS interacts with the individual Basic Control Systems (BCSs[1]). This is accomplished by providing permissives for execution on the basic control systems. The logical configuration of the system shall be detailed in a system software specification.

b. General requirements for the system are provided in the NSTX-U General Requirements Document [1].

c. System requirements are provided in Operations and Safety Systems System Requirements Document [2]. This document flows the system requirements in that SRD down to specific implementation requirements.

2: Definitions

The definitions are included in Ref [2].

3: Design Requirements

3.1: Personnel Safety System Safety Instrumented System Interaction

a. The CCS shall be capable of receiving inputs from the PSS-SIS for all communicated signals.
b. The CCS shall have the ability to receive “safe to enable FCPC” and “safe to enable NB” signals from the PSS-SIS.
c. The CCS shall have the ability to receive “FCPC configured for dummy load” and “NB configured for dummy load” from the PSS-SIS.
d. The CCS shall be capable of receiving NSTX-U Emergency Stop status from the PSS-SIS.
e. The CCS shall have the ability to receive the following area status information for the NSTX-U Test Cell and MER Mezzanine areas from the PSS-SIS:
    i. ACCESS
    ii. Search & Secure (S&S) in progress
    iii. NO ACCESS
    iv. LOCKDOWN

[1] A “ BCS” is the subsystem(s) (FCPC, NB, HHFW) primary control system.

f. The CCS shall have the ability to receive the following area status information for the Test Cell Basement Cage Area and the Cable Spread Room from the PSS-SIS:
    i. ACCESS
    ii. NO ACCESS
    iii. LOCKDOWN
g. The CCS interface to the PSS-SIS shall not degrade the safety capability of the PSS-SIS.
h. Communication between the PSS-SIS and the CCS shall be electrically isolated for control signal levels.
i. The CCS shall be capable of receiving SIS-alarm signals from the PSS-SIS.

3.2: Trapped Key System Interaction

a. The CCS shall receive the status of select trapped key blocks including, but not exclusive to the following:
    i. NB Ready to Enable Key
    ii. FCPC SLD Ready to Enable Key
    iii. HHFW Ready to Enable Key
b. The CSS shall allow enable and arm permissives when monitored trapped key blocks are properly configured.
c. The CCS shall utilize one key to control the operationally sequenced subsystems, described in section 3.3.

3.3: Operationally Sequenced Systems

3.3.1: General Considerations for Operationally Sequenced Systems

a. The arming permissive shall not be asserted when the enabling permissive is not asserted or when the PSS-SIS is asserting an NSTX-U Emergency Stop.
b. Provision shall be made for the addition of new equipment as the system evolves.
c. Electrical isolation shall be provided between the CCS and the systems to which it provides permissives.
d. The CCS shall be able to initiate a disable and/or disarm of subsystems from the Chief Operating Engineer (COE) stations, for individual systems or en mass.
e. All signals originating from the CCS shall be latched outputs unless otherwise specified as momentary.

3.3.2: Enable/Arm Permissives

a. The CCS shall provide enable/arm permissive capability for the equipment as identified in Table 3.3.2-1. This table provides the list of operationally sequenced systems.
b. The CCS enable and arm permissives shall permit the subsystems to operate.

c. The CCS shall provide a hardwired master disable button that will immediately disable and disarm all subsystems.
d. The CCS shall provide a hardwired master disarm button that will immediately disarm all subsystems.
e. The CCS enable and arm permissives shall not directly operate subsystems under independent BCS control.

Table 3.3.2-1*: Systems for which the CCS provides a complete set of enable/arm permissives*

1	Neutral Beams - High Voltage
2	FCPC Power Supplies
3	HHFW
4	ECH-PI

3.3.3 Neutral Beams

a. The neutral beam system shall be divided into two subsystems (NB #1 and #2, powered by TFTR era NB lineup #5 and #4). From the CCS perspective each beamline will be treated independently.
b. The CCS shall send the following signals to the Neutral Beams BCS
    i. Enable permissive
    ii. Arm permissive
c. The CCS shall only issue enable/arm permissives to the Neutral Beams when the following conditions exist:
    i. The “safe to enable NB” input signal from PSS-SIS is high
    ii. The “No NSTX-U E-Stop” input signal from PSS-SIS is high
d. The CCS shall support HV Conditioning, HV Operations, and Dummy Load Testing modes.
e. The CCS shall receive the following control status signals from the Neutral Beams BCS:
    i. Enabled
    ii. Disabled
    iii. Disarmed
    iv. Armed
f. Both enable and arm permissives shall be able to be revoked by the COE.
g. The CCS Neutral Beamlines 1 & 2 interface shall provide a unique key switch to permit enabling.
h. The CCS Neutral Beamlines 1 & 2 interface shall provide a unique key switch to permit arming.
i. The CCS Neutral Beamlines 1 & 2 interface shall provide a unique hardwired pushbutton to disable each subsystem.
j. The CCS Neutral Beamlines 1 & 2 interface shall provide a unique hardwired pushbutton to disarm each subsystem.

3.3.4 FCPC Rectifiers[2]

a. The CCS shall send the following signals to the FCPC BCS:
    i. Enable permissive

[2] Inclusive of SPAs

ii. Arm permissive
iii. Configure (labeled “switch permit” on legacy HIS documents)
iv. Fault reset (shall be a momentary signal)

b. The CCS shall only issue enable/arm permissives to the FCPC subsystem when the following conditions exist:
   i. The “safe to enable FCPC” input from PSS-SIS is high
   ii. The “No NSTX-U E-Stop” input signal from PSS-SIS is high
c. The CCS shall support FCPC Dummy Load and Open Circuit Testing Mode.
d. The CCS shall receive the following control status signals from the FCPC BCS:
   i. Disable Complete
   ii. Disarm Complete
   iii. Level 1 Fault
   iv. Level 3 Fault
   v. Level 4 Fault
   vi. Coils in Configure
e. Both enable and arm permissives shall be able to be revoked by the COE.
f. The CCS shall only permit switching to the configure mode[3] when the FCPC rectifiers are enabled.
g. The CCS FCPC interface shall provide a unique key switch to permit enabling of the rectifiers.
h. The CCS FCPC interface shall provide a hardwired three-way switch with the positions arm, disarm, and configure. The switch shall be configured with disarm in the middle position.
i. The CCS FCPC interface shall provide a unique hardwired pushbutton to disable the subsystem.
j. The CCS FCPC interface shall provide a unique hardwired pushbutton to disarm the subsystem.
k. The Level 1, 3, and 4 rectifier fault reset signal shall be able to be sent by the CCS to the FCPC BCS through the CCS CHMI.

3.3.5 Safety Lockout Device (SLD)

a. The CCS shall provide two permissives to the Safety Lockout Device that will allow a change of mode. Both signals shall be hardwired momentary signals.
   i. Permit Restoration of Air
   ii. Permit Removal of Air
b. The CCS shall only issue the permit removal of air signal when the:
   i. FCPC is safe as indicated by its shutdown or disabled signals
c. The CCS shall only issue a permit restoration of air signal when:
   i. “Safe to enable FCPC” signal is high
   ii. “No NSTX-U Estop” signal is high
d. The CCS shall receive the following status signals from the SLD:
   i. Air Restored to Control Room
   ii. Lockout Complete (Safe) to Control Room
e. The FCPC shall provide a unique hardwired three-way switch with the positions permit to restore air, neutral, and permit to remove air. The switch shall be configured with the neutral position in the middle.

[3] Configure Mode is a condition in which FCPC can open/close line switches and ground switches without sending power to coils in the NTC.

3.3.6 RF Systems

a. The CCS shall provide one permit to enable signal to both RF systems, HHFW and ECH-PI.
b. The CCS shall only issue the enable permissive to the RF subsystems when the following conditions exist
    i. The “No NSTX-U E-Stop” input signal from PSS-SIS is high
    ii. The “NO ACCESS” input signal from PSS-SIS is high for the NTC area
c. The permit to enable signal shall be able to be revoked by the COE.
d. The RF interface shall provide a unique key switch to permit enabling.
e. The RF interface shall provide a unique hardwired pushbutton to disable the subsystems.

3.3.6.1 HHFW System

a. From the CCS perspective, all six HHFW transmitters shall be treated as one system.
b. The CCS shall send the following commands to the HHFW BCS:
    i. Enable permissive (RF permit to enable)
    ii. Arm permissive
c. The CCS shall only issue the arm permissive to the HHFW subsystem when the following conditions exist
    i. The “No NSTX-U E-Stop” input signal from PSS-SIS is high
    ii. The “NO ACCESS” input signal from PSS-SIS is high for the NTC area
d. The CCS shall receive the following control status signals from the HHFW BCS:
    i. Enabled
    ii. Disabled
    iii. Disarmed
    iv. Shutdown
e. The permit to arm signal shall be able to be revoked by the COE.
f. The HHFW shall provide a unique key switch to permit arming.
g. The HHFW shall provide a unique hardwired pushbutton to disarm the subsystem.

3.3.6.2 ECH-PI System

a. The CCS shall send the following commands to the ECH-PI BCS:
    i. Enable permissive (RF permit to enable)
    ii. Arm permissive
b. The CCS shall only issue the arm permissive to the ECH-PI subsystem when the following conditions exist
    i. The “No NSTX-U E-Stop” input signal from PSS-SIS is high
    ii. The “NO ACCESS” input signal from PSS-SIS is high for the NTC area
c. The CCS shall receive the following control status signals from the ECH-PI BCS:
    i. Enabled
    ii. Disabled
    iii. Disarmed
    iv. Shutdown

d. The permit to arm signal shall be able to be revoked by the COE.
e. The ECH-PI shall provide a unique key switch to permit arming.
f. The ECH-PI shall provide a unique hardwired pushbutton to disarm the subsystem.

3.4: Systems Requiring "No NSTX-U E-Stop" Signal Only

a. The CCS shall provide a fail-safe "No NSTX-U E-Stop" signal for the equipment as identified in Table 3.3.2-1 and Table 3.4-1
b. "No NSTX-U E-Stop" signal shall go low upon an NSTX-U Emergency Stop being declared.
c. The CSS shall allow the "No NSTX-U E-Stop" signal to be energized when the PSS-SIS is in an ACCESS state, under administrative control.

***Table 3.4-1**: Systems for which the CCS provides the "No NSTX-U E-Stop" signal*

1	Bakeout Helium
2	Bakeout DC Heating System
3	Bakeout MTWS
4	Glow Discharge Cleaning/Boronization
5	Emissive Filament Bias Supplies
6	MPTS Laser
7	High Pressure Pump
8	MSE-LIF
10	Mass Gas Injection
11	OH Water Heater

d. The CCS shall provide a fail-safe "Loop Set" signal for the equipment identified in Table 3.4-2.
e. The "Loop Set" signal shall go low upon the NSTX-U test cell entering the ACCESS or LOCKDOWN states.
f. The "Loop Set" signal shall only be high when the NSTX-U test cell is in the NO ACCESS state.

***Table 3.4-2**: Systems for which the CCS provides the "Loop Set" signal*

1	Glow Discharge Cleaning/Boronization
2	Emissive Filament Bias Supplies
3	Mass Gas Injection
4	MPTS Laser
5	High Pressure Pump
6	OH Water Heater

3.4.1 Bakeout Helium, Bakeout DC Current Supply, and Bakeout MTWS

a. No Additional requirement

3.4.2 GDC and Boronization System

a. No additional requirement

3.4.3 Emissive Filament Bias Supply

a. No additional requirements

3.4.4 MPTS Laser

Note: The MPTS laser is interlocked to the CCS through the MPTS Laser Interlock Box. This box has historically accepted "No ESTOP" and "Loop Set" signals from the HIS. It combined those signals with other MPTS related interlocks to generate a local Laser Permissive and a local permissive to open the laser guillotine.

a. The CCS shall provide signals to the MPTS Laser Interlock Box that provide functional equivalents to the legacy "No ESTOP" and "Loop Set" signals.

3.4.5 High Pressure Pump

a. No additional requirements

3.4.6 MSE-LIF

a. No additional requirements

3.4.7 Mass Gas Injection (MGI)

a. The CCS shall provide signals to the MGI system that provide functional equivalents to the legacy "No ESTOP" and "Loop Set" signals.

3.4.8 OH Water Heater

b. The CCS shall provide signals to the OH Water Heater system that provide functional equivalents to the legacy "No ESTOP" and "Loop Set" signals.

3.5 Administrative Test Cell Access Control

A. The CCS shall provide signals to revoke the ACAMS access to the following man doors:
    a. NTC North door
    b. NTC South door

3.6 Human Machine Interface

a. The CCS HMI (CHMI) shall have a master overview display page indicating a summation of the condition of the facility.
b. The CHMI may have menu-driven sub pages that displays detailed information.
c. The CHMI shall have the means for displaying status and providing control capability for the COE from the NSTX-U control room.
d. The CHMI shall provide means for the operator to authenticate using a password.
e. The CHMI shall appear different from the PSS-HMI so that operators and users do not confuse the two systems.
f. The CHMI shall have the ability to display any or all status and control information it receives from the PSS-SIS.
g. The CHMI shall provide only one operations-relevant operator role; for the NSTX-U Chief Operating Engineer (COE).
h. The layout of indications and inputs (buttons, switches) on the CHMI shall be determined in consultation with the NSTX-U COE(s).
i. The CHMI will provide the following indications for each sub-system within the capabilities of the interface to include but not limited to:
    i. subsystem disabled
    ii. subsystem enabled
    iii. subsystem disarmed
    iv. subsystem armed
    v. subsystem permissive(s) granted
j. The CHMI shall have a push button (or equivalent) to return an individual operationally sequenced subsystem to the disabled condition.
k. The CHMI shall allow the operator to individually disarm operationally sequenced subsystem
l. The CHMI shall indicate the status of the Safety Lockout Device.
m. The CHMI shall have indication that the SLD may be operated to its unsafe position to restore the air to the Safety Disconnect and Grounding Switches.
n. The CHMI shall indicate the summation of the FCPC Safety Disconnect and Ground Switch Positions Loop "Lockout Complete (Safe) to Control Room".
o. The CHMI shall indicate when the FCPC subsystem is in configure mode.
p. The CHMI shall provide an indication of when each sub-system may be advanced from the disabled mode to the enabled mode.

q. The CHMI shall provide an indication when all operationally sequenced subsystems are enabled.
r. The CHMI shall be expandable to include additional equipment.
s. The CHMI shall provide a PSS-SIS state indicator status (ACCESS, NO ACCESS, LOCKDOWN).
t. The CHMI shall provide alarms to alert the COE, at a minimum, of the following abnormal situations:
    i. CCS PLC Errors & Failures
    ii. PSS-SIS input signal mis-match
    iii. PSS-SIS NSTX-U E-Stop
u. The CHMI shall allow the COE to acknowledge or clear an alarm.

3.7 Archive Historian

a. The CCS shall be capable of communicating status signals to the EPICS network for archiving, including but not limited to the following:
    i. PSS-SIS status (e.g. NSTX-U E-Stop and access modes)
    ii. Trapped key block status
    iii. Operationally sequenced subsystem status
    iv. Local PLC errors & alarms
b. The CCS shall be capable of sending signals to the EPICS network at a rate of up to 1 Hz.
c. The CCS shall provide a local backup archive for status signals including but not limited to the following:
    i. PSS-SIS status (e.g. NSTX-U E-Stop and access modes)
    ii. Trapped key block status
d. The CCS shall provide a means for engineering staff to retrieve local archive data without interruption of normal operations.

3.8 Design Standards and Verification

a. The CCS shall not be required to meet the requirements of an IEC 61508/61511 compliant Safety Instrumented System.
b. The CCS shall use typical process control signal voltages (e.g. 120 Vac, 24 Vac/dc, 5 Vdc)
c. Communications protocols and the physical layer that may be optionally used by the CCS shall be industry-standard for CCS-type applications.

3.9 Interfaces

See interface tables in Ref. [2]