PRINCETON PLASMA PHYSICS LABORATORY

ENG-050 - RD - REQUIREMENT DOCUMENT

Centralized Control System Software Requirements Document

NSTXU_1-7-3-8_RD_101

Work Planning #:
Effective Date: **01/08/2020**
Prepared By: **Benjamin Smith**

Reviewed By	Peter Dugan, System Engineer	01/08/2020 09:40:51 AM
Reviewed By	Joseph Petrella, Cognizant Individual	01/06/2020 10:44:57 AM
Reviewed By	Timothy N. Stevenson, Responsible Engineer	01/07/2020 15:37:35 PM
Reviewed By	Paul Sichta, Technical Authority	01/06/2020 11:50:05 AM
Reviewed By	Benjamin Smith, Preparer	01/07/2020 09:57:22 AM
Approved By	Yuhu Zhai, Project Engineer	01/08/2020 10:24:59 AM

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

NSTX-U Centralized Control System Software Requirements Document

NSTXU_1-7-3-8_RD_101 Rev 0

DATE

_____

Prepared by: Ben Smith, Plant I&C Engineer

_____

Reviewed by: Peter Dugan, Systems Engineering and Integration

_____

Reviewed By: Joseph Petrella, PSS COG

_____

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

_____

Reviewed by: Paul Sichta, Control and Data TA

_____

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

Record of Revisions

Date	Version	Brief Description of Changes
	Rev 0	Initial Release

1: Introduction

1.1 Purpose and Scope

a. This document specifies implementation requirements for the NSTX-U Centralized Control System (CCS) software. 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]). The logical configuration of the system shall be detailed in this document.

b. General requirements for the system are provided in Ref [1].

c. System requirements are provided in Ref [2]. This document flows the system requirements in that SRD down to specific implementation requirements.

D. Specific CCS requirements are provided in Ref [4].

1.2 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-024, NSTX-U Personnel Safety System Requirements
[4] NSTX-U-RQMT-RD-025, NSTX-U Centralized Control System Requirements
[5] NSTX-U-RQMT-RD-026, NSTX-U Trapped Key System Requirements
[6] ANSI/ISA 5.1, Instrumentation Symbols and Identification
[7] PPPL Quality Assurance Plan Description
[8] PPPL Procedure QA-028, Software Quality Assurance
[9] PPPL Procedure ENG-033, Design Verification
[10] PPPL Procedure ENG-030, PPPL Technical Procedures
[11] PPPL Procedure ENG-062, Planning and Performing Tests
[12] PPPL Procedure ENG-010, Control of Drawings
[13] PPPL Environment, Safety & Health Directive 5008
[14] PPPL Standard Cyber Security Program Plan, CSPP
[15] PPPL Procedure QA-003, Procurement Quality Assurance and Supplier Qualification
[16] Procurement Division Policies and Procedures Manual

[1] A " BCS" is the subsystems (FCPC, NB, RF) primary control system.

1.3 Definitions, Acronyms, and Abbreviations

Table 1.3-1 details several acronyms and abbreviations that are commonly used throughout the document.

Table 1.3-1: *Definitions, acronyms, and abbreviations found in CCS software spec.*

BOA	Basic Ordering Agreement
BCS	Basic Control System
CCR	Central Control Room
CCS	Centralized Control System
COE	Chief Operating Engineer
COTS	Commercial Off The Shelf
ECH-PI	Electron Cyclotron Heating - Pre-Ionization
ECN	Engineering Change Notice
FCPC	Field Coil Power Conversion
GDC	Glow Discharge Cleaning
HHFW	High Harmonic Fast Wave
HIS	Hardwired Interlock System
HMI	Human Machine Interface
I/O	Input / Output
IP	Installation Procedure
ISTP	Integrated System Test Procedure
IT	Information Technology
MSE-LIF	Motional Stark Effect with Laser-Induced Fluorescence
MGI	Mass Gas injection
MGS	Motorized Ground-Disconnect Switch
MPTS	Multi Pulse Thompson Scattering
NB	Neutral Beamline

NTC	NSTX-U Test Cell
NTP	Network Time Protocol
OPC	Open Platform Communications
PLC	Programmable Logic Controller
PSS	Personnel Safety System
PTP	Preoperational Test Procedure
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SLD	Safety Lockout Device
TFTR	Tokamak Fusion Test Reactor
TF Twist	Toroidal Field Twist
TKS	Trapped Key System
TVPS	Torus Vacuum Pumping System
UDT	User Defined Type
UPS	Uninterruptible Power Supply

2: Overall Description

2.1 Product Perspective

The CCS has been designed in conjunction with the PSS to replace the existing Hardwired Interlock System (HIS) that is currently used to coordinate specific NSTX-U subsystems. The HIS system was installed as part of the legacy Tokamak Fusion Test Reactor (TFTR) and was then modified to accommodate NSTX. The responsibilities of the PSS are described fully in Ref [3] but fundamentally its function is to monitor the configuration of NSTX-U and ensure personnel safety. The role of the CCS is to provide an interface for the Chief Operating Engineers (COE's) to coordinate the plant Basic Control Systems (BCS's). Figure 2.1-1 shows a high level overview of the subsystems the CCS interfaces with.

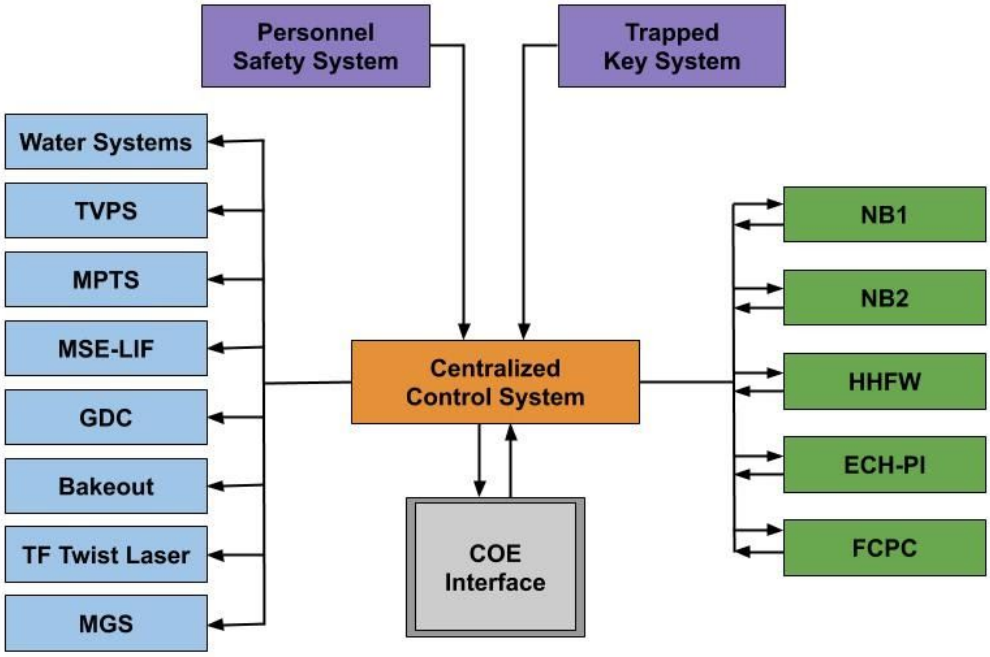

Figure 2.1-1: *Overview sketch of CCS showing subsystems and interfaces.*

2.2 Product Functions

The fundamental role of the CCS is to provide an interface for the COE to monitor the status of plant and grant permissives to the controlled subsystems. The CCS does not directly control the connected BCS's, it only provides and revokes permissives that allow them to operate. The CCS shall receive signals from the PSS-SIS that will be used to determine when subsystems are permitted to operate.

The CCS shall also receive and display signals from the Trapped Key System (TKS) to allow the COE to monitor the operating state of NSTX-U.

Certain BCS's require a complex set of commands to operate and these are referred to as operationally sequenced subsystems. These are listed below and described more fully in section 4.2:

- Field Coil Power Conversion (FCPC)
- Neutral Beamline 1 (NB1)
- Neutral Beamline 2 (NB2)
- High Harmonic Fast Wave Heating (HHFW)
- Electron Cyclotron Heating - Pre-Ionization (ECH-PI)

The remainder of the subsystems do not receive the same complex set of commands, they only receive signals equivalent to the (HIS) legacy "No E-Stop" and "Loop Set". The "No E-Stop" signal will now be referred to as "No NSTX-U E-Stop". The conditions for this signal are detailed fully in section 4.3, and the subsystems receiving these inputs are listed below:

- Massive Gas Injection (MGI) via the Torus Vacuum Pumping System (TVPS) PLC
- Bakeout System
- Glow Discharge Cleaning (GDC)
- Multi Pulse Thompson Scattering (MPTS)
- Motional Stark Effect with Laser-Induced Fluorescence (MSE-LIF)
- Water System PLC
    - OH Water Pre-heater
    - High Pressure & Low Pressure Pumps
- Motorized Ground-Disconnect Switch (MGS)
- Toroidal Field Twist Laser (TF Twist)

Table 2.2-1: *Systems receiving No NSTX-U E-Stop and Loop Set signals.*

System	No NSTX-U E-Stop	Loop Set
TVPS	X	X
MPTS	X	X
MSE-LIF	X	X
Bakeout	X	
GDC	X	
Water Systems	X	X
MGS		X
TF Twist	X	X

2.3 User Classes and Characteristics (Use Cases)

The most important user class of the CCS is the COE. The COE's are individuals who are trained and qualified to safely operate the NSTX-U facility, and as such they are the only individuals permitted to control the system. The design of the CCS shall prioritize the requirements of the COE's over any other users as they will interface with it most frequently, and they are ultimately responsible for the operation of NSTX-U. Those requirements are:

- Provide clear feedback on the operating status of the plant
- Allow the COE to quickly and easily remove permissives to operationally sequenced systems
- Provide a secure physical user interface

Another user class of the CCS are engineers who are qualified to, when appropriate, alter or test the system. This user class will only have infrequent interaction (e.g. annual testing) and so their requirements for the system are of lower priority than the COE's. The requirements for the engineering class user are:

- Provide the capability for an ethernet connection to the PLC from a secure laptop without physically entering the CCS cabinet
- Provide USB accessibility to remove data logs

The final user class of the CCS is the guest user who has no system rights, but can view the status of the plant via the COE interface panel and CCS HMI. The guest user has the ability to disable and disarm subsystems through the pushbuttons on the COE interface panel, in the event the COE becomes incapacitated during operations.

2.4 Operating Environment

The CCS shall be programmed using a COTS product portfolio, so no unique engineering solutions are foreseen. The software that the system must be capable of supporting is listed below:

- Windows 10 Enterprise 64bit version 1803 or newer
- Studio 5000 version 32.02 or newer
- FactoryTalk View Site Edition - version 11.00 or newer
- FactoryTalk Linx version 6.10 or newer

2.5 Design and Implementation Constraints

The following design and implementation constraints must be adhered to:

- The PLC and HMI must be developed using the software listed in section 2.4
- The PLC must be configured using the hardware described in section 3.2
- The PLC logic must be commented with rung comments at least every 5 rungs
- The HMI must be implemented with a secure login feature
- The front panel interface must be finger-safe to below 50V
- The CCS equipment must be powered by an uninterruptible power supply (UPS)

- The CCS must provide spare capacity of at least 25% for both digital inputs and digital outputs, as well as space for 2 spare in-chassis cards
- The CCS must provide a PPPL approved computer to run the HMI
- The CCS PC must be able to be time-synchronized through NTP with a PPPL NTP server
- The CCS PLC must be time-synchronized with the local PC using the Logix5000 Clock Update Tool

2.6 User Documentation

A user manual shall be developed to describe how to operate the system. This shall be delivered when the system has been fully installed and commissioned. The user manual will not cover the details of operating NSTX-U, it will only cover how to utilize and interface with the system.

2.7 Assumptions and Dependencies

In addition to the assumptions detailed in Ref [2], the team responsible for the design and development of the CCS assumes the following:

1. Existing field connections between the CCS and the BCS's are still intact and have been left unaltered since the beginning of the NSTX-U recovery project.
2. The BCS equipment is capable of being shut down safely in the allotted 1 second before the PSS-SIS takes action.
3. The external ethernet connections from the CCS to the PPPL network shall be protected by an IT-managed enterprise firewall as appropriate for a controls network VLAN.

3: External Interface Specifications

3.1 User Interfaces

The CCS shall utilize two primary user interfaces: a physical front panel display as well as a computer-based human machine interface (HMI). The primary goal for both of these interfaces is to allow the COE to monitor and control the operationally sequenced subsystems. As such the COE's shall be consulted throughout the design process to ensure their satisfaction with the interfaces.

3.1.1 Physical Front Panel

The CCS shall provide a physical interface located on the front of the CCS control panel that will provide the means to control the operationally sequenced subsystems. The front panel shall display the status of all the operationally sequenced subsystems in a clear and consistent fashion. The CCS front panel shall be distinct from the PSS front panel since these will share space in the same control rack. The CCS front panel shall be capable of expansion to incorporate future systems.

All control elements (e.g. pushbuttons, lights, key switches) shall be 24V DC powered to provide a finger-safe interface. All control elements shall be configured to fail safe. The front panel will utilize one COE key to perform all enable and arm functions, and provide a means to lock this key so that unauthorized users may not tamper with the system.

3.1.2 Human Machine Interface

The CCS shall provide an HMI for the user to view status and control the system. This section will describe the generic features and methods that will be used in implementation rather than detail specific screens. The HMI will be provided using FactoryTalk Site Edition software.

3.1.2.1 HMI Color / Animation standards

HMI operation screens shall be developed following the principals of high-performance HMI. The CCS shall follow a nominal color convention that may be altered if agreed upon by PPPL subject matter experts. The screenshot below shows the general layout and standards for what color and animation types are used for displays.

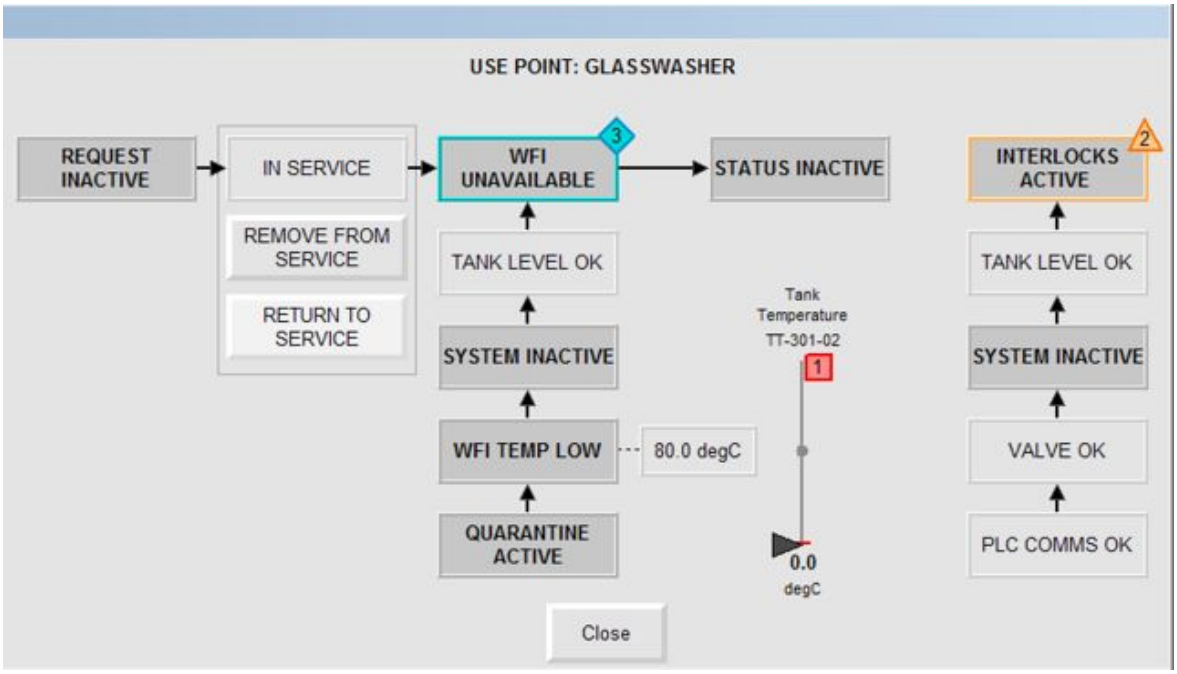

Figure 3.1.2.1-1: *Example graphic of the high-performance HMI standard*

The color scheme used in the example figure 3.1.2.1-1 is detailed below, which may be altered during implementation of the system:

Background: Gray
On/Active: White or light gray

Off/inactive: Dark gray
Overridden: Orange outline
Alarm: Determined by priority, summarized in the following table.

Table 3.1.2.1-1: *Table of alarm levels and their corresponding symbols, colors, and numbers*

Alarm Level	Symbol Color	Symbol	Number
High	Red	Square	1
Medium	Yellow	Triangle	2
Low/Diagnostic	Teal	Diamond	3

3.1.2.2 Digital Input

Digital Input objects display an input's status, override mode, and alarm state. If the input is active (enabled, high, open, etc.) then the indicator is shown with a white background. If the input is inactive (disabled, low, closed, etc.) then the indicator is shown with a gray background. When the input is in override mode the indicator is shown with an orange border. If an alarm is active a red triangle with the number '1' is shown to the left of the indicator. All possible object states are shown below with a description of what information is conveyed about the digital input.

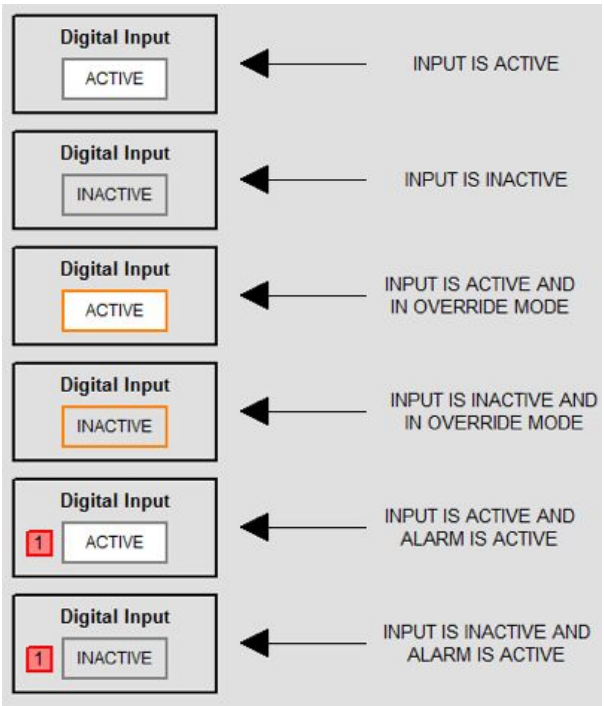

Figure 3.1.2.2-1: *Graphic showing the different states of a digital input*

Clicking the Digital Input object opens the Configuration popup for that respective input. The Digital Input's override and alarm can be configured from this popup.

To put the digital input in OVERRIDE mode, click on the MODE button which says "NORMAL" (the button will change to "OVERRIDE" with an orange outline). Click on the OVERRIDE STATUS button to force the current status to change. Clicking the MODE and OVERRIDE STATUS buttons will toggle their respective values. The HMI shall not allow the OVERRIDE mode to be activated, or the OVERRIDE STATUS to be changed, if the user does not have the appropriate authorization. All override events shall be logged by the CCS. Screenshots of this process are shown below.

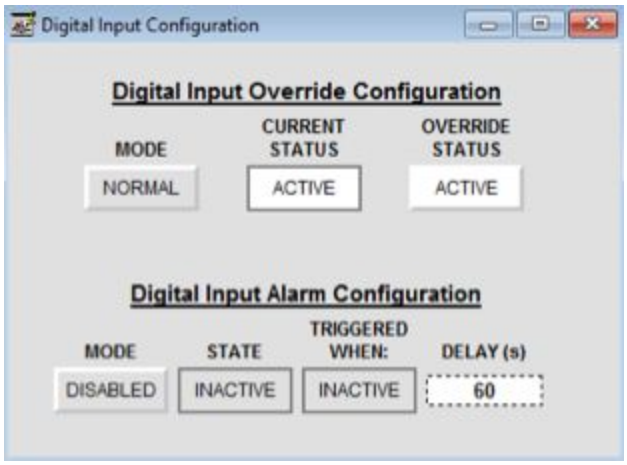

Figure 3.1.2.2-2: *Digital input graphic in the normal mode*

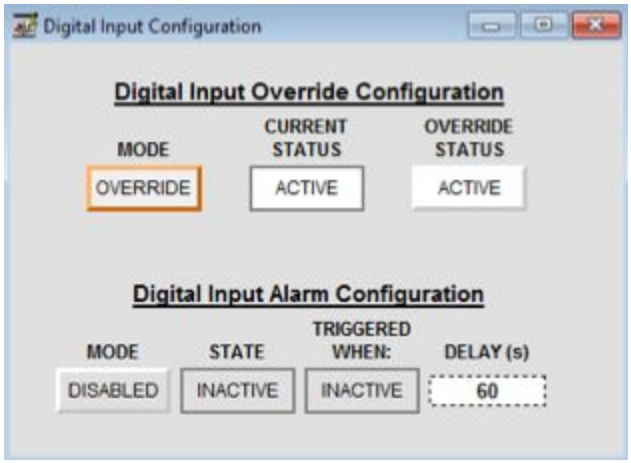

Figure 3.1.2.2-3: *Digital input graphic in the override mode*

The Alarm Configuration section is in the lower portion of the popup. It allows a user to enable or disable whether an alarm is produced when the trigger state is maintained and adjust the length of the delay to annunciate the alarm. The MODE button will display "DISABLED" when the alarm is disabled. Clicking the button will change the display to "ENABLED" with a white background and the alarm will be enabled. Click on the DELAY numeric input and enter the length of the alarm delay in seconds.

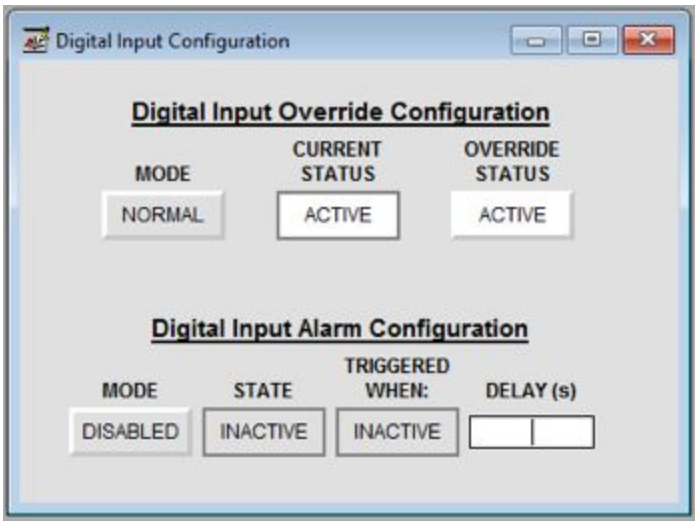

Figure 3.1.2.2-4: *Graphic showing digital input alarm configuration*

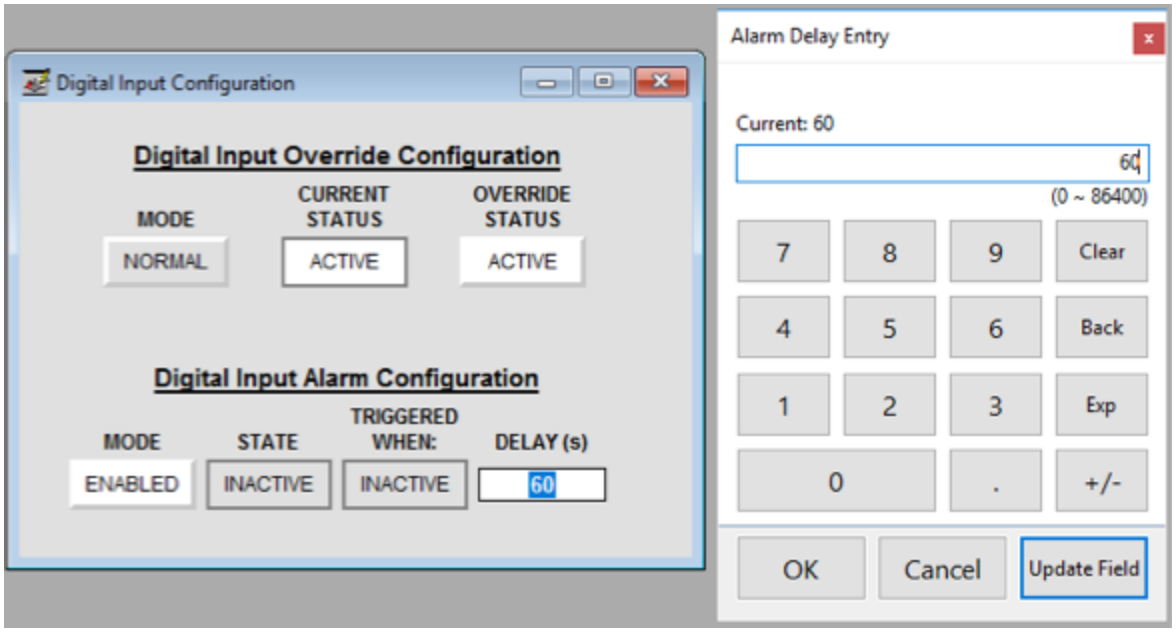

Figure 3.1.2.2-5: *Graphic showing the digital alarm time delay input field*

3.1.2.3 Digital Output

Digital Output objects display an output's status and override mode. If the output is active (enabled, open, etc.) then the indicator is shown with a white background. If the output is inactive (disabled, closed, etc.) then the indicator is shown with a gray background. When the output is in override mode the indicator is shown with an orange border. All possible object states are shown below with a description of what information is conveyed about the digital output.

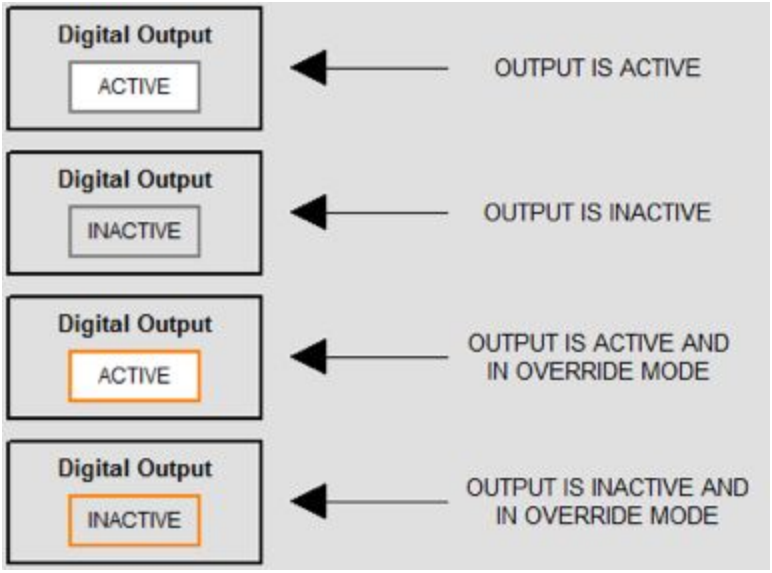

Figure 3.1.2.3-1: *Graphic showing the different states of a digital output*

Clicking on the Digital Output object opens the Override Configuration popup for that respective output. To put the digital output in override mode, click on the MODE button which says “NORMAL” (the button will change to “OVERRIDE” with an orange outline). Click on the OVERRIDE VALUE button to force the current status to change. The HMI shall not allow the OVERRIDE mode to be activated, or the OVERRIDE STATUS to be changed, if the user does not have the appropriate authorization. All override events shall be logged by the CCS. Screenshots of this process are shown below.

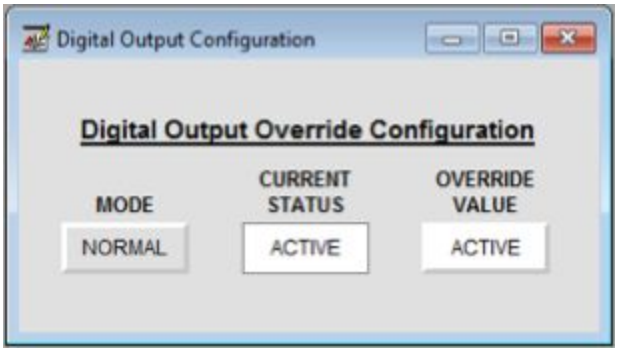

Figure 3.1.2.3-2: *Display of digital output graphic in the normal mode*

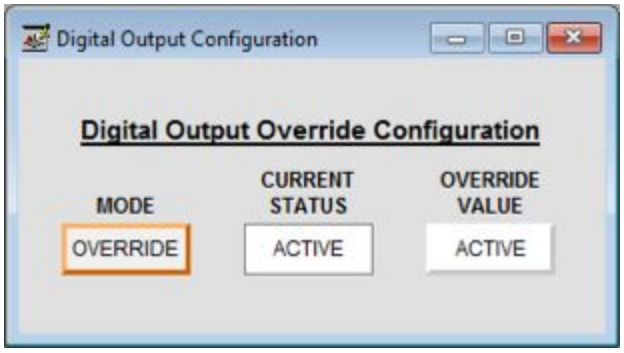

Figure 3.1.2.3-3: *Display of digital output graphic in the override mode*

3.2 Hardware Interfaces

The CCS Hardware Interface shall consist of a Logic Solver, IO modules and Operator Interface terminal. All components of the CCS shall be commercial off the shelf (COTS) items. Cut sheets for all hardware interface components shall be delivered as part of the system installation.

3.2.1 Logic Solver

CCS system is based on the Allen Bradley ControlLogix programmable logic controller (PLC) product line. The PLC is an L80-series PLC which includes a single integral Ethernet IP connection port.

3.2.2 Signal Monitoring & Control Modules

The CCS consists of digital input and output signals. 1756-series IO modules will be chassis-mounted and either local to the CCS PLC, or monitored over Ethernet I/P.

Digital Input signals will be monitored by 16-channel input modules at either 120V AC or 24V DC. Isolated modules will be used where signal voltages originate from sources outside the CCS panel.

Digital Output signals will be driven by 16-channel output modules at either 120V AC or 24V DC. Isolated modules will be used where CCS outputs are driving voltages that originate from sources outside the CCS panel.

3.2.3 Network Communication Modules

The CCS shall utilize 1756 series in-chassis network cards to expand the network communication capability of the PLC controller. Any network port that is not actively being utilized will be disabled to prevent any external access. Any component of the CCS that is capable of wireless communication shall have its wireless connection(s) disabled.

3.3 Software Interfaces

The software components of the CCS are all standard COTS Rockwell Automation features that are designed to operate together, therefore no unique engineering solutions are envisioned. The software components that will be used are detailed below:

- Studio 5000
- RSLinx
- FactoryTalk View Site Edition
    - FactoryTalk Alarms & Events
    - FactoryTalk Historian
    - FactoryTalk Security
    - FactoryTalk Directory
- Logix5000 Clock Update Tool
- Studio 5000 Logix Emulate

3.4 Communications Interfaces

The CCS shall be capable of transmitting signals via ethernet to an external OPC DA server. The local network infrastructure shall be capable of transmitting signals at a rate of at least 1 Hz. As stated in section 2.7 this connection shall be protected with an enterprise firewall rule.

All local network connections shall be via ethernet using Rockwell Automation COTS software, therefore no unique engineering solutions are envisioned.

3.5 Tagnames

The CCS will use structured tagname conventions to ensure consistency throughout the software. The purpose of the tagnames is to describe the function and associate it with a certain field device or subsystem. Two structures have been created; one for input and output signals that follows a strict template, and another for internal logic variables.

This tagname structure follows that of the PSS-SIS system so that engineers and users can readily work with each system, but also delineate between the two.

3.5.1 Input / Output Tagname Structure

As the CCS must interface with numerous NSTX-U systems a tagname structure has been developed that identifies which external interface is being communicated with, and what information that signal is relaying. There are specific abbreviations for each of the tagname fields detailed in Appendix A,

though the tagnames are not limited to only those listed. In the event the CCS expands to control more plant equipment new abbreviations may be required, but the structure will always be followed.

PREFIX	LOCATION	COMPONENT	FUNCTIONAL ID	LOOP NUMBER and (optional) SUFFIX	I/O TYPE (optional)

The tagname fields defined are:

- PREFIX: An abbreviation of the system that owns the device or signal. For all tags in the CCS, this abbreviation is CCS.
- LOCATION: An abbreviation for the physical location of the end device.
- COMPONENT: An abbreviation for the component that the tag is interfacing with.
- FUNCTIONAL ID: An abbreviation for the functional device type. These abbreviations were created using the ANSI/ISA 5.1 Standard Ref [6].
- LOOP NUMBER: A two-digit number that represents the control loop the tag is associated with. This field is optional.
- LOOP SUFFIX: A single letter designation immediately following the loop number to create a unique tag in situations where a duplicate tagname would exist. This field is optional.
- I/O TYPE: An abbreviation identifying what type of signal the tag represents.

The tagnames use an underscore to separate the fields. The software environment should support tagnames having up to 40 characters.

Example: CCS_FCPC_SLD_EY_DO
This tag describes a device located in the field coil power conversion (FCPC) building that is associated with the safety lockout device (SLD). The signal is an output relay (EY) and its type is a digital output (DO)

3.5.2 Internal Variable Tagname Structure

A different tagname structure was developed for internal variables that is simpler for developers and engineers to work with. Any tag that directly interfaces with the external systems will follow the structure given in section 3.5.1. By using different structures it is clear to all users which signals directly interface with end devices and which do not.

NAME	SUFFIX (optional)

A description of the tagname fields are:

- NAME: An alpha-numeric string that is descriptive of the tag's meaning.
- SUFFIX: An optional field to enhance the meaning of the tagname. The developer may use more than one suffix.

The internal variable tagnames use an underscore to separate the fields. The fields can use any alpha-numeric characters. The software should support tagnames up to 40 characters in length.

Example: FCPC_Dummy_Load_OK
This tag describes an internal variable that represents permission for the FCPC system to enter into the dummy load testing mode.

4: Software Modules

The CCS shall be developed using common software modules for all functions where this is possible. These common software modules shall be tested during development, which will help reduce time during commissioning. Utilizing common solutions will also reduce the effort to add new systems in the future.

4.1 Software I/O Conditioning

Each I/O type (digital input, digital output) shall be be programmed in the CCS as a standard User-Defined Type (UDT). This will provide a common structure for programming, interface design and data monitoring/archiving.

4.1.1 Digital Inputs

All digital inputs monitored by the CCS shall have a physical address, associating it's rack location, slot location, and point number. These input points shall be mapped to logical tags in the CCS, which is what will ultimately be used in the programming.

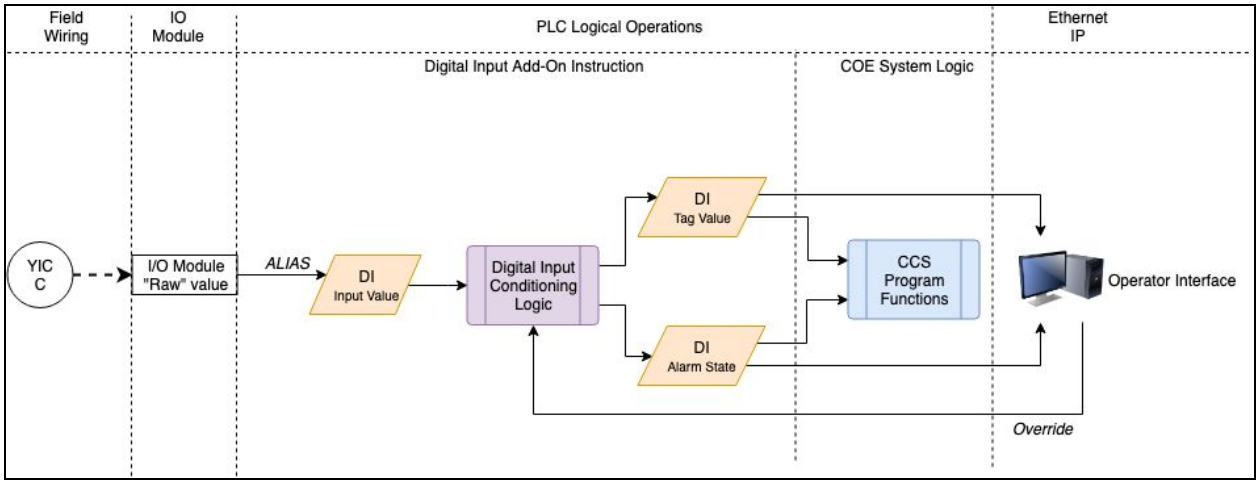

Figure 4.1.1-1: *Diagram showing the operations on a digital input signal.*

4.1.2 Digital Outputs

All digital outputs controlled by the CCS shall have a physical address, associating it's rack location, slot location, and point number. These output points shall be mapped to logical tags in the CCS, which is what will ultimately be used in the programming.

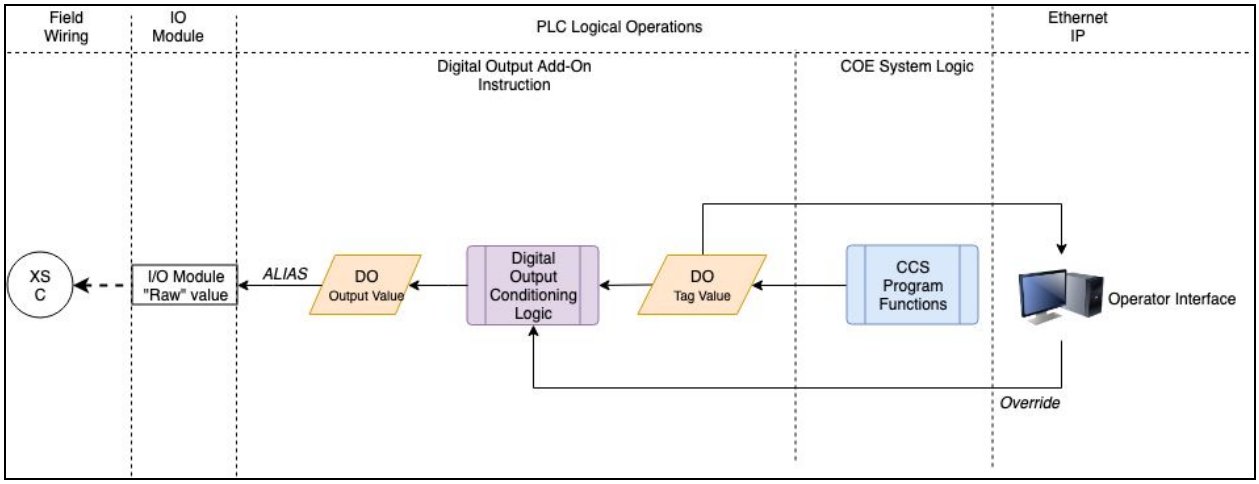

Figure 4.1.1-2: *Diagram showing the operations on a digital output signal.*

4.2 Operationally Sequenced Control

Certain BCS's require sequenced commands to operate. These commands are the enable and arm signals, which must be sent sequentially in that order. These systems are referred to as the operationally sequenced subsystems. This delineates these subsystems from the others which require only the simple permissives (No NSTX-U E-Stop, Loop Set) which are detailed in section 4.3. The subsystems requiring sequenced commands are listed in the "Operationally Sequenced Systems" section of Ref [4].

The CCS will provide a common set of signals to all of the operationally sequenced subsystems. These signals and their initiating conditions are described fully in the following subsections.

4.2.1 Permit to Enable

The permit to enable signal is a unique permissive signal sent by the COE to each operationally sequenced BCS. The signal shall transition to the high state when the COE actuates the unique key switch on the COE interface panel to the correct position and remain latched in the high state until the permissive is revoked. In the event the signal transitions from the high state to the low state, it

shall not return to the high state until the COE again actuates the unique key switch on the COE interface panel.

The permit to enable signal can be deactivated at any time using the COE interface panel, or via commands on the CCS HMI. Table 4.2.1-1 lists all the conditions that would revoke the permit to enable signals to the subsystems. All signals that are used as conditions to deactivate the permit to enable signals shall be implemented to be fail-safe (i.e. power off shall revoke the permissive).

Table 4.2.1-1: *List of conditions that revoke the permit to enable signals to the BCS's*

Subsystem	**Conditions that Revoke Permit to Enable**	
	PSS-SIS	**COE Interface**
NB1	Loss of PSS-SIS Emergency Stop Loss Safe to Enable NB	Master Disable Pushbutton NB1 Disable Pushbutton
NB2	Loss of PSS-SIS Emergency Stop Loss Safe to Enable NB	Master Disable Pushbutton NB2 Disable Pushbutton
FCPC	Loss of PSS-SIS Emergency Stop Loss Safe to Enable FCPC	Master Disable Pushbutton FCPC Disable Pushbutton
RF	Loss of PSS-SIS Emergency Stop Loss of NTC in NO ACCESS	Master Disable Pushbutton RF Disable Pushbutton

4.2.2 Permit to Arm

The permit to arm signal is a unique permissive signal sent by the COE to each operationally sequenced BCS. The signal shall transition to the high state when the COE actuates the unique key switch on the COE interface panel to the correct position and remain latched in the high state until the permissive is revoked. In the event the signal transitions from the high state to the low state, it shall not return to the high state until the COE again actuates the unique key switch on the COE interface panel.

The permit to arm signal can be deactivated at any time using the COE interface panel, or via commands on the CCS HMI. Table 4.2.2-1 lists all the conditions that would revoke the permit to arm signals to the subsystems. All signals that are used to deactivate the permit to arm signals shall be implemented to be fail-safe (i.e. power off would revoke the permissive).

Table 4.2.2-1: *List of conditions that revoke the permit to arm signals to the BCS's*

Subsystem	**Conditions that Revoke Permit to Arm**

	PSS-SIS	COE Interface
NB1	Loss of PSS-SIS Emergency Stop Loss Safe to Enable NB	Master Disable Pushbutton Master Disarm Pushbutton NB1 Disable Pushbutton NB1 Disarm Pushbutton
NB2	Loss of PSS-SIS Emergency Stop Loss Safe to Enable NB	Master Disable Pushbutton Master Disarm Pushbutton NB2 Disable Pushbutton NB2 Disarm Pushbutton
FCPC	Loss of PSS-SIS Emergency Stop Loss Safe to Enable FCPC	Master Disable Pushbutton Master Disarm Pushbutton FCPC Disable Pushbutton FCPC Disarm Pushbutton
HHFW	Loss of PSS-SIS Emergency Stop Loss of NTC in NO ACCESS	Master Disable Pushbutton Master Disarm Pushbutton RF Disable Pushbutton HHFW Disarm Pushbutton
ECH-PI	Loss of PSS-SIS Emergency Stop Loss of NTC in NO ACCESS	Master Disable Pushbutton Master Disarm Pushbutton RF Disable Pushbutton ECH-PI Disarm Pushbutton

4.2.3 Disable

The disable signal is a unique signal sent by the COE to revoke the permit to enable and permit to arm signals of an operationally sequenced BCS. The disable signal can be actuated at any time using the COE interface panel, or via commands on the CCS HMI. The master disable signal located on the COE interface panel shall send disable commands to all operationally sequenced subsystems.

4.2.4 Disarm

The disarm signal is a unique signal sent by the COE to revoke the permit to arm signal of an operationally sequenced BCS. The disarm signal can be actuated at any time using the COE interface panel, or via commands on the CCS HMI. The master disarm signal located on the COE interface panel shall send disarm commands to all operationally sequenced subsystems.

4.2.5 Permit to Remove Air

The Safety Lockout Device (SLD) receives a permit to remove air signal (vent) from the CCS. The signal shall transition to the high state when the COE actuates the three way switch that controls the SLD to the “vent” position and all FCPC rectifiers report that they are disabled. The permit to remove air signal shall be momentary.

4.2.6 Permit to Restore Air

The SLD receives a permit to restore air signal (pressurize) from the CCS. The signal shall transition to the high state when the COE actuates the three way switch that controls the SLD to the “pressurize” position. The signal shall only transition to the high state when the PSS-SIS Emergency Stop and Safe to Enable FCPC from PSS-SIS signals are configured properly. The permit to restore air signal shall be momentary.

4.2.7 Feedback from Operationally Sequenced Systems

The CCS shall receive feedback signals from the operationally sequenced systems that, at a minimum, defines their current operating status. These signals shall be used by the COE interface panel and the CCS HMI to indicate the status of the plant to the COE. Table 4.2.7-1 lists all the feedback signals from each BCS that will be monitored by the CCS.

Table 4.2.7-1: *Feedback signals from operationally sequenced systems.*

Subsystem	**Feedback Signals**	
NB1	Disabled Disarmed	Shutdown Enabled
NB2	Disabled Disarmed	Shutdown Enabled
FCPC	TF Disabled TF Disarmed TF Coils Level 1 Fault TF Coils Level 3 Fault TF Coils Level 4 Fault TF Coils in Configure	EF Disabled EF Disarmed EF Coils Level 1 Fault EF Coils Level 3 Fault EF Coils Level 4 Fault EF Coils in Configure
SLD	Lockout Complete	Air Restored
HHFW	Disabled Disarmed	Shutdown Enabled
ECH-PI	Disabled Disarmed	Shutdown Enabled

4.3 Legacy HIS Signal Equivalents

The CCS will provide certain legacy signals from the Hardwired Interlock System (HIS) that are still required. The logical implementation of certain signals have changed, which is captured in the following subsections.

4.3.1 No NSTX-U E-Stop

The CCS shall provide the No NSTX-U E-Stop signal as an equivalent to the legacy No E-Stop signal. This signal is used by numerous NSTX-U systems that do not receive the full operationally sequenced commands as a permissive to operate. The No NSTX-U E-Stop signal shall be high when the PSS-SIS Emergency Stop is high, and low otherwise. The full list of systems receiving this signal can be found in Table 2.2-1.

4.3.2 Loop Set

The CCS shall provide the Loop Set signal as an equivalent to the legacy Loop Set signal. This signal is used by numerous NSTX-U systems that do not receive the full operationally sequenced commands as a permissive to operate. The Loop Set signal shall be high when the PSS-SIS NTC Area NO ACCESS signal is high, and low otherwise. The full list of systems receiving this signal can be found in Table 2.2-1.

4.4 Testing / Bypassing

The CCS will require testing throughout its lifecycle to verify it is operating properly. There are several testing cases foreseen, which include but are not limited to:

- System commissioning
- Operational proof testing
- Troubleshooting or diagnosing faults

While different administrative protocols may be used in each of the above cases, the program shall provide one solution that can be used for all cases.

4.4.1 Input Testing

In order to confirm the signal from a given field device is being monitored properly by the PLC it is necessary to alter the state of the device (e.g. opening a cabinet door to confirm the door switch reports the change in state). Testing in this manner confirms the entire configuration of the signal loop, from the device to the local terminal blocks, through any conduit and junction boxes, and

ultimately to the PLC. However when this occurs the program logic will take actions based on that change of state, which may not be tenable to the system at that given time.

To accommodate this the CCS will provide the capability to override the field signal, allowing the testing team to monitor the change of the input state without affecting the system. Figure 4.4.1-1 below shows a graphical representation of the override function being applied.

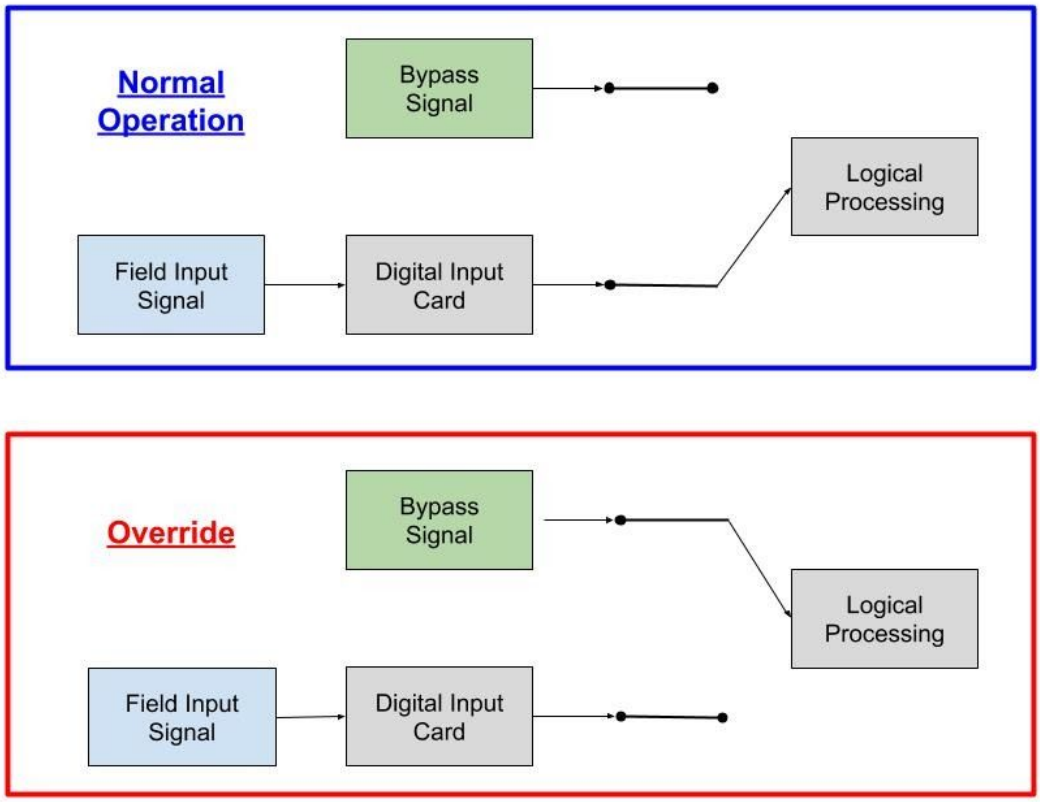

Figure 4.4.1-1: *Representation of normal operation and the override function in the software.*

4.4.2 Output Testing

In similar fashion to the input testing, it is necessary to confirm the output signal from the PLC communicates to the end device in the field, verifying the action(s) taken have the desired effects. In certain cases using the system logic as configured may be possible, but in others it may be inconvenient or impractical to do so. Additionally, it may not be desirable to actuate certain field devices more than once during functional testing as it would cause more wear without providing additional value.

In these cases the CCS will provide the ability to force the output signal to a given state. This will allow the testing team to simulate a change in state and confirm the overall system response, or to

maintain an output state to prevent deterioration during extended logic testing. Figure 4.4.2-1 depicts the configuration of the output override being applied.

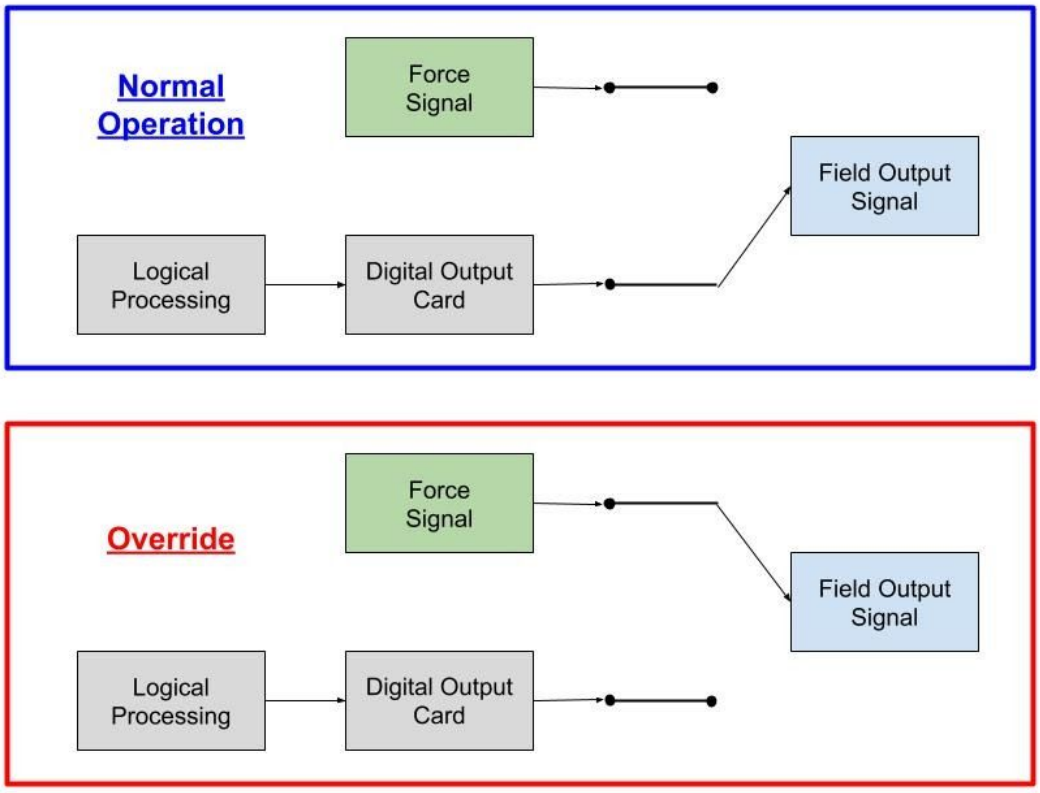

Figure 4.4.2-1: *Representation of normal operation and the override function in the software.*

4.5 Alarms

PLC and Process Alarms will be generated within the CCS PLC. These alarms will be displayed on the CCS User Interface. CCS alarms may only be acknowledged from the CCS User Interface. The CCS PC shall be capable of audibly annunciating alarms.

Definitions of PLC alarms and their configuration shall be detailed in an alarm list to be developed during the implementation phase of the project. This alarm list shall be maintained throughout the life of the system as configuration changes are made.

4.5.1 I/O Alarms

The CCS PLC will monitor and compare the actual state and expected state of digital inputs. Should there be a misalignment between the actual and expected states after a prescribed time delay, the CCS PLC will activate the alarm.

4.5.2 Process Alarms

Process alarms are used to indicate an abnormal condition or event which is determined by logical configured with the CCS PLC. The definition of process alarms and the conditions or events that will drive them will be defined in the alarm list.

4.5.3 Alarm States

Within the CCS FactoryTalk application, the following alarm states will exist:

- Active: Driven by the CCS PLC, an alarm will be active when conditions that generate the alarm are present.
- Inactive: Driven by the CCS PLC, an alarm will be inactive when conditions that generate the alarm are not present.
- Acknowledged: Driven by the CCS user interface application, the acknowledged state indicates operators have confirmed their knowledge of the alarm condition. Operators signal their acknowledgement through software buttons programmed in within the interface application.
- Unacknowledged: Driven by the CCS user interface application, the unacknowledged state indicates operators have yet to confirm their knowledge of the alarm condition.

4.5.3.1 Activation Response

The CCS PLC shall react to an active alarm according to the program logic.

At the User Interface, an active alarms may result in changes to the display. Object coloring may change, symbols may appear, animations may be initiated. The interface program shall log, date and timestamp when the alarm became active. The alarm will be listed in the alarm list.

4.5.3.2 Inactivation Response

The CCS PLC shall react to an active alarm according to the program logic. Some alarms may be contain logic requiring an operator reset the affected system(s) once the alarm condition has resolved; requirement of operator initiated reset shall be detailed in the alarm list.

At the User Interface, an inactive alarm may result in changes to the display. Object coloring may change, symbols may be hidden, animations may be inhibited. The interface program shall log, date and timestamp when the alarm became inactive.

4.5.3.3 Alarm Acknowledgement

The operation of the CCS PLC will not be affected when an alarm is acknowledged.

If active when acknowledged:
At the User Interface, an acknowledged active alarms may result in changes to the display. Object coloring may change, symbols may appear, animations may be initiated. The interface program shall log, date and timestamp when the alarm was acknowledged. The acknowledged inactive alarm will be listed in the alarm list.

If inactive when acknowledged:
An acknowledged inactive alarms may result in changes to the display. Object coloring may change, symbols may appear, animations may be initiated. The interface program shall log, date and timestamp when the alarm was acknowledged. An acknowledged inactive alarm will be removed from the active alarm list.

4.6 Archive Historian

The CCS will provide an archive historian as a means for the NSTX-U operations team to historically examine, analyze, and trend data. The primary method for this will be transmitting signals to the existing OPC server on site where it can be stored by EPICS. The CCS will also provide a local historian to capture a subset of the data. This can be used to diagnose issues encountered during operation or as a backup source of data in the event the primary OPC interface is temporarily inactive.

4.6.1 OPC Server

The CCS shall provide an ethernet connection to the existing plant OPC network to allow EPICS to reach and archive data. This connection shall be on a separate VLAN from the other CCS networked devices. The switch port that this communication utilizes shall be appropriately protected in a manner decided upon by the PPPL cyber security team.

The tags to be sent to the OPC server should include, but not be limited to, the following:

- Signals from PSS-SIS Chain A
- Signals from the TKS
- Inputs from the controlled subsystems
- Inputs from the COE interface
- Outputs to the controlled subsystems
- Password login by COE’s
- System alarms

4.6.2 Local Archive Historian

The local historian will be programmed using FactoryTalk View Site Edition Data Logging software. This feature is provided with FactoryTalk View Site Edition, which will be installed and operating on the local computer to provide the user interface. The Data Logging program can be configured by the user to log up to 10,000 data points. The data is written to a plain text Comma Separated Value (CSV) file and can be stored on the local hard drive, another computer, or a USB drive. The log shall include a timestamp with at least 1 second resolution.

Since the local historian is configured as a backup only a limited subset of the available data will be archived. The tags that will be stored include, but are not limited to, the following:

- Signals from PSS-SIS Chain A
- Signals from the TKS
- Inputs from the controlled subsystems
- Outputs to the controlled subsystems

5: Other Nonfunctional Requirements

5.1 Simulation Requirements

The system shall be capable of simulation using the Rockwell Automation RSLogix Emulate 5000 software program. This is a standard COTS program provided by Rockwell Automation for use with Studio 5000, so no unique engineering solutions are envisioned.

5.2 Performance Requirements

The CCS must adhere to the following performance requirements:

- The CCS must be capable of initiating a safe shutdown signal in 0.25 seconds or faster
- The PLC must be capable of reading the inputs at a frequency of 10 Hz
- The PLC must be capable of updating output signals at a rate of 10 Hz
- The PC used for the CCS must be capable of supporting up to 4 color display monitors with resolution of 1920 x 1080 @ 60Hz

5.3 Safety Requirements

The CCS shall be compliant with Ref [13]. Additional safety-related requirements are detailed in section 2.5 and section 5.4.

5.4 Security Requirements

The CCS allows several important and potentially hazardous NSTX-U subsystems to operate. As such, there are a number of security requirements which are detailed in the following subsections.

5.4.1 Physical Security

The physical hardware associated with the CCS must be appropriately protected to ensure none of the controlled subsystems are affected, incidentally or intentionally.

5.4.1.1 Front Panel Interface Security

The COE front panel interface shall be controlled by one unique key that will be locked and retained until the COE logs in with their password to the HMI and releases the key. Releasing the key shall activate a timer in the PLC, and if the key is not utilized on the front panel before the duration of the timer ends the HMI shall annunciate an alarm. If the COE logs out of the HMI before returning the key to the appropriate locked position the HMI shall annunciate an alarm.

5.4.1.2 Control Cabinet Security

The cabinet that houses the CCS equipment shall utilize door switches to monitor any access events into the cabinet. When a door switch detects an entry the HMI shall annunciate an alarm and log the date and time of the event. The cabinet shall be locked with uniquely keyed fasteners that cannot be removed without the use of a specially designed tool. This tool will be administratively locked away and will only be provided to qualified PPPL staff who have taken the appropriate training. Any accessible ports to CCS control equipment (PLC, PC, etc.) shall be covered to prevent access.

5.4.2 Cyber Security

The CCS shall be assessed by the development team and the PPPL Cyber Security Department using Ref [14]. This assessment shall categorize any potential breach of security as either low, medium, or high impact. The CCS shall be designed and implemented to meet the necessary security mitigation based on this categorization. A comprehensive test plan shall be developed and executed after installation of the system to ensure all controls have been implemented and are functioning as expected.

5.4.2.1 Network Interface Risk Mitigation Measures

The CCS local network shall be maintained on a separate VLAN than existing PPPL networks. The ethernet connection to the PPPL network shall be protected using an enterprise firewall maintained by the PPPL IT department. The interface between the CCS and the PSS-SIS shall be hardwired electrical signals that only transmit data from the PSS-SIS to the CCS, creating an air-gapped interface between the PPPL network and the PSS-SIS.

5.4.2.2 Hardware Risk Mitigation Measures

The following equipment utilized for the CCS shall be tracked by the IT department using the System Change Notice process and Device Registration Forms:

- PLC Hardware
- Network Switch
- Computer

5.4.2.3 Software Risk Mitigation Measures

The computer used to run the CCS HMI and data logging software shall be protected using PPPL two-factor authentication. The following software programs shall be password protected to ensure only authorized PPPL engineering staff can make changes when necessary:

- Studio 5000 (logic programming)
- FactoryTalk
    - View (HMI programming)
    - Alarms & Events
    - Security (HMI user rights & passwords)

The CCS HMI program shall be password protected and provide the three user classes defined in section 2.3. A timeout function shall be implemented to prevent users from remaining logged in after periods of inactivity.

5.4.2.4 Vendor Risk Mitigation Measures

The CCS will be developed by an internal PPPL engineering team in collaboration with outside vendors. Any vendor assisting in the CCS design shall be qualified through a Basic Ordering Agreement (BOA), which requires assessment and approval by the PPPL QA department in accordance with Ref [15]. Any software developed by the vendor will be vetted and approved by the PPPL engineering team responsible for CCS prior to implementation. Vendors will not be permitted to directly access the system.

5.5 Software Quality Assurance

According to Ref [7] and the categorization process described in Ref [8] the CCS is categorized as A-3 software. As such the only required control is software categorization and inventory, however additional controls will be applied as a means of best practice.

The requirements of the system have been developed using Ref [9], and shall be approved by a set of appropriate signatories. The software design description shall be developed in accordance with Ref [8]. Changes are expected over the lifecycle of the system; these will be documented in the design description and tracked.

Verification tests shall be produced according to Ref [10] and Ref [11] and executed prior to using the system for operations. These shall include Installation Procedures (IP's) for any installed components, including but not limited to control cabinets, wiring, and conduit runs, and an Integrated System Test Procedure (ISTP) to confirm the entire system is configured properly. In addition, Preoperational Test Procedures (PTP's) will be developed to confirm the system has not been altered in between run periods and is ready to support the ISTP.

Drawings related to the system shall be updated to as-built status following the installation and commissioning of the system. This shall be accomplished using the Engineering Change Notice (ECN) process as described in Ref [12].

5.6 Business Rules

All purchases for CCS equipment shall be made through the PPPL procurement office in compliance with Ref [16]. Vendors who assist in the development of the CCS software shall be assessed and approved by the PPPL QA department in accordance with Ref [15].

6. Appendices

Appendix A: Tagname components for CCS input / output variables

Tagname Field	Abbreviation	Description
Prefix	CCS	Centralized Control System
Location	CCR	Central Control Room
Location	FCPC	Field Coil Power Conversion
Location	NBPC	Neutral Beam Power Conversion Building
Location	RFE	RF Enclosure
Location	NTC	NSTX-U Test Cell
Location	TCB	Test Cell Basement
Component	PERM	Permissive or Status of Subsystem
Component	SIS	Safety Instrumented System
Component	COE	COE Station
Component	TKBXX	Trapped Key Block (XX = unique identifier)
Functional ID	EY	Voltage-operated relay
Functional ID	HMS	Hand-operated momentary switch
Functional ID	HS	Hand-operated switch (key)
Functional ID	YIC	State Indicating Controller (PLC)
Functional ID	YY	State of Device
Functional ID	ZS	Position Switch
Functional ID	ZSSC	Position of Safety Switch Closed (Door Switch)
I/O Type	DI	Digital Input
I/O Type	DO	Digital Output