PRINCETON PLASMA PHYSICS LABORATORY

ENG-050 - RD - REQUIREMENT DOCUMENT

Safety Instrumented System Software

NSTXU_1-7-3-1_RD_100

Work Planning #: **3032**
Effective Date: **01/06/2020**
Prepared By: **Joseph Petrella**

Approved By	Kathleen Lukazik, Preparer	01/06/2020 16:14:07 PM

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

NSTX-U Personnel Safety System - Safety Instrumented System Software Requirements

NSTXU_1-7-3-1-1_RD_100_00

December 17, 2019

PAUL SICHTA Digitally signed by PAUL SICHTA Date: 2019.12.20 16:58:20 -05'00'

Prepared by: Paul Sichta, Control and Data TA

Timothy N. Stevenson Digitally signed by Timothy N. Stevenson Date: 2019.12.20 17:14:17 -05'00'

Reviewed by: Timothy Stevenson, Application Owner, NSTX-U Operations Head, OSS RE

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: 2019-12-23 10:06:20

Reviewed by: Joseph Petrella, Project Cognizant Engineer

Peter Dugan Digitally signed by Peter Dugan Date: 2019.12.30 07:31:27 -05'00'

Reviewed by: Peter Dugan, Systems Engineering and Integration

GREGORY J TCHILINGUIRIAN Digitally signed by GREGORY J TCHILINGUIRIAN Date: 2020.01.02 10:35:49 -05'00'

Reviewed by: Greg Tchilinguirian, Control and Data TA

Robert Ellis Digitally signed by Robert Ellis Date: 2020.01.03 16:50:27 -05'00'

Approved by: Bob Ellis, PPPL Chief Engineer

Yuhu Zhai Digitally signed by Yuhu Zhai Date: 2020.01.03 22:24:10 -05'00'

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

Record of Revisions

Date	Version	Brief Description of Changes
12/17/19	Rev 0	Initial Release

Table of Contents

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] NSTXU_1-7-3-1_CALC_100 PSS-SIS Calculations
[4] NSTX-U-RQMT-RD-024, NSTX-U Personnel Safety System - Safety Instrumented System Requirements
[5] NSTXU_1-7-3-1-1_DOC_100. NSTX-U PSS-SIS Software Design Description
[6] NSTX-U-RQMT-RD-025, NSTX-U Centralized Control System Requirements
[7] QA-028 , Software Quality Assurance, Revision 1, January 2019.
[8] NSTXU_1-7-3-1-1_QAP-100-00, NSTX-U Personnel Safety System - Safety Instrumented System Software Quality Assurance Plan
[9] NSTXU_1-7-3-1-2_DOC_100, NSTX-U PSS-SIS Cyber Security Assurance
[10] NSTXU_1-7-3-1-1_TPLAN_100, NSTX-U PSS-SIS Software Test Plan

1. Introduction

1.1 Purpose and Scope

This document will specify the NSTX-U Safety Instrumented System's (SIS) software functionality and features. The SIS requirements are described in [1] and this document flows applicable requirements down to the software engineering realm. The primary role of this document is to define the functional requirements of the software. The *System Features* chapter contains a depiction of the logic functions that are used to protect personnel from the identified hazards at NSTX-U. The description will refer to the areas, equipment, and operating modes that apply specifically to NSTX-U. Most of the other chapters in this document are generic to any SIS based upon a programmable logic solver. It is expected that all of the software specified here can be provided by a COTS (SIS) Limited Variability Language (LVL) product portfolio; no customization is anticipated to the COTS software package.

1.2 Definitions

Most definitions relevant to this document are provided in the Ref. [2]. For document-specific definitions see Table 1.2-1 below.

Table 1.2-1 Definitions, Acronyms, Abbreviations

Item	Description
debounce	Debounce is the act to remove rapid logic transitions that some monitoring devices exhibit when near to their switching threshold. After debouncing, the device will seemingly provide a single, stable transition.
inconsistent status	When the allowed and present state of Interlocked equipment does not agree, if interlocked equipment is in an unsafe state.
LVL	Limited Variability Language: type of language that provides the capability to combine predefined, application specific, library functions to implement the safety requirements specifications.
module	A module is a container of subroutines.
Process Variable	A process variable is the current measured value of a particular part of a process which is being monitored or controlled. It can also be an internally-derived variable used by software.
program mode	A mode the PLC can be set to, typically with a front panel key. In PROGRAM mode, the CPU Unit is stopped. Programming can be created or modified, memory can be cleared, programs can be checked.
RPI	Requested packet interval (RPI): The RPI specifies the period at which data updates over a connection. For the SIS, this pertains to a PLC to I/O module data transfers.

run mode	A mode the PLC can be set to, typically with a front panel key. RUN mode is used for normal system operation. Bits cannot be force-set/reset, and present values and set values cannot be modified using programming devices.
safety tag	A tag that has a safety pedigree. This means that the tag's value was generated from safety I/O, and/or safety logic instructions that have used only safety tags for its input(s).
subroutine	Subroutines are small programs to perform specific tasks that can be called for use in larger programs.
Tag, Tagname	A tag is a name that is used in application programs to uniquely identify data.
time-to-interdict	An elapsed time; starting with the action that initiates the interdiction and ending when the interdiction has been confirmed.

2. Overall Description

2.1 Product Perspective

The NSTX-U Personnel Safety System (PSS) ensures workers are protected from the special hazards that are inherent in the operation of NSTX-U. Multiple independent protection layers are used to build a defence-in-depth scheme as depicted in fig. 2.1-1. The software specified in this document is a critical component of the PSS for NSTX-U. The SIS sensors, hardware, and software must meet or exceed the minimum required risk reduction factor as calculated in reference [3]. An overview of the SIS architecture is shown in fig. 2.1-2.

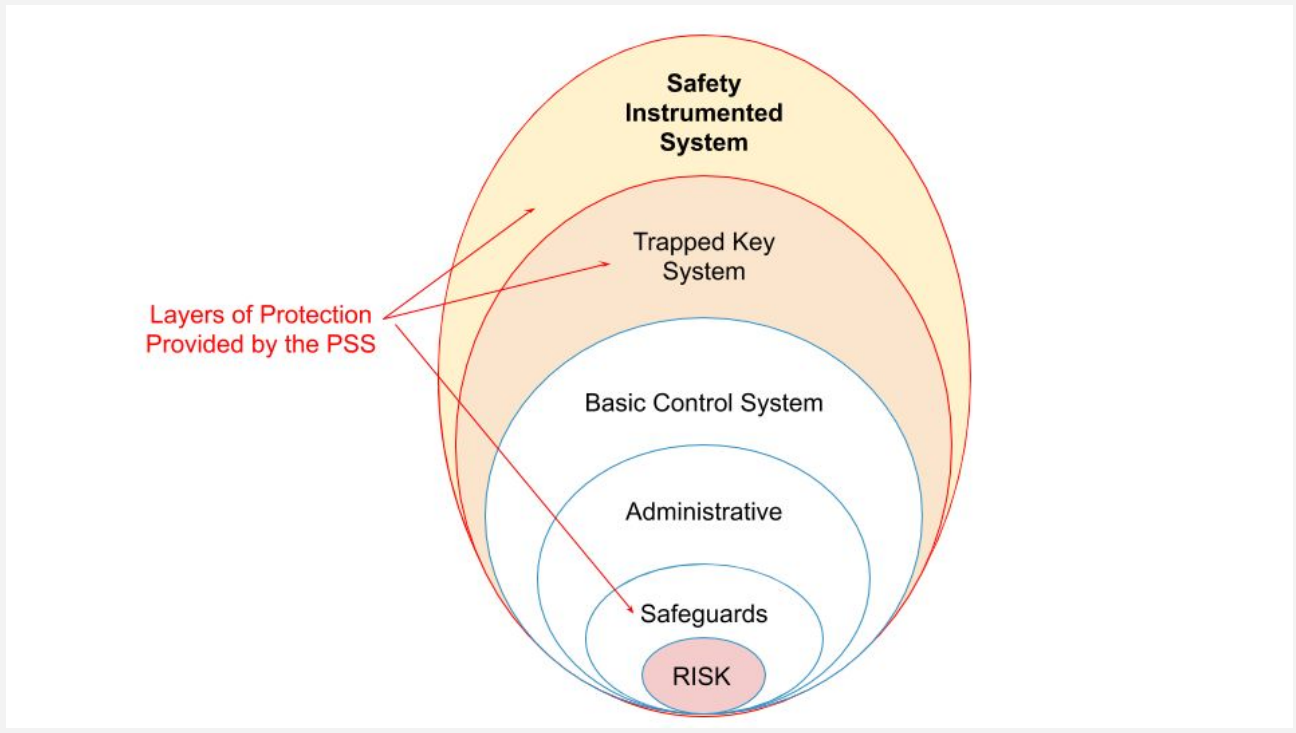

Figure 2.1-1 A diagram showing the layered approach to safety at NSTX-U. The SIS and its software provides the final layer of personnel protection.

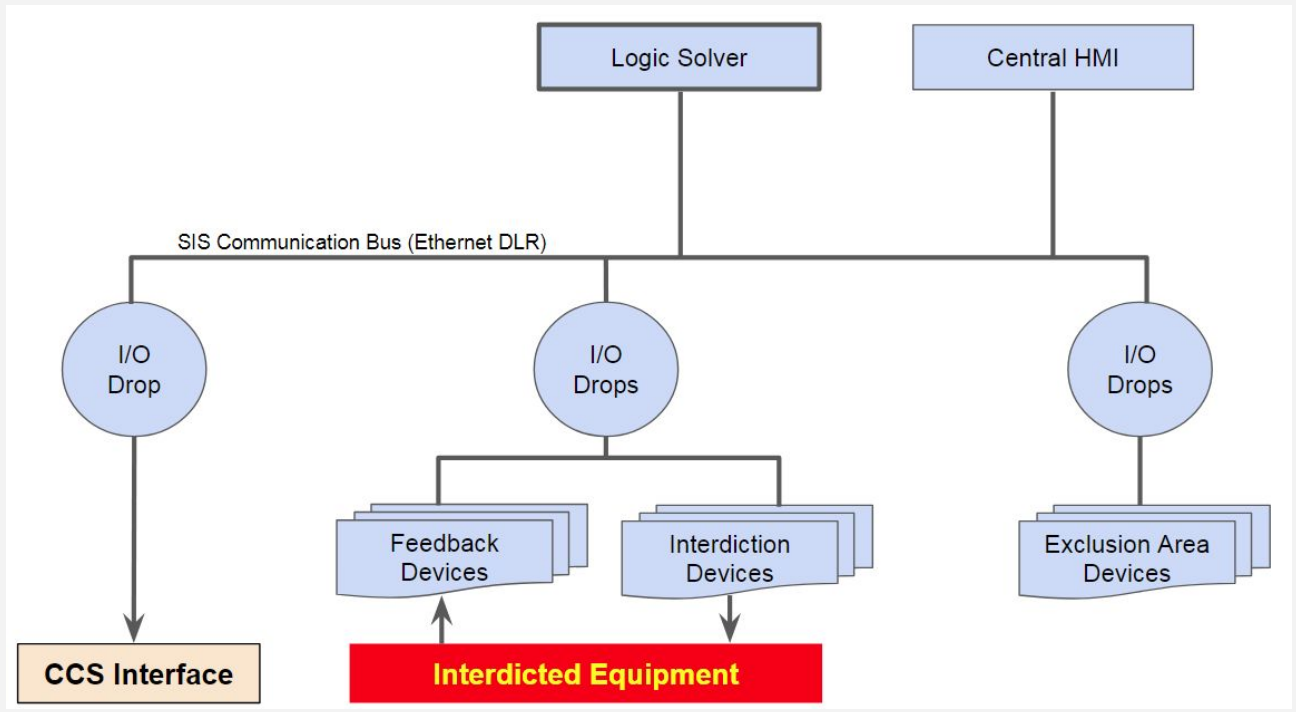

Figure 2.1-2 A diagram representing the architecture of the PSS-SIS.

2.2 Product Functions

The essential product functions are depicted in the fig. 2.2-1 below. The (core) safety application program inside the blue ellipse directly contributes to the safety functions; those outside provide functions and features that are essential to effectively operating and maintaining the SIS. Some of the software modules are shown in the diagram, the most critical is in red, the *Actions* module. This module has the logic to maintain a safe working environment through the interdiction of hazardous equipment.

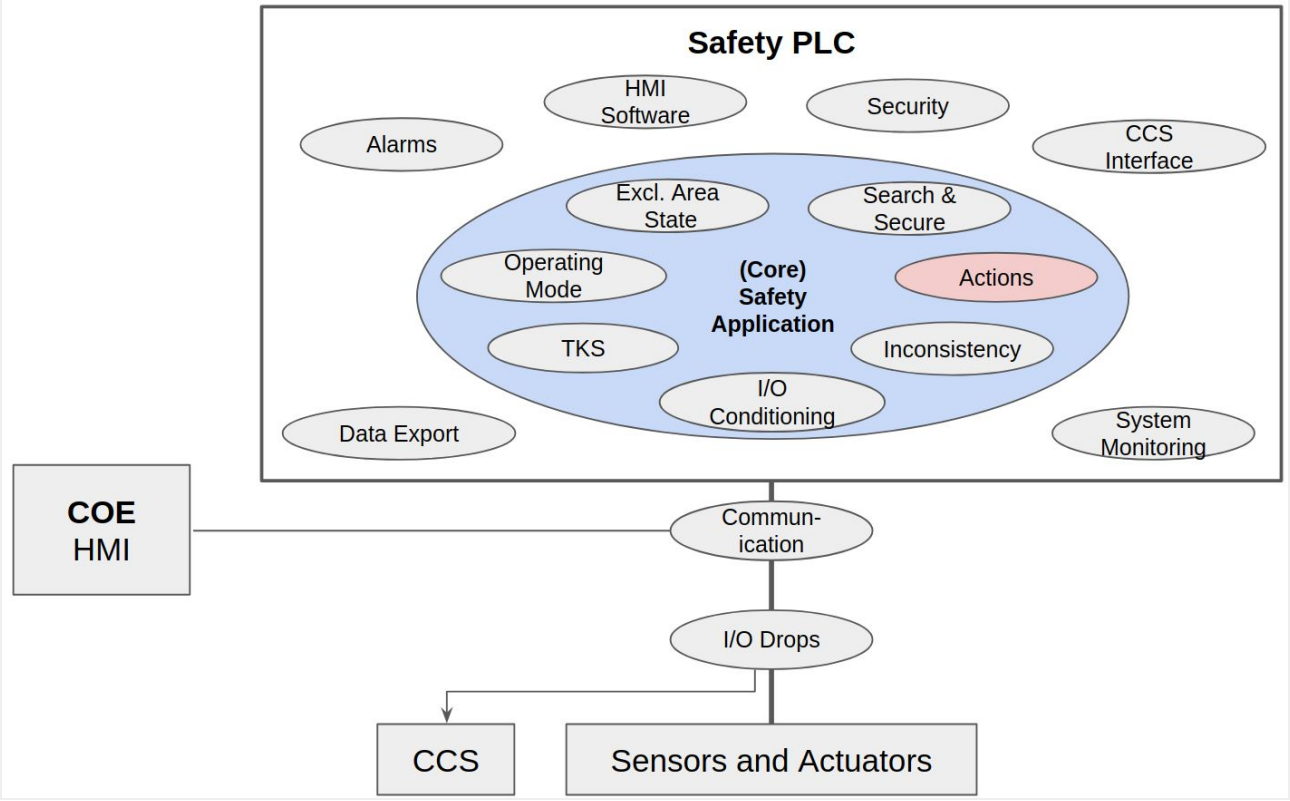

Figure 2.2-1 A diagram representing various software modules of the PSS-SIS. The items in the blue ellipse represent the core safety application - required software to fulfill the safety instrumented functions.

2.3 User Classes and Characteristics (Use Cases)

There will be a number of users of the SIS and its software. The actors and their use of the system are depicted in fig. 2.3-1. The PSS Engineering Team will be deeply involved in all aspects of the software. All actors will be involved in the testing, validation, and commissioning of the system and its software. The largest "customer base" is the Exclusion Area Occupants, so particular attention to providing them with a clearly understood and effective user interface is essential.

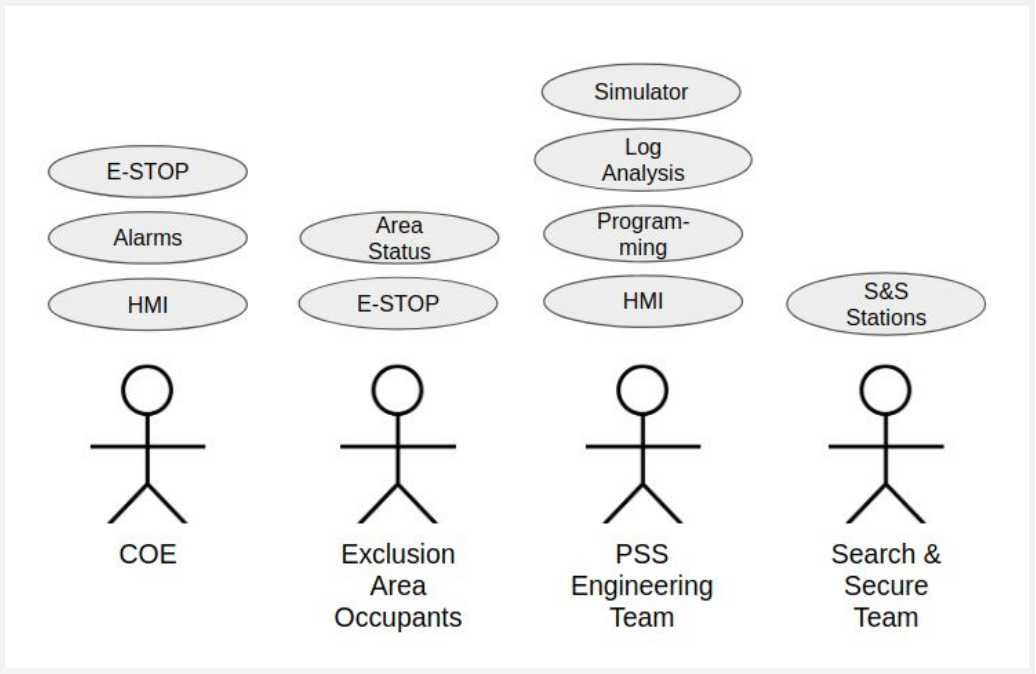

Figure 2.3-1 A diagram showing the PSS-SIS users types and which aspects of the system they interact with.

2.4 Operating Environment

The software will operate using a single logic solver that is designed for safety applications. The I/O modules will be distributed throughout the experimental complex. The communication mechanism between the logic solver to I/O modules (and their controllers if present) will incorporate design characteristics that provide fail-safe operation for the required safety instrumented functions as defined in reference [2]. The system will be air-gapped, meaning there shall be no off-network communication (wired, optical, or wireless).

2.5 Constraints

The design that is developed from this software specification must have certain attributes:

a) The software design and development plans must be in accordance with the PPPL's referenced documents.
b) The software development and execution environments must use COTS items that are appropriate for safety applications.
c) The configuration of the COTS software (tags, databases, behavior parameters, timeouts, LVL, etc…) will be performed in accordance with vendor's instructions and training.
d) There shall be no customization of the COTS software (infrastructure).
e) The COTS software for producing the SIS software will be installed on a computer running a (currently) supported version of the Microsoft "Windows" operating system.
f) If the PLC application includes both safety and non-safety functions, there shall be a logical and visible distinction between the standard and safety-related portions of the application.

g) Software subroutines and modules that contribute to providing Safety Instrumented Functions shall only use safety-qualified I/O, tags, and operations.

2.6 Assumptions

These are the assumptions that have guided the development of this software specification:

a) The higher level PSS requirements documents [2,4] are stable and have been approved.
b) The "performance" chapter in this document, in particular the preliminary timing analysis for interdiction, list several assumptions about the data processing and I/O. They are shown in that chapter so they can be seen into their proper context.
c) A single application program may be developed that provides both safety and non-safety functions.
d) The hardware design will use redundant field sensors, I/O modules, and data processing for fulfilling safety instrumented functions.
e) The digital output hardware will be fail-safe such that if the logic program stops or loses communication, the output points will automatically command the field equipment to its safe state.
f) The non-functional software requirements shall comply with PPPL (engineering) policies and procedures. These may reference non-PPPL documents including DOE and industry standards; the PSS-SIS requirements are not required to be in full compliance with these references.
g) There is no non-volatile data memory. When the logic program starts, all internal variables will consistently be in their initialized state.

2.7 User Documentation

As part of the COTS solution that is selected for the software design, it is required that it include software installation and configuration manuals, operating manuals, maintenance manuals, help and reference materials, and training/tutorials.

An SIS Software Design Description [5] will be written that describes the COTS products, the PPPL design approach, and documentation that were used to provide the performance, functionality, and features delineated in this document.

3. External Interface Specifications

3.1 User Interfaces

As shown on the "Users" diagram (fig.2.3-1) there are only a few types of user interfaces and these can be placed in two classes, 1) graphical HMI (computer screen), and 2) discrete devices such as lights, klaxons, buttons, keys, and switches. The HMI may be a touch screen device or use a mouse/touchpad. It provides complete oversight of the SIS. The chapter on the *Centralized HMI* will specify in detail the features of the user displays. The second class of user interface, discrete devices, are simple since each interface generally has one device presented to the user. The interface uses the SIS's distributed I/O, so the interface with the software is conventional.

3.2 Hardware Interfaces

All hardware interfaces are considered to be part of the configurable COTS product portfolio. No custom engineering is anticipated. Hardware interfaces for the software are only remote digital I/O modules (both safety and non-safety types). The types of devices that are interfaced with the SIS hardware digital input and output points are listed below. The manner in which each is used by the software can be found in the tables used to describe functions.

Types of Devices monitored by Digital Input Points

- Exclusion Area Door monitoring
- 13.8 kV Breaker position
- Ground switch position
- Emergency Stop buttons
- Light Curtains
- Intrusion detection devices
- Search and Secure buttons

Types Devices controlled by Digital Output Points

- Safety relays for 13.8 kV breaker interdiction
- Relays for door strike (lock) circuit
- Lamps, signage, and klaxon to convey area status information

3.3 Software Interfaces

All software interfaces are considered to be part of the configurable COTS product portfolio. No custom engineering is anticipated.

3.4 Communications Interfaces

All communication interfaces are considered to be part of the configurable COTS product portfolio. No custom engineering is anticipated. The SIS will be a private, air-gapped system; there shall be no networked communication (electrical, optical, or wireless) outside of the SIS.

That being said the communications component of the SIS, which is not part of the logic portion of software shall have these features:

- Support DLR networking, at least three rings.
- Have bandwidth and latency sufficient to support the needs described in the *Performance Requirements* chapter.
- Provide a configurable RPI for each module or I/O station.
- Provide an RPI period of 100ms or less.
- All communication faults shall be capable of being alarmed.
- A communication fault which stops the program execution shall be capable of automatic recovery (restart of logic processing).
- A communication fault with the CHMI shall be capable of automatic recovery (restart of updating display variables).

4. Software Modules

To provide clarity in understanding the mission that the SIS software must perform, it has been characterized by a series of modules. Each module has been decomposed into a number of functions of relative simplicity. In many instances the modules and functions exchange data and perform their respective functions sequentially to perform a particular higher-order function. The chapters below describe the modules, functions, and their interaction.

Each function has been named FUNC-xxxx-yy and is described using a table. The xxxx codes correspond to a module and are listed below. The yy is a number.

1) SACT: Safety Actions module
2) AACT: Additional Actions module
3) COND: I/O Conditioning module
4) MODE: Operating Mode module
5) ASTAT: Exclusion Area Status module
6) INC: Inconsistency module
7) TKS: TKS and CMS module
8) SS: Search and Secure module
9) CCS: CCS Interface module
10) CHMI: Centralized HMI module
11) ALM: Alarm module
12) SYSM: System Monitoring module
13) SIM: Simulation module (for testing)
14) TEST: Functions to support testing

4.1 Actions Module

The Actions module provides the safety instrumented functions that lie at the core of the PSS-SIS mission, as well as some additional actions as specified in [2,4]. These actions are the culmination of a number of other SIS functions; the first-level is illustrated in figure 4.1-1.

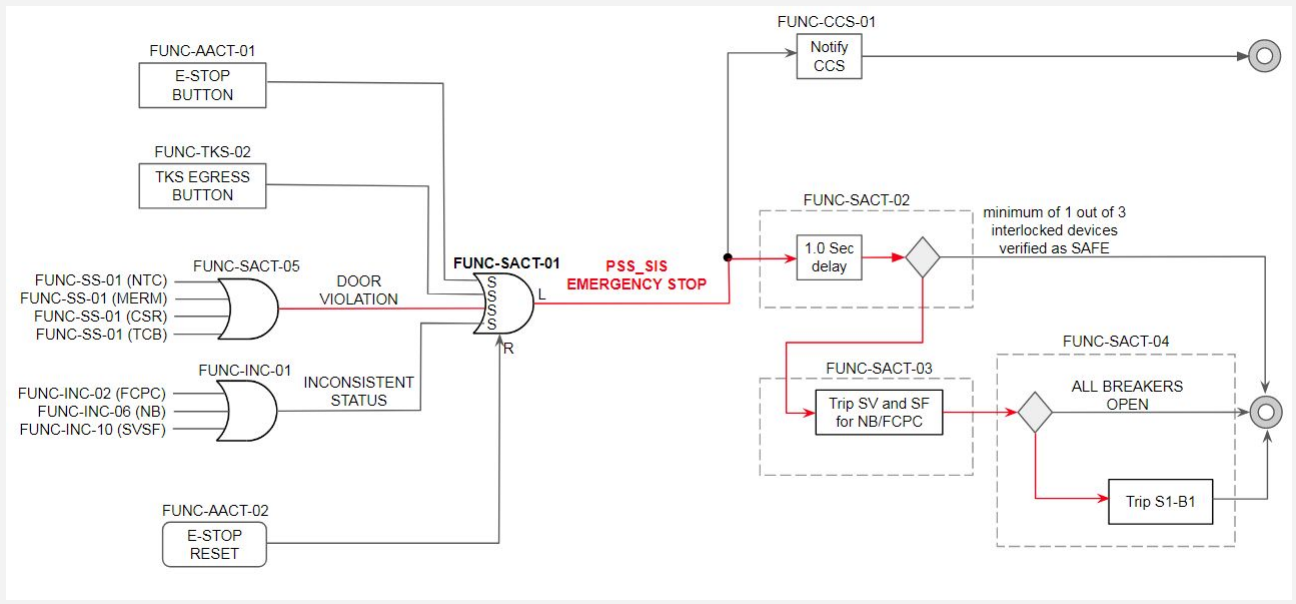

Figure 4.1-1 Diagram showing the functions that are used to fulfill the SIS safety instrumented functions. The letters at the logical OR gate representing FUNC-SACT-01 mean: S=set, R=reset, L=latched output.

4.1.1 Safety Actions

This section will describe the safety actions. Diagrams will be attached to this specification and will be used to illustrate how the various functions are used together to fulfill a safety action. These functions may also be used by the "additional actions", which are described in the next chapter.

Safety Action logic associated with Safety Instrumented Functions must be produced only with safety tags and safety logic instructions. A safety action should not be dependent or inhibited by a non-safety rated device or software instruction.

Table 4.1.1-1 PSS-SIS Emergency Stop

FUNCTION ID	FUNC-SACT-01
Title	PSS-SIS Emergency Stop Condition
Description	Per Table 3.3-2 in reference [2], declare and latch a PSS-SIS Emergency Stop condition, which will initiate the Interdiction action.
Dependency	● FUNC-AACT-01 (E-Stop buttons) ● FUNC-TKS-02 (TKS Egress buttons) ● FUNC-SACT-05 (door violation) ● FUNC-INC-01 (inconsistent status) ● FUNC-AACT-02 (E-Stop Reset)
Result	A *process variable* for a PSS-SIS Emergency Stop Condition will be set. This variable is latched and will require field device reset and operator intervention to reset the condition (FUNC-AACT-02).

Table 4.1.1-2 Delay/Check to Allow CCS/BCS Action

FUNCTION ID	FUNC-SACT-02
Title	Delay for CCS/BCS, then check for safe condition
Description	This action will initialize when a PSS-SIS Emergency Stop (shutdown) condition has been received by the core logic. It's purpose is to first allow the CCS/BCS to remove any unsafe condition. ● A 1.0 delay action is required so that CCS/BCS has time to execute its functions for safety. ● If CCS/BCS successfully renders at a minimum one logical element of each Interdicted Device within the allotted 1.0 seconds, then no further action is required by the SIS.
Dependency	● FUNC-SACT-01 (PSS-SIS Emergency Stop) ● FUNC-AACT-04 (area safe)
Result	Conditional, either interdict all SV and SF breakers (FUNC-SACT-02), or take no action if CCS/BCS has rendered the areas safe per FUNC-ASTAT-09.

Table 4.1.1-3 Trip SVSF Breakers

FUNCTION ID	FUNC-SACT-03
Title	Trip SV-SF Breakers
Description	Trip SV and SF Breakers for NB and FCPC
Dependency	FUNC-SACT-02 (Allow CCS/BCS attempt)
Result	Trip all applicable breakers.

Table 4.1.1-4 Trip S1-B1 Breaker

FUNCTION ID	FUNC-SACT-04
Title	Trip S1-B1 Breaker
Description	Trip the S1-B1 breaker if all of the "downstream" SV and SF breakers for NB and FCPC are not open (safe).
Dependency	● "downstream" SV and SF breaker positions for NB and FCPC ● FUNC-SACT-03 completion
Result	Conditionally, trip the S1-B1 breaker.

Table 4.1.1-5 Aggregate Door Violation

FUNCTION ID	FUNC-SACT-05
Title	Aggregate Door Violation
Description	Summation of door violations for all securable areas.
Dependency	• FUNC-SS-01 area door violation(s).
Result	A door violation is declared.

4.1.2 Additional Actions

These are additional safety-relevant actions performed by the SIS. These are not considered a *Safety Instrumented Function*.

Table 4.1.2-1 SIS Emergency-Stop Buttons

FUNCTION ID	FUNC-AACT-01
Title	SIS Emergency-Stop
Description	An SIS E-STOP button has been pushed.
Dependency	All SIS E-STOP buttons (loop 11)
Result	An Emergency Stop condition is declared (via FUNC-SACT-01)

Table 4.1.2-2 RESET PSS-SIS Emergency Stop

FUNCTION ID	FUNC-AACT-02
Title	RESET PSS-SIS Emergency Stop Condition
Description	Once declared, resetting the PSS-SIS EMERGENCY STOP condition shall be achieved through the COE coordinating the resetting the field device(s) as well as the execution of dedicated E-STOP restoration procedures. All areas must be in the ACCESS state which requires that the areas are safe.
Dependency	• FUNC-SACT-01 (Emergency Stop contributing factors have been cleared) • FUNC-ASTAT-03 (in ACCESS mode) • FUNC-HMI-02 (COE reset of E-Stop)
Result	The *process variable* for a PSS-SIS Emergency Stop Condition will be reset. Breakers will be permitted to operate after FUNC-AACT-04 (release UV Trip) completes.

Table 4.1.2-3 Release UV Trip

FUNCTION ID	FUNC-AACT-03

Title	Release UV Trip (circuit)
Description	FUNC-SACT-03 will have de-energized a safety relay in each breaker's UV Trip circuit. After the E-Stop has been cleared, the safety relay may be re-energized. To avoid an in-rush of current on the SIS control power supply, the relays should be re-energized in a staggered manner.
Dependency	FUNC-SACT-03 (SV & SF Trip)
Result	The UV Trip circuit is released, so SIS is no longer prohibiting operation of the breakers.

Table 4.2.1-4 Area Safe

FUNCTION ID	FUNC-AACT-04
Title	Area safe
Description	An area is safe for occupancy if, at a minimum, a single logical element of each PSS-SIS monitored device is in a safe mode, AND, the TKS interlocked key for the area is in the unlocked position. Each exclusion area will need to check for particular hazards. Appendix A shows, for each exclusion area, the device feedback that will contribute to the safe condition.
Dependency	The device conditions are listed in Appendix A.
Result	The Area safe/unsafe status for each exclusion area is declared.

4.2 I/O Conditioning Module

Input and output signals are sometimes required to debounce or minimize signal chatter; this may be performed by the hardware (if supported by the digital input module) or by the logic software. The signal conditioning can filter spurious noise that could potentially falsely trigger the logic, or on the output end, to potentially protect external equipment by suppressing rapid, repeated actuation.

Figure 4.2-1 shows the raw and conditioned signals. The signal conditioning will have the option to be applied to digital input points that monitor devices such as door position sensors, breaker position, or SIS intrusion detectors. The signal conditioning will have the option to be applied to digital output points, as desired, for devices that control devices such as klaxons or door strike circuitry. Any I/O conditioning shall not impede the operation of Safety Instrumented Functions or Additional Actions.

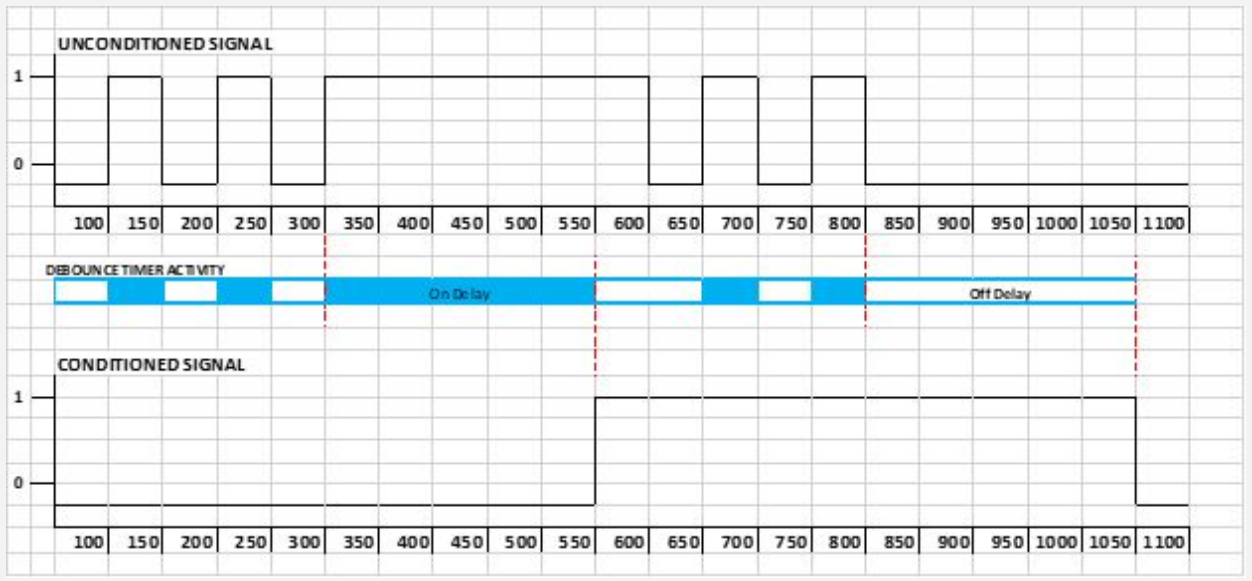

Fig 4.2-1 A diagram that shows the unconditioned and conditioned signal. The 'debounce' timer's active state is indicated in blue. For illustration purposes time increments of 50 ms are used.

Figure 4.2-2 below shows the data flow for a signal from an external incoming input point, as well as conditioning for an output signal. Each external input signal will have the option to be conditioned then sent to the core logic for processing. In contrast any output logic from the core will have the option to be conditioned before it is sent to an external output point.

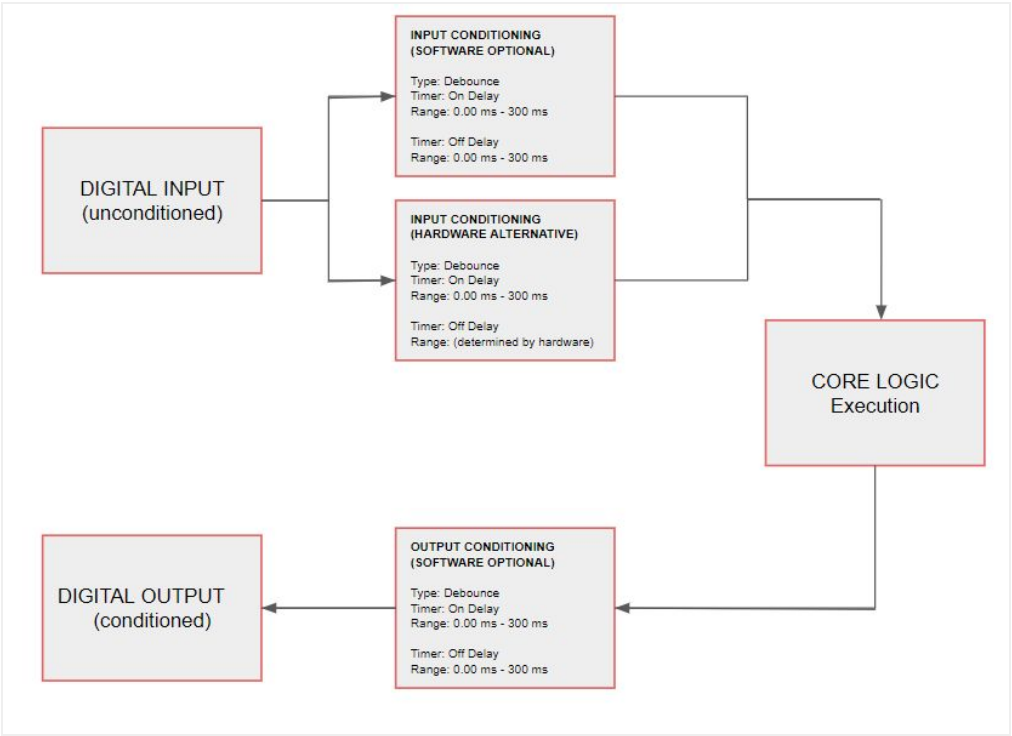

Figure 4.2-2 : A Diagram that shows optional software signal conditioning as well an alternative hardware solution.

The raw signals may be manipulated to prepare the signal for further processing by adjusting an "On delay" and an "Off delay" of the **conditioned signal** up to 300 mS in 10 mS increments. *Note that the 10 ms resolution may not be achievable because the PLC's logic scan rate may be longer; this is understood as an inherent and possibly unavoidable constraint. A hardware alternative is acceptable as well, if it is able to meet the system's delay and safety requirements.*

Signals connected to the Logic Solver's remote I/O modules are sometimes governed by a separate processor which is used to periodically update the status of I/O (e.g RPI) by sending/receiving data to/from the main PLC controller. The behaviour of the inputs and outputs with regards to this additional module scan time, should be taken into consideration in the system timing analysis.

Table 4.2-1 Input Signal Conditioning

FUNCTION ID	FUNC-COND-01
Title	Input Signal Conditioning
Description	This function will logically debounce any incoming signals. This function will take unconditioned raw input signals (see e.g. Fig 4.2-2) and condition them so that they can be used by the core program. This function will provide a user-configurable 0 - 300 mS range with 10 mS resolution. This function can be internally enabled or disabled from within the software. This option will be available for all raw input (bit) signals.
Dependency	Raw input signal (bit)
Result	Conditioned digital input signals are used by program logic

Table 4.2-2 Output Signal Conditioning

FUNCTION ID	FUNC-COND-02
Title	Output Signal Conditioning
Description	This function will logically debounce any outgoing signals from the core logic. This function will take unconditioned signals (see e.g. Fig 4.1-1) and condition them so that they can be sent to field devices. This function will provide a user-configurable 0 - 300 mS range with 10 mS resolution. This function can be internally enabled or disabled from within the software. This option will be available on all signals connected to raw outputs. The result will yield signals free of erroneous state transitions.
Dependency	Internal program signal (Core Logic Internal Output)
Result	Conditioned program output logic is used by digital outputs

4.3 Operating Mode Module

The SIS Software will have two operational modes as shown in figure 4.2-1 below:

- Normal Mode
- Interdict Mode

Due to a hardware failure or software malfunction the system failure (state) could be realized, and is shown to illustrate that it is not considered an operational mode. Due to the fail-safe design of the PSS-SIS (system), all interlocked equipment will be interdicted during a system failure.

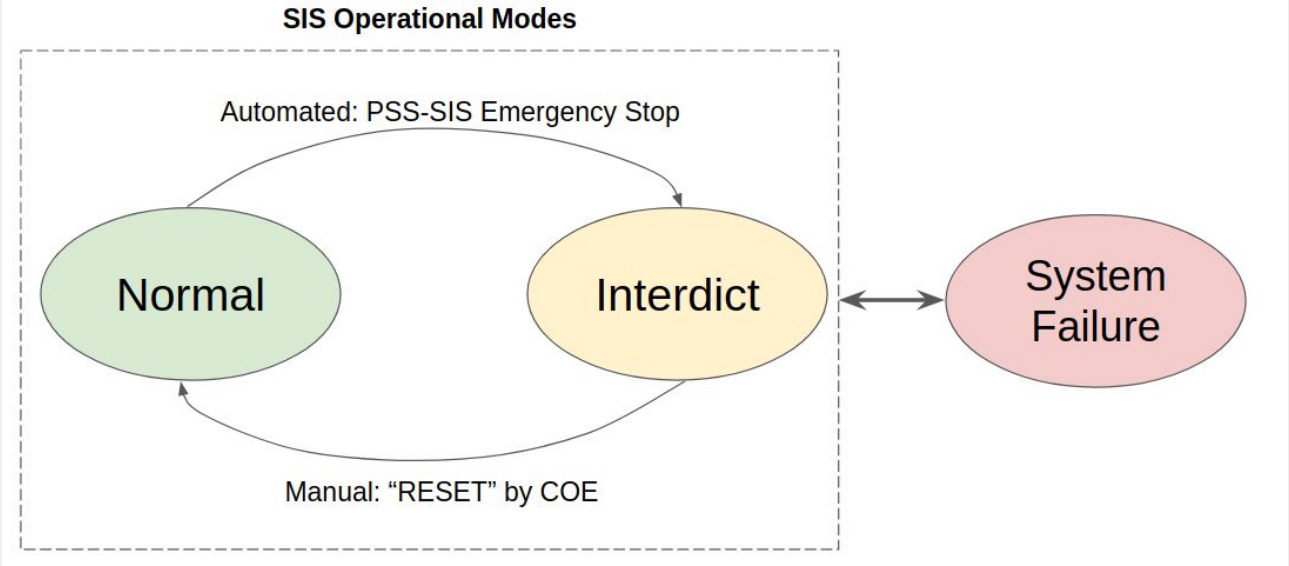

Figure 4.3-1 A diagram depicting the operating modes of the SIS.

Table 4.3-1 Normal Mode

FUNCTION ID	FUNC-MODE-01
Title	Normal Mode
Description	● In the Normal Mode the SIS components are operating normally and the SIS is actively providing all of its required safety functions. ● When the PSS-SIS system is started it will begin operating in the Normal mode.
Dependency	Once entered, the normal mode will be maintained until any of the situations listed below occur: ● FUNC-SACT-01 (Emergency Stop)
Result	Transition to FUNC-MODE-02 (Interdict Mode)

Table 4.3-2 Interdict Mode

FUNCTION ID	FUNC-MODE-02
Title	Interdict Mode
Description	● In the Interdict mode, the SIS is fully operational. ● In the Interdict mode the SIS will interdict all of the energy sources that may contribute to an SIS-protected hazard. ● The Interdict mode will be maintained until the Emergency Stop has been RESET.
Dependency	● FUNC-AACT-02 (RESET E-Stop)
Result	Transition to FUNC-MODE-01 (Normal Mode)

4.4 Exclusion Areas State Module

The access state is one prerequisite of any SIS action that is applied to the interlocked devices. The access state module provides the following three access states (per reference [4]) for the exclusion areas defined in reference [2]. The access states and transitions are depicted in figure 4.4-1. There shall be one and only one state configured per exclusion area at any given time. Separate exclusion areas may concurrently be in different access states.

1. ACCESS state
2. NO ACCESS state
3. LOCKDOWN state

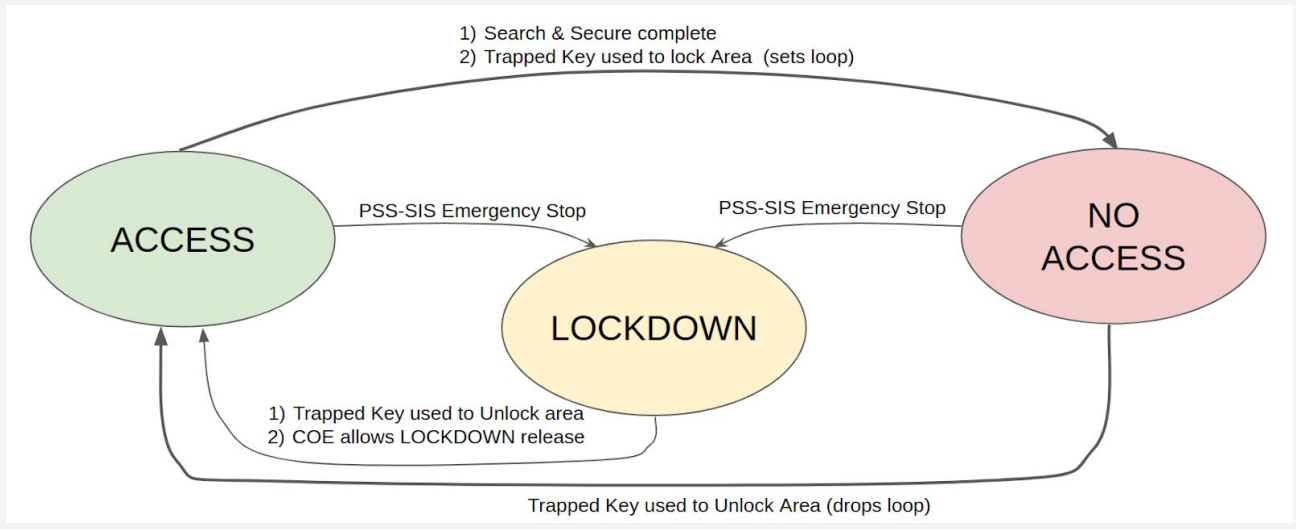

Fig 4.4-1 A diagram showing the valid Area States and transitions.

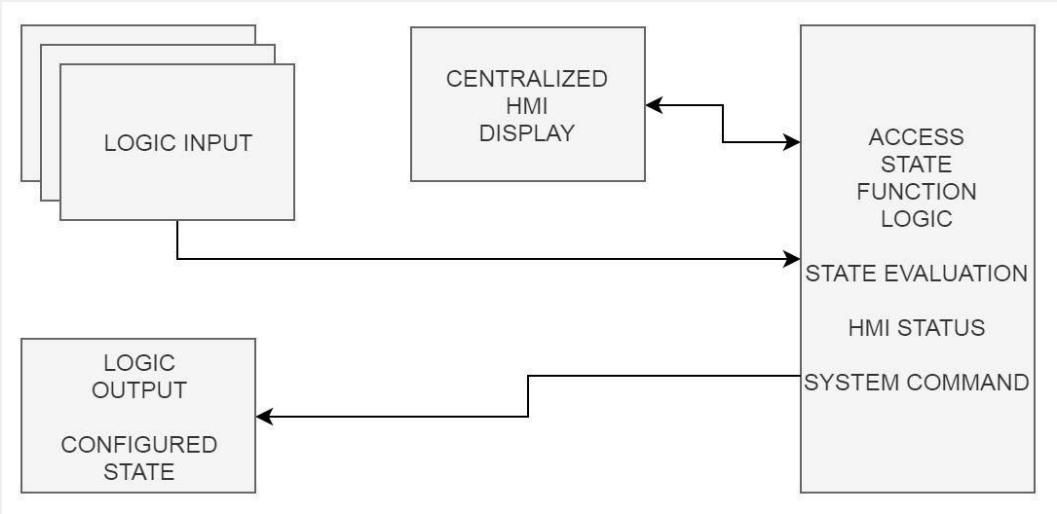

Fig 4.4-2 A diagram to show the data flow for the Area State software.

The ACCESS state in itself does not inhibit the ACAMS card reader access to the exclusion areas, but the SIS operator (COE) has the capability to use the SIS to disable the card reader, at-will. . Note that the ACAMS card reader may also be inhibited by other (not SIS) systems. From the safety perspective it is assumed personnel are in the exclusion area. The NO ACCESS state prohibits ACAMS card reader access to the exclusion areas. In NO ACCESS, no personnel are permitted within the exclusion area. The LOCKDOWN state also inhibits ACAMS card readers to prevent access to the exclusion areas (so equipped). In LOCKDOWN, personnel will be prevented from entering the area, but people may already be in the exclusion area if it was in the ACCESS state or the area access was violated.

To fulfill the exclusion areas access requirements, the state logic uses logic inputs from other sections of this specification, and provides logic outputs for use by other modules in the core software.

4.4.1 Functional Description

The functions that support access state will be described below.

Table 4.4.1-1 Exclusion Area Status

FUNCTION ID	FUNC-ASTAT-01
Title	Exclusion Area Status
Description	There are three valid states for an exclusion area, as defined in [2]; one and only one state may be active for a specific exclusion area. ● LOCKDOWN ● ACCESS ● NO ACCESS If none, or multiple states remain active, the error condition will be declared and

	a critical alarm will be raised. Note that FCPC and NB safe to enable signals require the NO ACCESS state.
Dependency	● FUNC-ASTAT-02 (LOCKDOWN state) ● FUNC-ASTAT-03 (ACCESS state) ● FUNC-ASTAT-04 (NO ACCESS state)
Result	Set a process variable that indicates the current state of the area (ACCESS, NO ACCESS, LOCKDOWN).

Table 4.4.1-2 LOCKDOWN State

FUNCTION ID	FUNC-ASTAT-02
Title	Lockdown State
Description	This state is initiated upon a PSS-SIS Emergency Stop condition. Note: It is possible personnel are within the exclusion area during LOCKDOWN. All areas enter lockdown together, but are released independently.
Dependency	To enter: ● FUNC-SACT-01 (PSS-SIS Emergency Stop condition transition to active) To exit: ● FUNC-AACT-04 (Area is safe for entry). ● FUNC-HMI-02 (COE commands lockdown release for the specific area.) ● Note that the Emergency Stop condition may (still) be active while exiting LOCKDOWN.
Result	Set a process variable that indicates the access state of the area.

Table 4.4.1-3 ACCESS State

FUNCTION ID	FUNC-ASTAT-03
Title	Access State
Description	This function will assert the ACCESS state. The access state shall allow personnel access to the exclusion area provided the ACAMS card reader authorizes them. In the ACCESS state it is assumed that personnel may be in the exclusion area. During the search and secure, the area will be in the ACCESS state.
Dependency	● FUNC-TKS-01 (Area key in the unlocked position) ● FUNC-AACT-04 (Area is safe for occupancy).
Result	Set a process variable that indicates the access state of the area.

Table 4.4.1-4 NO ACCESS State

FUNCTION ID	FUNC-ASTAT-04
Title	No Access State
Description	In NO ACCESS state, no personnel are permitted within the exclusion area. The Search & Secure process has been successfully completed and all doors have been closed and locked. ● The conditions and sensors to enter and remain in the NO ACCESS state are described in [2].
Dependency	To enter: ● FUNC-SS-02 (Loop-set) To exit: ● FUNC-SACT-01 (PSS-SIS Emergency Stop Condition Active), or ● FUNC-TKS-01 (Trapped Key used to unlock area)
Result	Set a process variable that indicates the access state of the area.

Table 4.4.1-5 ACAMS Card Reader Interdiction

FUNCTION ID	FUNC-ASTAT-05
Title	ACAMS Card Reader Inhibit
Description	The ACAMS card reader is enabled for personnel card access for applicable areas when the area is in the ACCESS state. Exception: The search and secure is performed in the ACCESS state, but the card reader is disabled once the first S&S station has been reached. The operator shall have independent disable-control of each card reader.
Dependency	● FUNC-ASTAT-03 (when ACCESS state is not active) ● FUNC-SS-03 (detect commencement of the S&S). ● FUNC-HMI-02 (COE commands card reader disabled)
Result	The ACAMS card reader (door strike circuit) is interdicted.

Table 4.4.1-6 Area Status lights

FUNCTION ID	FUNC-ASTAT-06
Title	Area status lights
Description	A single, multi-color light will visually indicate an area's condition. Each exclusion area may have multiple instances of the lights.
Dependency	● FUNC-ASTAT-01 (Area status) ● FUNC-AACT-04 (Area Safe) ● FUNC-SS-03 (S&S status)

<table>
<tr><td>Result</td><td>Set the color of the light, based upon the area conditions:

<table>
<tr><th>Area Safe *</th><th>NO ACCESS or LOCKDOWN state</th><th>ACCESS state</th><th>S&S is Active</th><th>Light Color</th></tr>
<tr><td>0</td><td>x</td><td>x</td><td>x</td><td>Red (Unsafe)</td></tr>
<tr><td>1</td><td>0</td><td>1</td><td>0</td><td>Green (Safe)</td></tr>
<tr><td>1</td><td>0</td><td>1</td><td>1</td><td>Yellow (S&S)</td></tr>
<tr><td>1</td><td>1</td><td>0</td><td>x</td><td>Red</td></tr>
</table>
* at a minimum, a single logical element of each PSS-SIS monitored device is in a safe mode. This applies to the hazards in each specific area.</td></tr>
</table>

Table 4.4.1-7 Area Status Audible Alerts

<table>
<tr><td>FUNCTION ID</td><td>FUNC-ASTAT-07</td></tr>
<tr><td>Title</td><td>Area Status Audible Alerts</td></tr>
<tr><td>Description</td><td>

Operate a klaxon-type device to warn occupants of an unsafe or a pending change to an area’s condition.
The sound emitted by the ~20 klaxons in the NTC must be intelligible and not startling to its occupants. So, the tone patterns described here may require post-installation modifications.

<table>
<tr><th>Area Condition</th><th>Audible Behavior</th></tr>
<tr><td>ACCESS</td><td>no sound</td></tr>
<tr><td>NO ACCESS</td><td>~300 seconds of alternating sound upon entering the state. This will happen at the completion of the S&S.</td></tr>
<tr><td>LOCKDOWN</td><td>● After a 10 second delay, ~5 seconds of continuous sound after entering LOCKDOWN. The delay will allow for immediate vocal instruction or warnings, and to allow unobfuscated recording of sounds surrounding the E-Stop event.
● A “reminder chirp” shall sound for 5 seconds every 60 seconds while in LOCKDOWN</td></tr>
<tr><td>Search and Secure: starting now</td><td>A three pulse 500ms pulse duration sound repeating every 30 seconds for 180 seconds that is started when the S&S process has been initiated at the</td></tr>
</table>
</td></tr>
</table>

	<table><tr><td></td><td>master station.</td></tr><tr><td>Search and Secure: *error*</td><td>A chirp will sound if the S&S did not follow the prescribed sequence.</td></tr></table>
Dependency	● FUNC-ASTAT-01 (Area status) ● FUNC-SS-03 (S&S status)
Result	Sound the klaxon for a specific are as described above.

4.5 Inconsistency Module

One of the reasons for the SIS to declare a PSS-SIS Emergency Stop is when particular "Inconsistent Status" is detected as described in [2,4]. Functions that support inconsistent status will be shown in the following sections, but it is essentially an inconsistency between the allowed state and the present state of Interlocked equipment. Since the logic for this status can include complex conditionals there are separate functions described for each type of inconsistency. All inconsistencies will be alarmed and logged.

Table 4.5-1 Aggregate Unsafe Inconsistency

FUNCTION ID	FUNC-INC-01
Title	Aggregate Inconsistent Status Condition introducing an unsafe condition.
Description	This is a summation of the lower-level inconsistent status functions.
Dependency	● FUNC-INC-02 (FCPC) ● FUNC-INC-06 (NB) ● FUNC-INC-10 (SV & SF Breakers)
Result	Declare the inconsistency in a process variable. This function will be used by FUNC-SACT-01 to declare an Emergency Stop.

4.5.1 FCPC Inconsistencies

The inconsistent states for the FCPC equipment is described in the tables below.

Table 4.5.1-1 FCPC Inconsistent Status

FUNCTION ID	FUNC-INC-02
Title	FCPC Inconsistent Status
Description	This is a summation of the lower-level inconsistent status functions for FCPC.

Dependency	● FUNC-INC-03 (LS-BKR) ● FUNC-INC-04 (GS-LS/BKR) ● FUNC-INC-05 (FCPC DUMMY LOAD)
Result	Declare the inconsistency in a process variable.

Table 4.5.1-2 FCPC Line Switch Inconsistent Status

FUNCTION ID	FUNC-INC-03
Title	FCPC Line Switch Inconsistent Status
Description	During ACCESS, any FCPC line switch is closed if its corresponding breaker(s) is closed, ● Exception: If the PCTS guard is configured for FCPC dummy load and no coil links within the PCTS are installed.
Dependency	● SDS Line Switch positions ● Associated 13.8 kV Breaker Positions ● FUNC-ASTAT-01 (NTC in ACCESS) ● FUNC-ASTAT-01 (CSR in NO ACCESS) ● FUNC-ASTAT-01 (TCB in NO ACCESS) ● FUNC-INC-05 (Dummy Load)
Result	Declare the inconsistency in a process variable.

Table 4.5.1-3 FCPC Ground Switch Inconsistent Status

FUNCTION ID	FUNC-INC-04
Title	FCPC Ground Switch Inconsistent Status
Description	During NTC ACCESS, any FCPC ground switch open if the corresponding line switches or breakers are closed ● Exception: If the PCTS guard is configured for FCPC dummy load and no coil links within the PCTS are installed.
Dependency	● SDS Ground Switch positions ● Associated SDS Line Switch positions ● Associated 13.8 kV Breaker Positions ● FUNC-ASTAT-03 (NTC in ACCESS) ● FUNC-ASTAT-03 (CSR in NO ACCESS) ● FUNC-ASTAT-03 (TCB in NO ACCESS) ● FUNC-INC-05 (Dummy Load)
Result	Declare the inconsistency in a process variable.

Table 4.5.1-4 FCPC Dummy Load Inconsistent Status

FUNCTION ID	FUNC-INC-05
Title	FCPC Dummy Load Inconsistent Status
Description	The PCTS is configured for FCPC Dummy Load, but sensors indicate that coil bus bars are installed.
Dependency	● FUNC-TKS-01 (FCPC dummy load key at PCTS key-block is removed) ● Coil bus bars within PCTS are present, per light curtain.
Result	Declare the inconsistency in a process variable.

4.5.2 NB Inconsistencies

The inconsistent states for the NB subsystems are described in the tables below.

Table 4.5.2-1 NB Inconsistent Status

FUNCTION ID	FUNC-INC-06
Title	NB Inconsistent Status
Description	This is a summation of the lower-level inconsistent status functions for FCPC.
Dependency	● FUNC-INC-07 (NB1) ● FUNC-INC-08 (NB2) ● FUNC-INC-09 (NB DUMMY LOAD)
Result	Declare the inconsistency in a process variable.

Table 4.5.2-2 NB1 Inconsistent Status

FUNCTION ID	FUNC-INC-07
Title	NB1 Inconsistency
Description	● During ACCESS, any NB1 source's Ross ground switch is not closed AND its associated Pringle ground switch is not closed. AND ● ESF2-SB05 is closed AND ● ESF1-SB10 OR ESV2-SB10 is closed
Dependency	● 13.8 kV breaker positions ● NB Ross ground switch positions ● NB Pringle ground switch positions ● FUNC-ASTAT-03 (ACCESS state for NTC)

Result	Declare the inconsistency in a process variable. Raise alarm.

Table 4.5.2-3 NB2 Inconsistent Status

FUNCTION ID	FUNC-INC-08
Title	NB2 Inconsistency
Description	● During ACCESS, any NB2 source's Ross ground switch open AND its associated Pringle ground switch is open. AND ● ESF2-SB05 is closed AND ● ESF1-SB10 OR ESV2-SB11 is closed
Dependency	● 13.8 kV breaker positions ● NB Ross ground switch positions ● NB Pringle ground switch positions ● FUNC-ASTAT-01 (ACCESS state for NTC)
Result	Declare the inconsistency in a process variable.

Table 4.5.2-4 NB Dummy Load Inconsistent Status

FUNCTION ID	FUNC-INC-09
Title	NB Dummy Load Inconsistent Status
Description	ESF2-SB05 trapped key position is inconsistent with the breaker position when the breaker is closed
Dependency	● NB Dummy Load key position (at ESF2-SB05) ● ESF2-SB05 Breaker position
Result	Declare the inconsistency in a process variable.

4.5.3 SV and SF Breakers Inconsistencies

The inconsistent states for the SV and SF 13.8 kV breakers are described in the tables below.

Table 4.5.3-1 SVSF Breaker Inconsistent Status

FUNCTION ID	FUNC-INC-10
Title	Aggregate Breakers Inconsistent Status
Description	A summation of all breaker inconsistencies
Dependency	● FUNC-INC-11 (breaker position), for each breaker

	• FUNC-INC-12, (relay feedback)for each breaker
Result	Declare the inconsistency in a process variable.

Table 4.5.3-2 Breaker Position Inconsistent Status

FUNCTION ID	FUNC-INC-11
Title	Single Breaker Inconsistency, for SF or SV bus
Description	The SIS is commanding an interdiction to open the breaker but it is indicating closed.
Dependency	• The commanded state of a breaker (a process variable). • The monitored state of the breaker (a device).
Result	Declare the inconsistency in a process variable.

Table 4.5.3-3 Breaker Interdiction Relay Inconsistent Status

FUNCTION ID	FUNC-INC-12
Title	Breaker Interdiction Relay Feedback Inconsistency
Description	The SIS commanded state of an interdiction relay does not match the relay's feedback.
Dependency	• The commanded state of a breaker (a process variable). • The interdiction relay's position feedback (a device)
Result	Declare the inconsistency in a process variable.

4.6 TKS Module

The PSS-SIS will monitor trapped key positions from those locations specified in [4], and monitor the state of TKS emergency egress punch-out buttons as specified in [4]. The Trapped Key System (TKS) Module will be composed of a number of functions as described below. The trapped key signals will be used by other software modules.

Table 4.6-1 Trapped Key Monitoring

FUNCTION ID	FUNC-TKS-01
Title	Trapped Key Monitoring
Description	The trapped keys that are connected to the SIS and their use is described in reference [4].

	Monitor the position of each trapped key that is monitored by the SIS. The logic that is influenced by the key, will be described in the appropriate software module: (e.g. FCPC Dummy Load Configuration FUNC-CCS-02)
Dependency	Operator physically inserts/removes the key and turns the key. Monitor the position of each trapped key that is monitored by the SIS. The logic that is influenced by the key, will be described in the appropriate software module: (e.g. FCPC Dummy Load Configuration FUNC-CCS-02)
Result	Post the position of the keys in process variables, which are then used by other software functions.

Table 4.6-2 Emergency egress punch-out button

FUNCTION ID	FUNC-TKS-02
Title	Emergency egress punch-out button
Description	All vestibule emergency egress punch-out buttons, per [4], will be monitored.
Dependency	Personnel presses button and status is received by PSS-SIS PLC. Once actuated for egress, the button's mechanism must be (e.g. pulled/twisted) reset.
Result	Post the status of the buttons in process variables, which are then used by other software functions. Activate an alarm.

4.7 Search and Secure Module

Search and Secure (S&S) is a multi-person activity used to establish that no personnel are within an exclusion area. Reviewing figure 4.4-1, the, S&S is required to transition to an exclusion area's NO ACCESS state, which is a prerequisite for NSTX-U operations. The general S&S requirements are shown in [4]. This chapter will further describe the S&S activity and describe a number of functional elements that can be configured to produce software that supports the S&S.

For some complex spaces, engineered controls are used to enforce a prescribed search-path. Once the search has been successfully completed and the area has been locked (secured), the area is considered free of personnel and furthermore, a secure and monitored perimeter has been established (loop-set condition). For some exclusion areas the loop-set is configured using (just) a trapped key. Before hazardous equipment is permitted to become energized, "loop-set" conditions must exist in all areas where that equipment's operation could pose a hazard.

The general S&S progression is shown here, from the software perspective:

Search and Secure for Complex Spaces

- The S&S team tours the area and warns everyone to leave.
- While the area is in the ACCESS state, and all doors to the area are closed, then the area is READY to commence a S&S.
- An S&S team member turns the key switch at the master S&S station to the S&S position.
- Use Klaxon (via FUNC-ASTAT-07) to warn personnel of pending S&S.
- After the S&S warning time, set the area status lights change to yellow (via FUNC-ASTAT-06), indicating a S&S is in-progress.
- Within 30 seconds the search team enters the area and then the ACAMS card reader, if present, is disabled (FUNC-ASTAT-05).
- All doors to the area must be closed and remain closed throughout the S&S.
- The search team may now use the pushbutton at the first S&S station.
- Within an allotted(configurable) time, see that the first S&S station “S&S” button has been pressed.
- Within an allotted time, observe the next S&S station button is pressed.
- Continue through all stations following the prescribed path.
- The final S&S station will allow the main door to open (within a time period). The search team exits the area through the main door.
- If present, close the area’s inner door; sometimes this is a radiation shield door
- Turn and remove the S&S key from the master station and use the key to lock the area’s outermost door. This action sets the loop for the area.
- Completion: The loop has been set and the area has transitioned to NO ACCESS.
- Any deviation from the prescribed sequence will terminate the S&S and require it to start over. The area status lights will revert to green. The klaxon will chirp to alert the operators of an error.

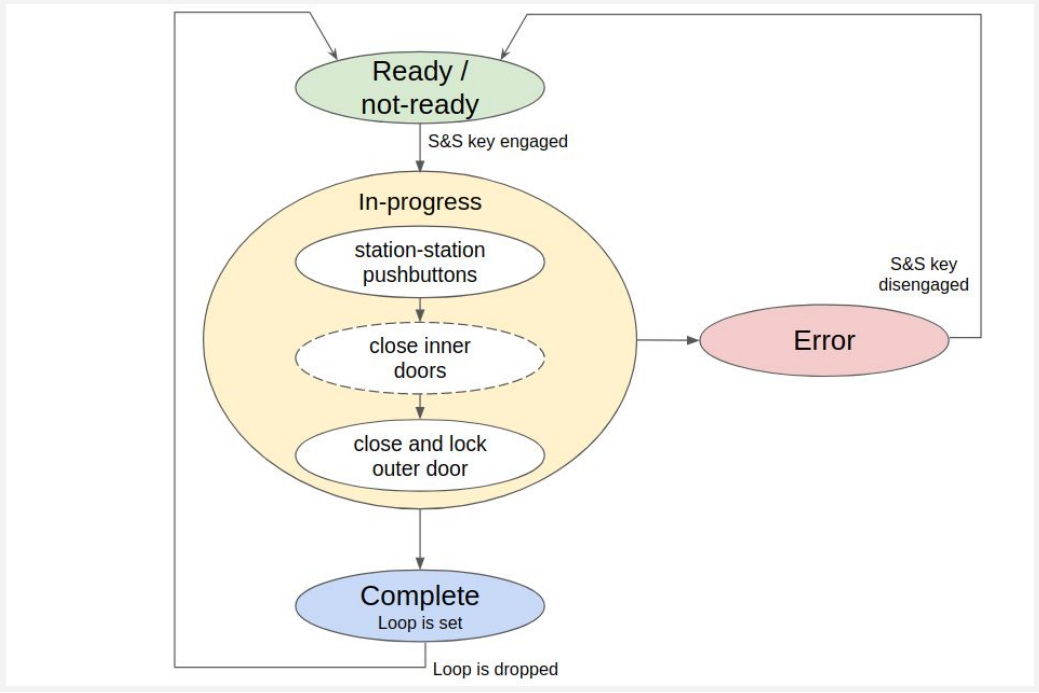

Figure 4.7-1 showing the search and secure states for a complex area, which uses engineered S&S stations.

Search and Secure for non-complexsSpaces

- These spaces have no S&S stations, and only a trapped key(s) to lock the doors.
- The search and secure is accomplished by the search team using a procedure. This is executed immediately prior to locking the area with the TKS.
- For these areas, the loop is set when 1) the loop is currently not set, and, when all of the trapped keys for the area transition to their locked position.
- The loop is dropped upon any of the following:
  - the trapped key is used to unlock the main door.
  - an emergency stop condition is declared
  - a door violation (door open while the trapped key is in the locked position).
  - A TKS emergency egress button is hit.

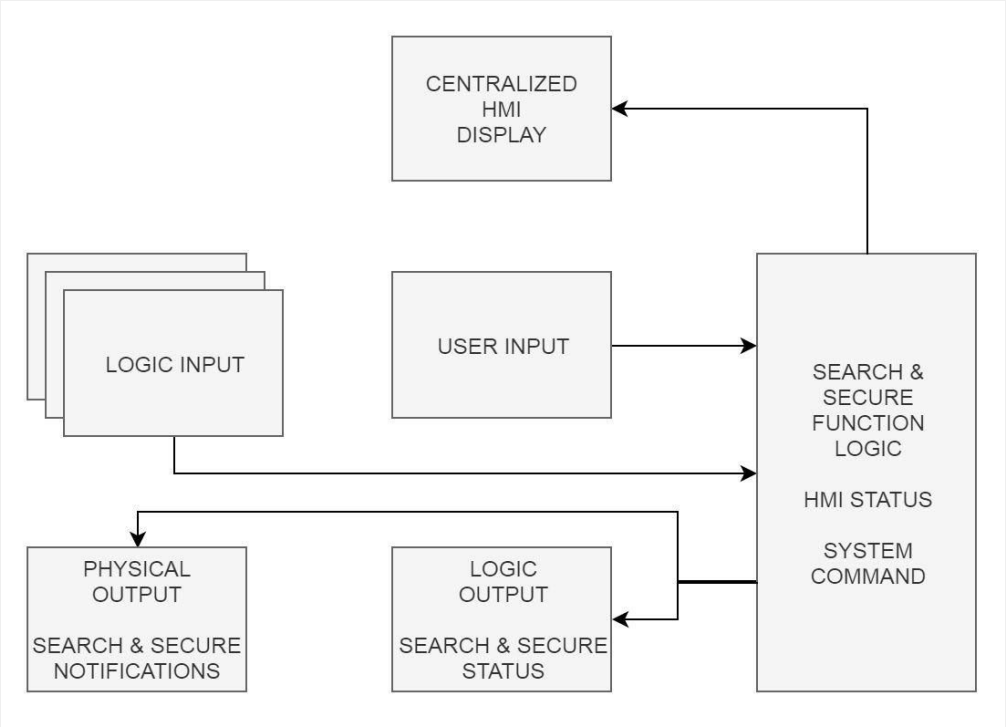

Figure 4.7-3 A diagram showing a representation of the data flow for the Search and Secure software.

4.7.1 S&S Functional Description

The functions that support search and secure will be described below. Dependencies, such as field I/O devices and other functions from this document, are shown.

Table 4.7.1-1 S&S Area Door Violation

FUNCTION ID	FUNC-SS-01
Title	S&S Area Door Violation

Description	After a specific search and secure area loop has been set, any area door opening becomes violation for the search and secure area. Most areas have multiple doors. The loop will drop (no longer set) upon a door violation.
Dependency	● FUNC-SS-02 (loop is set) ● Any door to the area opens
Result	● Door violation variable is set and latched. It will be reset when the area

Table 4.7.1-2 S&S Area Loop-Set Status

FUNCTION ID	FUNC-SS-02
Title	S&S Area Loop-Set Status
Description	The search and secure area loop is set when the search and secure process is completed. The area loop is maintained to be set until a door violation condition invoke and break the area loop. The loop is reset when the area is returned to ACCESS state.
Dependency	The following conditions decide if the area loop is set. ● FUNC-SS-03 (S&S status transition to "complete"). The following conditions decide if the area loop is unset/dropped. ● FUNC-SS-01 (area door violation), or ● FUNC-TKS-01 (trapped key unlocks area)
Result	The state of search and secure area loop is updated.

Table 4.7.1-3 S&S Status for an Area

FUNCTION ID	FUNC-SS-03
Title	S&S Status
Description	The status of the S&S for a specific exclusion area can be represented using a state machine as depicted in figure 4.7-1. The state machine's control will be directed by process variables posted by other software functions, as noted in the dependencies. The S&S states are: ● ready/not-ready to begin ● in-progress ● complete ● error
Dependency	● FUNC-SS-04 (ready/not-ready) ● complex area: FUNC-TKS-01 (S&S key at master station)

	● simple area: FUNC-TKS-01 (area key toggle) ● complex area: FUNC-SS-05 (complex Sequence Validation) ● simple area: FUNC-SS-06 (simple Sequence Validation) ● FUNC-SS-02 (Loop dropped)
Result	The S&S status will be posted in a process variable.

Table 4.7.1-4 Ready for S&S

FUNCTION ID	FUNC-SS-04
Title	Ready for S&S
Description	This function will indicate if an area is ready to initiate a S&S.
Dependency	● FUNC-ASTAT-03 (area in ACCESS state). ● complex area: FUNC-TKS-01 (S&S key at master station is in the "off" position) ● all doors to the area are closed.
Result	The process variable is updated accordingly.

Table 4.7.1-5 S&S Sequence Validation for a Complex Area

FUNCTION ID	FUNC-SS-05
Title	Complex S&S Sequence Validation
Description	Reference figure 4.7-1. Once the S&S is in the "in-progress" state (master S&S key transition), the search team will use the momentary button at each S&S station to acknowledge area inspection. Each specific area will have a unique number of stations, a specific order, and a time-limit between stations. The function will make the search progress available for the HMI and logging functions.
Dependency	● FUNC-SS-03 (S&S status is in-progress) ● FUNC-TKS-01 (S&S key position maintained in "S&S" position until after the final S&S station pushbutton) ● FUNC-ASTAT-03 (area remains in ACCESS state) ● area doors remain closed. Main door is allowed to open for egress after final S&S station pushbutton. ● Logic shall be written to ensure sequential order. ● Logic shall provide a limit for each station-station travel time.
Result	If the sequence completes normally, the S&S status will update to "Complete". Otherwise, a Sequence Error will be declared and the S&S status will be set to "error". Errors are sequence violation, time expiration, a door opening, or an E-Stop.

Table 4.7.1-6 S&S for a Simple Area

FUNCTION ID	FUNC-SS-06
Title	S&S for a Simple Area
Description	While the area is in the ACCESS state, the search team will enter and search the area, then exit and lockup the area. This sets the loop for that area.
Dependency	● FUNC-TKS-01 (trapped key position) ● all area doors must be closed when the TKS key transitions to the locked position.
Result	The loop is set for the area.

4.8 CCS Interface Module

The purpose of the interface between SIS and CCS is to allow the CCS to correctly operate, configure, and arm the sub-systems. Reference [6] specifies the required signals. The interface is unidirectional; signals are from SIS to CCS. This interface shall not impact the SIS's ability to provide its safety functions. In the next section, the inputs, logic, and sequencing that produce each signal's state will be shown.

Table 4.8-1 Summary of SIS Signals to CCS

Description	Format
PSS-SIS Emergency Stop	binary
FCPC Configured for Dummy Load	binary
FCPC Safe to Enable	binary
NB Configured for Dummy Load	binary
NB Safe to Enable	binary
NTC Area Access Status-Access	binary
NTC Area Access Status-No Access	binary
NTC Area Access Status-S&S in Progress	binary
NTC Area Access Status-Lockdown	binary
MERM Area Status-Access Status	binary
MERM Area Access Status-No Access	binary
MERM Area Access Status-S&S in Progress	binary

MERM Area Access Status-Lockdown	binary
Test Cell Basement Area Access Status ● ACCESS ● NO ACCESS ● LOCKDOWN	Three States*
Cable Spread Room Area Access Status ● ACCESS ● NO ACCESS ● LOCKDOWN	Three States*
SIS Alarm Notification ● no alarms ● all alarms acknowledged ● some un-acknowledged alarms	Three States*
● Time of Day fiducial	binary

* Three states are: Off, On, 1 Hz toggle.

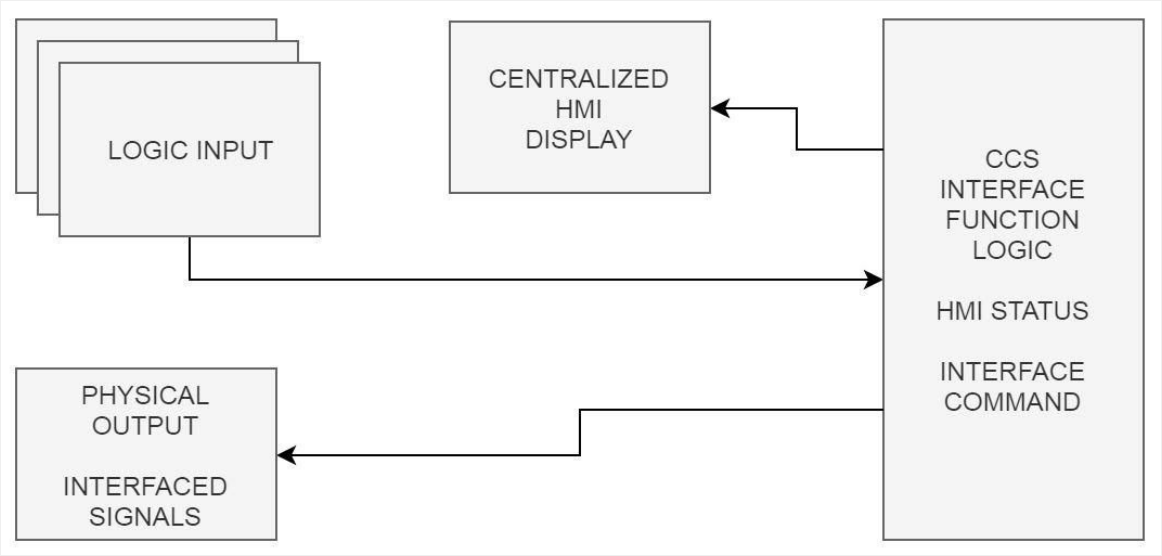

Figure 4.8-1 A diagram showing a representation of the data flow for the CCS Interface software.

Each group of interface signals is physically transmitted from SIS output modules to CCS input modules using discrete signals. There are two formats to transmit the groups of interface signals: binary or three-state.

- Binary: The 24VDC discrete signal is used to represent two states of one signal. The high voltage level indicates that the signal is activated, and the low voltage level indicates that the signal is deactivated.

- Three-state: A 24VDC discrete signal can also be used to represent three states of one signal. The high and low voltage levels indicate two states, and a slow pulse train on the order of one hertz represents the third state.
    - Using the three state method will likely add about 2 seconds of latency since the receiver must wait for the pulse train to be measured and established.
    - The slow pulse train will have these characteristics:
        - period between 0.75 and 1.25 seconds
        - duty cycle between 40% and 60%

The CCS interface function shall transmit the current state of each signal through the corresponding physical output and update centralized HMI with the latest status of the signals.

4.8.1 CCS Signals Functional Description

The criteria for asserting the SIS-to-CCS signals are described in the sections below.

Table 4.8.1-1 No PSS-SIS Emergency Stop

FUNCTION ID	FUNC-CCS-01
Title	No PSS-SIS Emergency Stop
Description	The status of SIS emergency stop condition is updated and transmitted from SIS to CCS. **Signal** / **Definition** 24 V / No E-Stop 0 V / E-Stop is active
Dependency	● FUNC-SACT-01
Result	The state of SIS emergency stop condition is sent to CCS.

Table 4.8.1-2 FCPC Dummy Load Configuration

FUNCTION ID	FUNC-CCS-02
Title	FCPC Dummy Load Configuration
Description	FCPC Dummy Load configuration will report its status by using a trapped key and light curtain feedback signals, once this is complete a status bit will be set and sent to CCS from SIS. The following conditions must be satisfied. See figure 4.8.1-1. ● The PCTS trapped key position indicates the coil's bus-links barrier is

	in-place. secured, and the trapped key has been removed (which locks the barrier in place). ● PCTS Light Curtain indicates no bus-links to the coils are installed **Signal** / **Definition** 24 V — FCPC in DL configuration 0 V — FCPC not in DL configuration
Dependency	● FUNC-TKS-01 (PCTS Trapped key) ● FUNC-CMS-01 (PCTS light curtain)
Result	The state of FCPC dummy load configuration is sent to CCS.

Table 4.8.1-3 Safe to Enable FCPC

FUNCTION ID	FUNC-CCS-03
Title	Safe to Enable FCPC
Description	The status of this permissive is updated and transmitted from SIS to CCS. ● The criteria for asserting the "Safe to Enable FCPC" signal is defined in the reference [4]. This logic is depicted in figure 4.8.1-1 below. **Signal** / **Definition** 24 V — Safe to Enable FCPC 0 V — Not Safe to Enable FCPC
Dependency	● FUNC-ASTAT-01 (exclusion areas in NO ACCESS) ● FUNC-CCS-02 (FCPC dummy load state is active) ● FUNC-CMS-01 (no coil links present in PCTS) ● FUNC-TKS-01 (PCTS links-barrier present and locked in place)
Result	The state of FCPC permissive is sent to CCS.

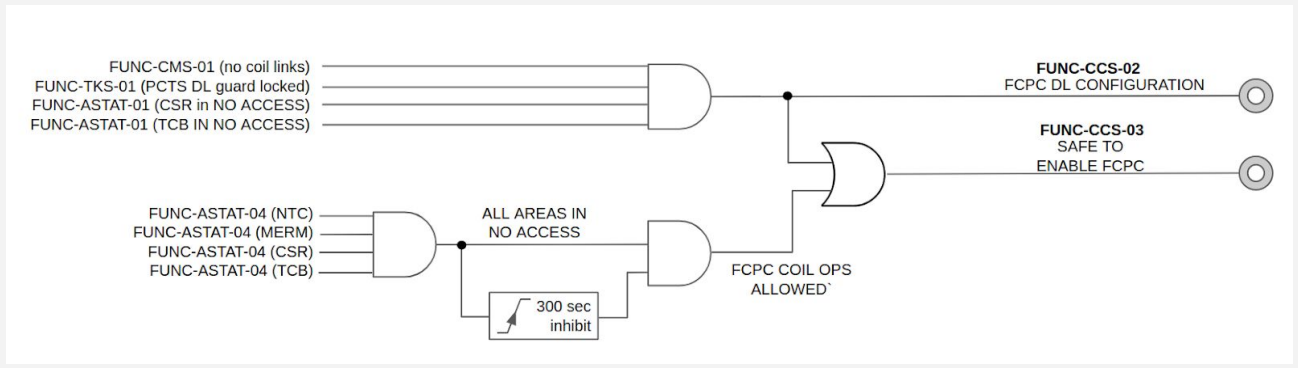

Figure 4.8.1-1 The logic used to create the SAFE TO ENABLE FCPC and the FCPC DUMMY LOAD signals to CCS.

Table 4.8.1-4 NB Dummy Load Configuration

FUNCTION ID	FUNC-CCS-04
Title	NB Dummy Load Configuration
Description	NB Dummy Load configuration will report its status by using a trapped key and breaker feedback signals, once this is complete a status bit will be set and sent to CCS from SIS. The following conditions must be satisfied.See figure 4.8.1-2. ● NB Dummy Load key is engaged at ESF2-SB05. This interdicts the "UV Trip" circuit to ensure the breaker cannot energize. ● The ESF2-SB05 breaker position indicates open (de-energized). **Signal** / **Definition** 24 V — NB in DL configuration 0 V — NB not in DL configuration
Dependency	● FUNC-TKS-01 (NB DL Key at ESF2-SB05) ● ESF2-SB05 (breaker position)
Result	The state of NB dummy load configuration is sent to CCS.

Table 4.8.1-5 Safe to Enable NB

FUNCTION ID	FUNC-CCS-05
Title	Safe to Enable NB
Description	The status of this permissive is updated and transmitted from SIS to CCS.

	• The criteria for asserting the "Safe to Enable NB" signal is defined in the reference [4]. This logic is depicted in figure 4.8.1-2 below. **Signal** / **Definition** 24 V — Safe to Enable NB 0 V — Not Safe to Enable NB
Dependency	• FUNC-CCS-04 (NB dummy load state is active) • FUNC-ASTAT-01 (exclusion areas in NO ACCESS)
Result	The state of NB permissive is sent to CCS.

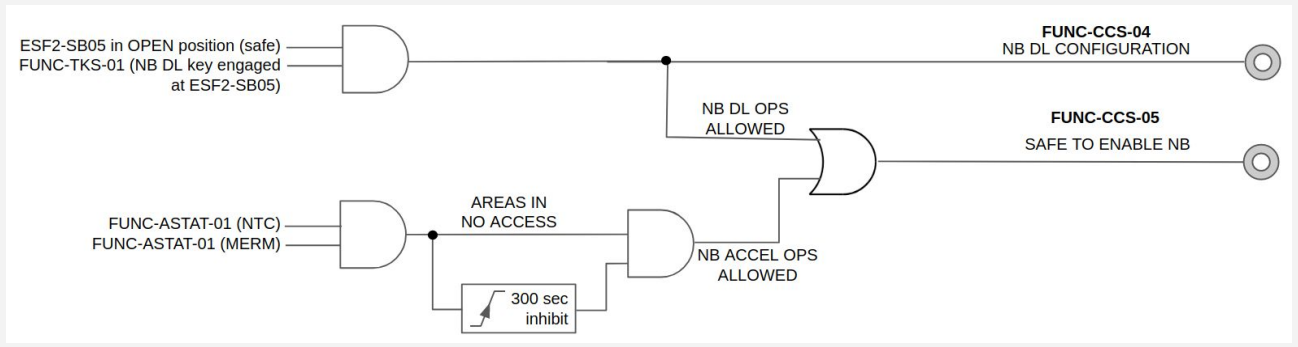

Figure 4.8.1-2 The logic used to create the SAFE TO ENABLE NB and NB DUMMY LOAD signals to CCS.

Table 4.8.1-6 Exclusion Area Access State for Complex Spaces

FUNCTION ID	FUNC-CCS-06
Title	Area Status for an exclusion area that incorporates Search and Secure
Description	The area status of an exclusion area is updated and transmitted from SIS to CCS. There are four bits used for each exclusion area. **Bit 1 Signal** / **Definition** 24 V — ACCESS state 0 V — not ACCESS state **Bit 2 Signal** / **Definition**

<table>
<tr><td></td><td>
<table>
<tr><td>24 V</td><td>S&S in-progress</td></tr>
<tr><td>0 V</td><td>S&S not in-progress</td></tr>
</table>
* Note that the S&S Secure in-progress will be asserted while the ACCESS state is also asserted.
<table>
<tr><th>Bit 3 Signal</th><th>Definition</th></tr>
<tr><td>24 V</td><td>NO ACCESS state</td></tr>
<tr><td>0 V</td><td>not NO ACCESS state</td></tr>
</table>
<table>
<tr><th>Bit 4 Signal</th><th>Definition</th></tr>
<tr><td>24 V</td><td>LOCKDOWN state</td></tr>
<tr><td>0 V</td><td>not LOCKDOWN state</td></tr>
</table>
</td></tr>
<tr><td>Dependency</td><td>

ACCESS (FUNC-ASTAT-03)
Search & Secure is in-progress (FUNC-SS-03)
NO ACCESS (FUNC-ASTAT-04)
LOCKDOWN (FUNC-ASTAT-02)

</td></tr>
<tr><td>Result</td><td>The state of the access status of a complex space is sent to CCS.</td></tr>
</table>

Table 4.8.1-7 SIS Alarm Notification

<table>
<tr><td>FUNCTION ID</td><td>FUNC-CCS-07</td></tr>
<tr><td>Title</td><td>SIS Alarm Notification</td></tr>
<tr><td>Description</td><td>The status of existing SIS alarm condition is updated and transmitted from SIS to CCS.
<table>
<tr><th>Signal</th><th>Definition</th></tr>
<tr><td>24 V</td><td>No SIS Alarms</td></tr>
<tr><td>0 V</td><td>there is one or more active alarms that have not been acknowledged by the PSS-SIS operator</td></tr>
<tr><td>1 Hz</td><td>there is one or more active alarms, and all have been acknowledged by the</td></tr>
</table>
</td></tr>
</table>

	PSS-SIS operator
Dependency	• FUNC-ALM-03 (Aggregate Alarm Indication)
Result	The state of the existing SIS alarm conditions is sent to CCS.

Table 4.8.1-8 Exclusion Area Access State for Simple (not complex) Spaces

FUNCTION ID	FUNC-CCS-08
Title	Area Status for an exclusion area that has no engineered Search and Secure stations.
Description	The area status of an exclusion area is updated and transmitted from SIS to CCS. There is one three-state bit used for each simple exclusion area. **Bit Signal** / **Definition** 24 V – NO ACCESS state 0 V – ACCESS state 1 Hz – LOCKDOWN state
Dependency	• ACCESS (FUNC-ASTAT-03) • NO ACCESS (FUNC-ASTAT-04) • LOCKDOWN (FUNC-ASTAT-02)
Result	The state of access status of a simple space is sent to CCS.

Table 4.8.1-9 Time of Day Fiducial

FUNCTION ID	FUNC-CCS-09
Title	Time of Day Fiducial
Description	Since the SIS will have no networked NTP time service the local time may drift. Once a day (e.g. 0600 hours) a 60-second fiducial signal will be sent tothe CCS. The CCS, which is likely NTP'd, can determine the SIS time drift and warn the operator if it exceeds a threshold. **Signal** / **Definition** 24 V – Timing Mark ON

	0 V | OFF
Dependency	• System Time of day
Result	A timing marks is sent to CCS.

4.9 Centralized HMI Module

4.9.1 CHMI Interface Functions

The Centralized HMI software will use COTS software to produce operators screens to allow the system status to be observed, and control widgets to allow authenticated operators to affect the system's status. Displays will also show system events and alarms.

Table 4.9.1-1 CHMI Monitoring

FUNCTION ID	FUNC-HMI-01
Title	CHMI PSS-SIS Monitoring
Description	All field equipment, inputs, outputs, and push buttons used on PSS-SIS will be configured to display their status on the CHMI. In addition, (internal) process variables that are determined by the SIS logic can be displayed. The following devices and equipment types will be displayed: • SV and SF breakers • S1-B1 breaker • Safety Relay s • Guards • Light Curtains • E-Stops • Doors • UPS • Sensors • Status Lights • Klaxons • Network • CPU Status • I/O Module's Status • Trapped Keys • TKS Emergency Egress push buttons
Dependency	Field equipment status and process variables.
Result	Status updates are sent to CHMI

Table 4.9.1-2 CHMI Operator Controls

FUNCTION ID	FUNC-HMI-02
Title	CHMI PSS-SIS Operator Controls
Description	Properly authenticated operators will be able to perform the following controls that affect the PSS-SIS operation using the CHMI: ● Disable the ACAMS card reader at the NTC north door (FUNC-ASTAT-05) ● Disable the ACAMS card reader at the NTC south door (FUNC-ASTAT-05) ● Reset the Emergency Stop Condition (FUNC-AACT-02) ● Release the LOCKDOWN state for a specific area (FUNC-ASTAT-02). This release can only be activated while in the LOCKDOWN state
Dependency	Operator type, with proper authentication.
Result	Commands are sent to the PSS-SIS logic for use by other functions.

Table 4.9.1-3 CHMI Alarm Display Functions

FUNCTION ID	FUNC-HMI-03
Title	CHMI Alarm Display Functions
Description	Monitored equipment will typically be associated with alarming logic that will be used to display status on the CHMI. Alarm categories are described in the Alarms software module section, FUNC-ALM-01 and -02. The operator must be authorized (username/password) in order to acknowledge alarms.
Dependency	Field equipment changes to a safe, unsafe, or inconsistent state and relevant process variables. Operator level.
Result	Alarm status updates are sent to CHMI

Table 4.9.1-4 CHMI Process Event Log

FUNCTION ID	FUNC-HMI-04
Title	CHMI Event Logic
Description	All monitored and program sequenced equipment will be associated with event logic that will be used to display the status of various PLC states, modes and operations on the CHMI. In addition, events may be triggered by other modules and functions.

	The following devices and equipment types may have associated events: ● SV-SF Trip ● S1-B1 Trip ● Guards ● E-Stops ● Door Violation ● Sensors ● S&S activities
Dependency	Field equipment changes state; mode changes; specific program operation occurs
Result	Event status updates are sent to CHMI

Table 4.9.1-5 CHMI System Event Log

FUNCTION ID	FUNC-HMI-05
Title	CHMI System Logic
Description	All monitored PSS-SIS system info will have system logic that will be used to pull system info from the CPU to be used in the program. The following CPU attributes are typical of what could be recorded in the system log. ● System started (PLC began scanning) ● Communication Errors ● I/O Station Power Supply and UPS ● Total memory ● Total free memory ● Maximum Scan Time ● Percent of the available CPU time that is assigned to communications ● Safety or CPU Passwords present ● Network ● CPU Status ● Module Status
Dependency	Specific system and CPU information.
Result	System event status updates are sent to CHMI

4.9.2 CHMI Screen Types

The Centralized HMI GUI will contain various screens used to monitor and control various pieces of PSS equipment. All screens will have a header and footer section that will contain the Screen Title, Date, Navigation Buttons and an Alarm/Events Banner similar to Figure 4.8.2-1 ; exceptions are allowed, as deemed appropriate.

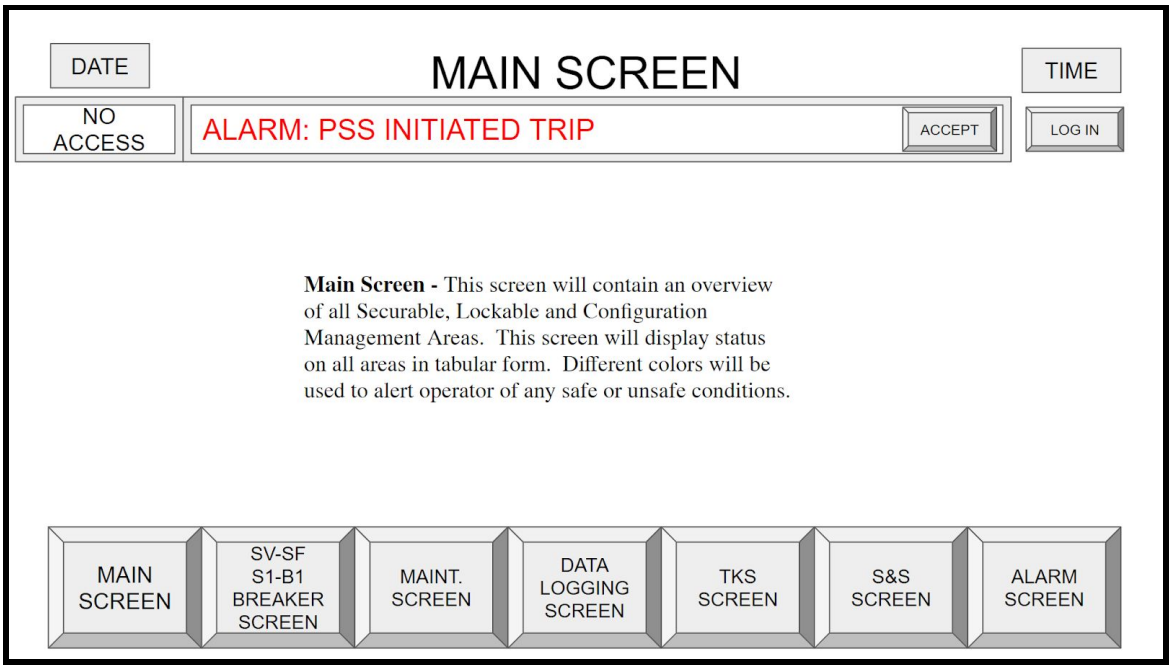

Figure 4.9.2-1 Shows Main screen header and footer

These screens can contain push buttons, graphic objects tables etc, to be used for showing additional details, information, data, or status of the system if necessary. A color convention for graphical objects , indicators, and text will be agreed upon before the display development and included in the user manuals that will be written.

Note: Shown below is a suggested layout of some required system screens and their intended purpose. The layout is not an exact representation of how the screens should be designed and function. Screens will be designed to suit the need of the users after a careful review is conducted by the PSS Team and COE during the time of its actual configuration and design.

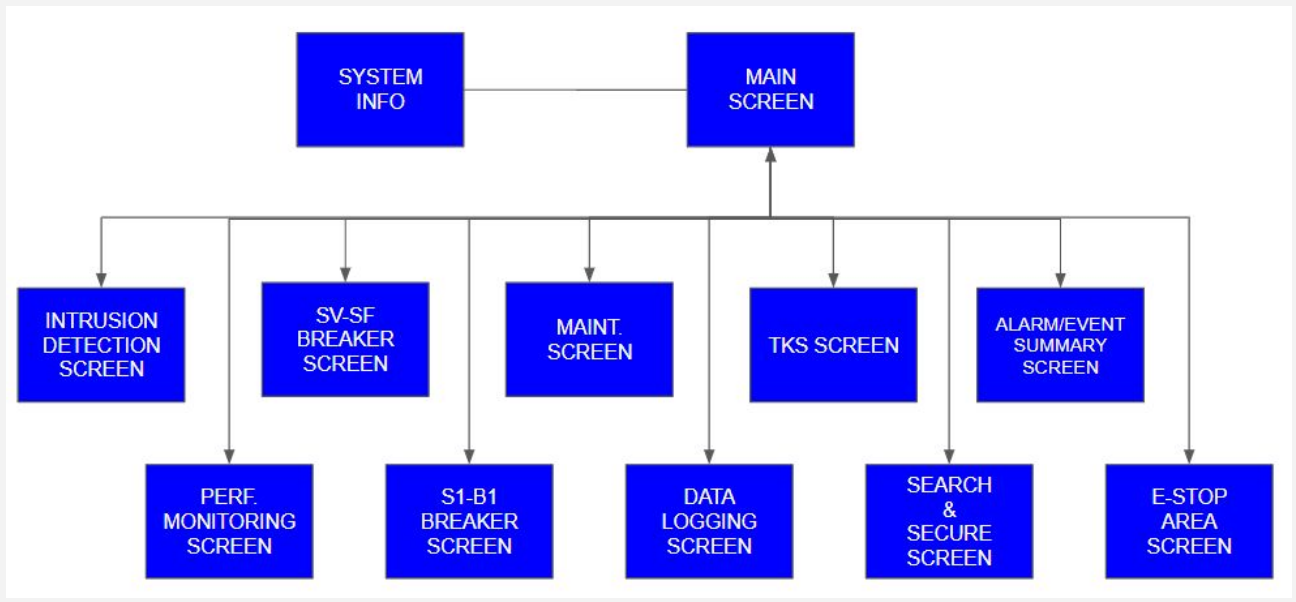

Figure 4.9.2-1 Shows sample screen navigation for the user.

Listed below are typical screen descriptions and their functionality.

- **Main Screen -** This screen will contain an overview of all Exclusion Areas that are Securable, Lockable and Configuration Management Areas. This screen will display status on all areas in tabular form. Different colors will be used to alert operator of any safe or unsafe conditions.

- **E-Stop Area Screen -** This screen will contain graphical or tabular status of systems or equipment that influence the Emergency Stop condition.

- **Area Status Screen -** This screen will contain graphical or tabular status showing the Area Status, and factors that contribute to the area's status (e.g. S&S, keys, doors).

- **Search & Secure Screen -** This screen will contain graphical or tabular status of all S&S locations. This screen will display S&S Total time countdown as well as a Total Station time countdown as well.

- **Alarm/Events Summary Screen -** This Screen will contain a history of all alarms and events, as well as currently active alarms. The screen will contain controls to acknowledge and/or reset "one" or "all" alarms as well as clear resolved alarms.

- **SV-SF, S1-B1 Breaker Screen -** This screen will contain graphical or tabular status of SV, SF and S1-B1 breakers. Different colors will be used to alert operator of any safe or unsafe conditions.

- **TKS (Trapped Key System) -** This screen will contain graphical or tabular status of Trapped Key connections to PSS-SIS. This includes trapped keys and egress buttons.

- **Maintenance Screens -** This screen will contain graphical or tabular status of objects used used for status, maintenance and testing of the system, see the list below for minimum data to be shown.
  - All I/O associated with the SIS system.
  - RIO Drop#, address, status and any fault indication.

- **Intrusion Detection Screen -** This screen will contain graphical or tabular status of all rack doors, cabinet doors, data ports and other enclosure covers.

- **System Info Screen:** This screen will display the following minimum information:
  - HMI Name and Version
  - PLC Program Name and Version
  - Time and Date
  - Contact information of end User

- **Performance Monitoring Screen:** This screen will contain graphical or tabular status of the PSS-SIS PLC performance.
  - Maximum Scan Time
  - Memory Usage
  - Watchdog timer

- **Data Export Screen** - This screen will allow data to be copied to a USB memory stick. It may call logic to convert the data, if necessary.

- **Log In/Log Out** - The system shall provide a mechanism to log in/out the active operator. Log in/out activity will be recorded in the system event log.

4.9.3 CHMI Screen Saver

The CHMI screens shall remain visible at all times; the screen saver shall be disabled at all times.

4.9.4 CHMI User Levels and Authentication

For the SIS application program, the User types in Table 4.9.4-1 below will be configured to allow user-access to screens after a User has entered their ID and password (authentication) from the login screen. Once authenticated, users will be able to access various screens depending on their assigned User Level.

The following User Groups will have varying levels of access.

- Guest = Level 1
- Engineer = Level 2
- COE = Level 3

Table 4.9.4-1 shows what screens permissions are granted to each user. All screens will be viewable for all users, but permission to modify a screen or object will only be allowed for users who have adequate privileges.

Table 4.9.4-1 Operator Permissions

PERMISSIONS	GUEST	PSS ENGINEER	COE
	Level 1	Level 2	Level 3
View Screens	X	X	X
Acknowledge Alarms		X	X
Control Widgets		X	X
Export Data (USB)		X	X

User levels will allow access to view and control the following if available:

- Alarm Screen/Alarm Banner
- Popup windows
- Objects such as switches, push buttons and data displays.
- Data Manager

The CHMI will provide the users with “Log In” and “Log Out” capability.

- Each operator will login in using a unique user ID and/or password assigned to each person.
- Login information shall be logged in the System Log.

4.10 Alarm Module

The purpose of the alarm module is to handle and track the alarms and present them to the operator. Alarm conditions are determined by SIS logic, and could be the result of a transient condition. In order not to generate false alarm, a time delay or other features should be built into the alarm-generating logic. The alarm module shall not influence the safety-relevant logic of the SIS.

The alarm module collects and manages alarms that are generated by the other modules; all alarms are logged and time-stamped. The alarm handling function shall transmit the current state of the generated alarm signal to the centralized HMI. Alarms will be latched and require an operator to acknowledge the alarm before it can be cleared from the alarm display.

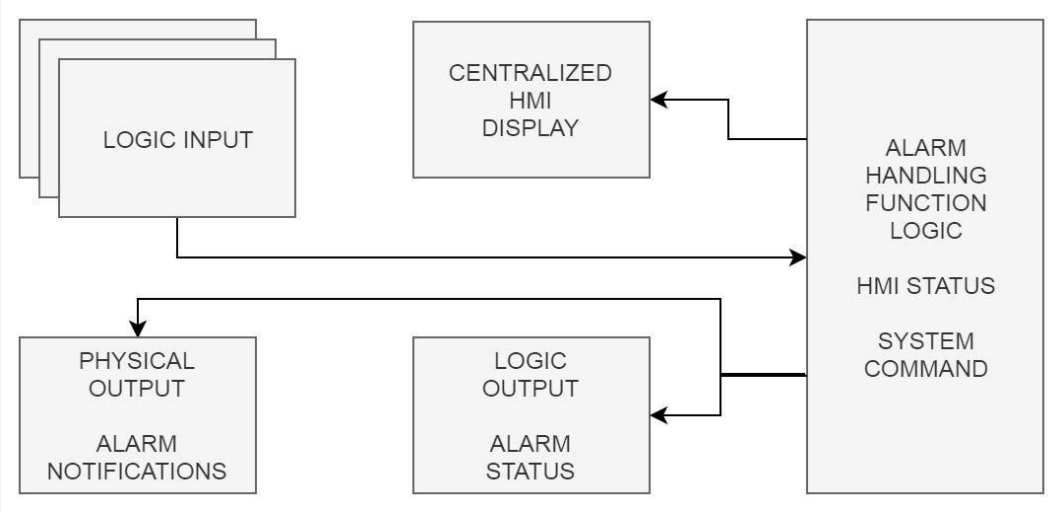

Figure 4.10-1 A diagram showing a representation of the data flow for the Alarm Handling software.

Alarms will be classified with two levels, Critical and Warning. Critical alarms typically compels action by the operator. This might be to administratively suspend NSTX-U operations, or to call upon system engineers to analyze the alarm situation and if necessary to perform repairs or tests. Warning-class alarms typically will not affect NSTX-U operations and do not impact the safety functions or degrade the performance of the system. Table 4.10.1-1 lists some typical alarms.

Table 4.10-1 Typical Alarm Categories

Category	Description	Level
E-STOP	SIS ESTOP condition	Critical
Door	SIS door access violation	Critical
Device	SIS field device circuit fault	Critical
System Power	SIS control system DC power	Critical
System Comm	SIS control system communications	Critical
System Door	SIS control system cabinet door	Warning
Search & Secure	SIS search and secure error	Warning
TKS	An Emergency-Egress TKS Push-to-exit button has been hit.	Warning
Device	A safety relay's auxiliary contacts disagree with its commanded position.	Warning

4.10.1 Alarms Functional Description

Table 4.10.1-1 SIS Critical Alarm

FUNCTION ID	FUNC-ALM-01
Title	SIS Critical Alarm
Description	A critical alarm condition has been activated; this occurrence of the alarm is latched. The alarm will clear once the causing conditions have terminated and the operator has acknowledged the alarm.
Dependency	The alarm condition is generated by SIS logic. The alarm is typically latched, and will be in the unacknowledged state until the operator acknowledges the alarm. ● SIS logic (initiates the alarm) ● FUN-ALM-05 (Acknowledge Alarm)
Result	SIS alarm status is updated at display terminal. An active alarm can be unacknowledged or acknowledged.

Table 4.10.1-2 SIS Warning Alarm

FUNCTION ID	FUNC-ALM-02
Title	SIS Warning Alarm
Description	A warning alarm condition has been activated; this occurrence of the alarm is latched. The alarm will clear once the causing conditions have terminated and the operator has acknowledged the alarm.
Dependency	The alarm condition is generated by SIS logic. The alarm is typically latched, and will be in the unacknowledged state until the operator acknowledges the alarm. ● SIS logic (initiates the alarm) ● FUN-ALM-05 (Acknowledge Alarm)
Result	SIS alarm status is updated at display terminal. An active alarm can be unacknowledged or acknowledged.

Table 4.10.1-3 SIS Aggregate Alarm Indication

FUNCTION ID	FUNC-ALM-03
Title	SIS Alarm Indication
Description	A three-state variable that summarizes the alarm situation.

Value	Definition
0	No SIS Alarms

	1 — there is one or more active alarms that have not been acknowledged by the PSS-SIS operator 2 — there is one or more active alarms, and all have been acknowledged by the PSS-SIS operator
Dependency	● FUNC-ALM-01 (status of Critical alarm) ● FUNC-ALM-02 (status of Warning alarm)
Result	SIS alarm status is updated at display terminal.. The aggregate alarm can be active or inactive. If it is active, it can be unacknowledged or acknowledged.

Table 4.10.1-4 SIS Alarm Logging

FUNCTION ID	FUNC-ALM-04
Title	SIS Alarm Logging
Description	All critical or warning alarms are logged at display.
Dependency	● FUNC-ALM-01 Any critical alarm is active. ● FUNC-ALM-02 Any warning alarm is active. ● Time-Stamp
Result	Active alarm log message is indicated at display terminal. The log message should include a timestamp.

Table 4.10.1-5 SIS Alarm Acknowledgement

FUNCTION ID	FUNC-ALM-05
Title	SIS Alarm Acknowledgement
Description	Any active critical or warning alarm is acknowledged at display.
Dependency	● The Alarm Screen at the CHMI ● An authenticated and authorized operator.
Result	Critical or warning alarm is acknowledged.

Table 4.10.1-6 SIS Alarm Clear

FUNCTION ID	FUNC-ALM-06
Title	Any active critical or warning alarm is cleared at display and panel.

Description	Any active critical or warning alarm is reset at display.
Dependency	● The Alarm Screen at the CHMI ● An authenticated and authorized operator.
Result	Critical or warning alarm is reset.

5. Non-functional Requirements

5.1 Safety Requirements

The PSS-SIS is itself a safety system and a credited control system at PPPL. The system's (including software and processing components) safety requirements are addressed in [2,4], which reference other PPPL, DOE, and international standards that apply to safety systems.

5.2 Software Quality Assurance

Software Quality Assurance (SQA) at PPPL is guided by reference [7]. A specific SQA Plan document has been prepared for the PSS-SIS software [8]; this calls for additional documents to be written.

5.3 Security Requirements

5.3.1 Physical Security

The SIS (system) will use physical security mechanisms to prevent unauthorized access to the processor, network components, and I/O equipment. The type, number, and location of these is a function of the hardware design; the number of intrusion detectors is on the order of 30. In the event one of the monitored signals transitions to "accessible" the software will provide an alarm. Intrusion detection (FUNC-SYSM-03) is described in the System Monitoring chapter.

The following requirement is for monitored intrusions.

- Rack and Cabinet Doors - An alarm will be logged on the Alarm summary screen if door is opened.
- Data Port and other enclosure covers - An alarm will be logged on the Alarm summary screen if the (monitored) cover is opened.

In addition, access to some SIS components may be restricted by using "secure fasteners". These are a mechanical solution, have no SIS monitoring, and are a function of special tooling coupled with administrative procedures (to access said tooling and perform work on the PSS).

5.3.2 Network and Cyber Security

The PSS-SIS requirements [4] includes some network and cyber security requirements. A separate document [9] that considers PPPL's Information Technology Department (ITD) perspective and oversight will be prepared.

In order to guard against potential Cyber attacks the PSS-SIS is required to employ an “air gapping” measure to ensure that the system (and its network) is isolated from public or other PPPL networks via wired or wireless connections (i.e “closed system”).

5.4 Performance Requirements

The following are the requirements for PSS-SIS PLC performance and program timing. These values will enable the system to operate within a satisfactory reaction time.

1) The overarching performance requirements is derived from reference [2], section 3.4a: *the time allowed for interdiction is up to 4 seconds*.
2) Assumption: logic will scan at least every 200 milliseconds. The references [2,4] do not require this scan time. It is presented here to support a preliminary timing analysis.

Diagram 5.4-1 illustrates a preliminary timing analysis of how the overarching performance requirement is reasonably achievable. The values used are fairly conservative and most times can be reduced in order to meet the 4 second timing requirements. The diagram shows that the time for interdiction following the “unsafe trigger event” to the opening of the breaker is estimated to be about 3.6 seconds. The I/O and processing events that take place in each of the A-B-C regions indicated on the timing diagram are detailed in table 5.4-1.

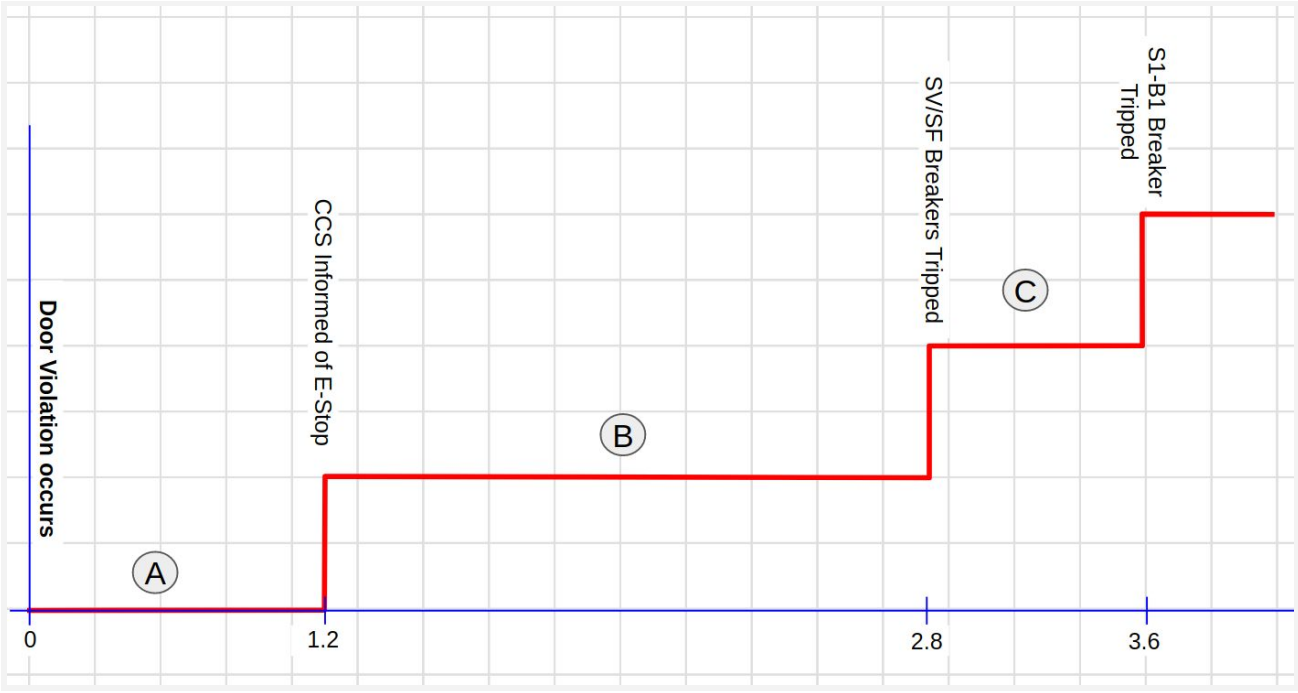

Figure 5.4-1 A diagram showing the “time-to-interdict”, and an estimation of the processing and elapsed time that the software and system might provide.

Table 5.4-1 Detail of the timing and sequencing in support of figure 5.4-1.

Action Phase	Phase Time (sec)	Actions (using 0.2 s logic scan)
A	1.2	● During NO ACCESS, a **door opens at T=0**. Digital input sees input change at T+0.2 s. ● FUNC-COND-01 Input signal conditioning take 0.2 s. ● FUNC-SS-01 then FUNC-SACT-05 then FUNC-SACT-01 uses 0.6 s. ● FUNC-CCS-01 asserts digital output. no output signal conditioning. 0.2 s ● **E-Stop is asserted, safe-to-enable revoked, to CCS at T+1.2 s.**
B	1.6	● FUNC-SACT-02 allows CCS/BCS 1.0 s to trip breakers and then evaluates need to interdict . ● FUNC-SACT-03 asserts interdiction process variables (0.2 s). ● FUNC-COND-02 use 0.3 s for signal conditioning, asserts digital outputs. ● assume 0.1 s for safety relay and SV/SF breaker trip. ● **SV/SF breakers open at T+2.8 s.**
C	0.8	● digital inputs read for SV/SF breaker positions. ● FUNC-COND-01 Input signal conditioning take 0.2 s. ● FUNC-SACT-04 decides whether S1-B1 interdiction is necessary, and asserts interdiction process variables (0.2 s). ● FUNC-COND-02 use 0.3 s for signal conditioning, asserts digital outputs. ● assume 0.1 s for safety relay and S1-B1 breaker trip. ● **S1-B1 breaker open at T+3.6 s.**

These are the assumptions used in the preliminary timing analysis:

- The logic scan period is 200 ms. This will likely be less.
- The I/O is synchronized with the logic scan. It the event the I/O is asynchronous or data-driven, the latency will be less.
- The I/O to CPU data transfer time over the network is negligible (a few ms).
- Where a chain of functions are required, only one function will execute per logic scan. It is likely the functions can be cleverly sequenced to allow multiple functions per scan. This will reduce the time to interdiction.
- The maximum output signal conditioning delay of 300 ms is used. To reduce the time to interdiction, this can be reduced or eliminated.

5.5 System Monitoring Module

This chapter contains a number of functions related to (SIS) system monitoring.

Table 5.5-1 System Performance Monitoring

FUNCTION ID	FUNC-SYSM-01
Title	Performance Subroutine Logic
Description	Performance information of PSS PLC will be available to the user at the CHMI. This information will enable the user to assess the PLCs ability for continued operation under typical operation. Typical metrics are : ● Maximum Scan Time - Max recorded execution time for program ● Used Memory will be no more than 70% ● Watchdog timer set value
Dependency	Depends on specific retrievable CPU information that can be accessed by logic.
Result	System performance updates are sent to CHMI

Table 5.5-2 Interdiction Timing Measurement

FUNCTION ID	FUNC-SYSM-02
Title	Timing Subroutine Logic
Description	The PSS PLC will be capable of shutting down the interdicted systems within an estimated time of 3.6 seconds (see figure 5.4.1-1), upon a successful detection of a PSS-SIS Emergency Stop condition and feedback of breaker circuit transitioning to open.
Dependency	● Event time for source terms (devices) leading to FUNC-SACT-01 (PSS-SIS Emergency Stop condition) ● Breaker position feedback
Result	The measured time-to-interdict information will be determined and made available for display at the CHMI in seconds (0.1 sec resolution).

Table 5.5-3 System Monitoring

FUNCTION ID	FUNC-SYSM-03
Title	SIS System Health
Description	The PSS SIS System health determines if all necessary components needed to operate the system are active and ready. If all monitored system components are considered ok, a “System health ok” bit will be set. If not an alarm will be triggered.

Dependency	Various control system (infrastructure) conditions. Some examples are: ● SIS system communications ● SIS system power ● I/O Faults ● Minor Faults ● Intrusion
Result	A "System health ok" bit set or "System health not ok" bit set. An event and alarm will be activated on the CHMI respectively.

5.6 Tagnames

The SIS software will use structured tagname (naming) conventions for process variables. The tagnames allow the developer and reader of the software to associate the software's logic functions with the field device or processing sequence. Two tagname structures will be specified, 1) for SIS input/output points, and 2) for internal processing variables. The capability to use variable name *aliasing* is acceptable.

Note that the SIS equipment vendor may have tagname rules for which the definitions described here would violate, or, there may be mandatory or reserved names and conventions for their hardware and software infrastructure. If this should occur then these specifications will be revised accordingly.

5.6.1 Input/Output Tagname structure

The I/O tagnames are shown on the control loop drawings (D-AE8100 through 199) to associate the field process control devices with the SIS input/output points; this tagname convention is derived from that. The PSS project-wide tag/cable/device naming convention is described on drawing D-AE8001. This drawing fully describes the tag structure and permitted field characters and structure.

LOCATION	COMPONENT	FUNCTION	CHAIN	LOOP # and (optional) LOOP SUFFIX	TYPE (optional)

Figure 5.6.1-1 showing the fields in a tagname.

A description of the tagname fields are.

- LOCATION: An abbreviation for the physical location of the (end) field device. This is not always the same as the location of the SIS I/O point.
- COMPONENT: An abbreviation for a component.
- FUNCTION: An abbreviation for the function of the field device.
- CHAIN: A or B for a redundant device; X for non-redundant device.
- LOOP #: A two-digit number that represents the control loop which the tag is directly associated with.
    - LOOP SUFFIX (optional): This has no underscore-separation following the 2-digit loop number. It can be used to provide a unique tag in situations where a control loop has more than one functional device associated with a component, or when a single device has multiple connections to the SIS.
- TYPE (optional): An abbreviation for identifying a specific characteristic of the root tagname.

The I/O tagnames use an underscore to separate the fields. Note that the tags for field devices and cable labels will use hyphens to separate these fields. The software environment should support tagnames having at least 40 characters.

Example: MG_SF205_EY_A_74C_DI

This describes a device located in or nearby the D-Site Motor Generator building, and the field component (or assembly) is a 13.8 KV breaker cabinet ESF2-SB05. The function of the field device is a safety relay (coil) which is the first of a redundant set. It is part of Control Loop 74 and furthermore uses the optional loop suffix of "C", and is a Digital Input point (type).

5.6.2 Process Variable Tagname structure

Since internal (process) variables are not necessarily associated with a physical location, component, or field-process function a different naming convention will be used. The naming convention for variable names is illustrated below. An underscore character is used to separate the fields.

PREFIX (optional)	NAME	SUFFIX (multiple, optional)

Figure 5.6.2-1 showing the fields in a process variable name.

A description of the tagname fields are.

- PREFIX: The prefix can optionally be used to designate a variable associated with a particular device or function. Tags that contribute to a safety instrumented function should use a standard prefix, such as SIF_ .
- NAME: An alpha-numeric string that is descriptive of the variable's meaning or context.
- SUFFIX: The suffix can be used to enhance the description or function of the variable. The developer may use more than one suffix.

The variable tagnames use an underscore to separate the fields. The name can use any alpha-numeric characters, in either upper or lower case as supported by the COTS software environment. The software environment should support tag names having at least 40 characters.

Example: mode_SIS_testing

This could describe an internal binary variable that declares the system is in SIS Testing mode.

Example: SIF_DoorViolation_NTC

This could describe an internal variable that represents a door violation for the NSTX-U Test Cell. The prefix SIF_ denotes this is a safety tag.

5.7 Data Export (USB)

With the importance of the SIS control system, it constantly monitors the safety of the operations. During operation, there are a lot of critical data being monitored, and it is important to record these critical monitored data to a safe location for further analysis or storing purposes.

The HMI unit can produce two types of data to be managed and stored, alarm data and control data. Each data type is managed and defined through its data export model before it is exported to the physical storage.

5.7.1 Alarm Data Export

The alarm data export model allows developer to define how the alarm data is exported to the physical storage. The type of removable storage media should be defined for the associated HMI unit. Accurate storage location needs to be properly written in the data export model. Timestamp has to be included as part of the data export model. During operation, alarm information shall be monitored continuously, and any alarm generation is first stored internally within the HMI unit. With available storage area, preconfigured alarm data information is processed and moved to the removable storage, and it can then be relocated to other storage locations.

FUNCTION ID	FUNC-DE-01
Title	Alarm information data export model
Description	This step is required to provide a working configuration, which allows alarm data to be frequently exported to an external storage location. The configuration shall be verified that it does not degrade the performance of the HMI unit.
Dependency	All of the following conditions are available. ● The export is to be CSV compatible.. ● External storage configuration is required. ● File name labelling configuration is required. ● Export triggering configuration is required.
Results	All available alarm data is transferred to the external storage location when a triggering event is active.

5.7.2 Control Data Export

The control data export model allows developer to define how the control data is exported to the physical storage. The monitored data points have to be selected into the data export model. The type of removable storage media should be defined for the associated HMI unit. Accurate storage location needs to be properly written in the data export model. Timestamp has to be included as part of the data export model. During operation, data points shall be monitored and stored continuously based on the defined exporting frequency. With available storage area, selected data points are processed and moved to the removable storage, and it can then be relocated to other storage locations.

FUNCTION ID	FUNC-DE-02
Title	Control data export model
Description	This step is required to provide a working configuration, which allows selected control data to be frequently exported to an external storage location. The configuration shall be verified that it does not degrade the performance of the HMI

	unit.
Dependency	All of the following conditions are available. ● The export is to be CSV compatible.. ● External storage configuration is required. ● File name labelling configuration is required. ● Export triggering configuration is required. ● Data points configuration is required.
Results	All available control data is transferred to the external storage location when a triggering event is active.

5.8 Time-Stamping Requirements

The PSS-SIS is required to have time and date stamps for logged alarms and events that are available to the operator for display and data export. This will ensure that items of importance can be viewed in chronological order and correlated with events recorded by other non-SIS systems. Since the SIS network will not have an NTP time source it is expected the time of day (i.e. wall clock time) will drift from the actual time. For timestamp correlation it is important that the SIS time can be correlated in some way.

A (SIS) time of day fiducial shall be provided to the CCS and is described in FUNC-CCS-09.

5.9 Testing Requirements

In order to validate the control program and CHMI, the SIS development process includes a series of testing steps to thoroughly verify the software and its functionalities. The tests will address the requirements in this document as well as the higher-level requirements [2,4]. To achieve objectivity, the tests will be directed by staff that did not program/code the software. The test methods will include:

- Simulated Verification
- Physical Verification
- Non-Functional Verification

Software testing shall be performed through one or more Preoperational Test Procedures (PTP). To fulfill SQA requirements, separate test plans will be developed [9, 10]; these will provide a full description and scope of software test plans. Note that the software will be used (tested again) in higher-level PSS and NSTX-U PTP and ISTP.

- Simulated input and output verification
- Simulated control program verification
- Actual input and output verification
- Final control program verification

5.9.1 Non-Functional Requirements Verification

The system's test plans shall include verification that the non-functional requirements in this document are performing adequately.

5.10 Business Rules

It is required that all PPPL Policies and Procedures must be followed. No exceptions are anticipated. Where exceptions are necessary, the documented exception-approval process must be followed.

6. Appendices

- **Appendix A: Minimum One Device is Safe Criteria**

Appendix A: Minimum One Device is Safe Criteria

Table A-1 The conditions required to present a SAFE condition within the NSTX-U Test Cell, and for the MER Mezzanine.

- At a minimum, for each system, at least one device must be in its safe position to prevent a hazard within the area.
- All systems must be safe for the area to be considered safe.

System	Safe criteria	device 1	device 2	device 3 (open)	device 4 (open)	device 5 (open)
TF Coil	device 1, 2, 3, or 4	ETF1-SDS ground switch closed	ETF1-SDS-1 line switch open	ESV1-SB01	ESF1-SB01	
	device 1, 2, 3, or 4		ETF1-SDS-2 line switch open	ESV1-SB02		
	device 1, 2, 3, or 4		ETF1-SDS-3 line switch open	ESV1-SB03		
	device 1, 2, 3, or 4		ETF1-SDS-4 line switch open	ESV1-SB04		
OH coil	device 1, or 2, or all items in 3 , or 4	ETF2-SDS ground switch closed	ETF2-SDS-1 line switch open	ESV2-SB01 and ESV2-SB02 and ESV2-SB03		
PF1AU	device 1, 2, 3, or 4	EOH1-SDS ground switch closed	EOH1-SDS-1 line switch open	ESV1-SB08		
PF1AL	device 1, 2, 3, or 4	EEF1-SDS ground switch closed	EEF1-SDS line switch open	ESV2-SB07		
PF1BU	device 1, 2, 3, or 4	EHF-SDS ground switch closed	ETF2-SDS-2 line switch open	ESV2-SB05		
PF1BL	device 1, 2, 3, or 4	EF/OH-SDS ground switch closed	ETF2-SDS-4 line switch open	ESV2-SB04		

PF1CU	device 1, or 2, or all items in 3 , or 4	EEF4-SDS ground switch closed	EEF4-SDS-1 line switch open	ESV2-SB07 and ESV2-SB12	ESF1-SB01	
PF1CL	device 1, or 2, or all items in 3 , or 4	EEF3-SDS ground switch closed	EEF3-SDS-1 line switch open	ESV2-SB06 and ESV2-SB12		
PF2U	device 1, or 2, or all items in 3 , or 4	EOH5-SDS ground switch closed	EOH5-SDS-1 line switch open	ESV1-SB09 and ESV2-SB09		
PF2L	device 1, 2, 3, or 4	EOH3-SDS ground switch closed	EOH3-SDS-1 line switch open	ESV1-SB12		
PF3U	device 1, or 2, or all items in 3 , or 4	EOH2-SDS ground switch closed	EOH2-SDS-1 line switch open	ESV1-SB07 and ESV1-SB12		
PF3L	device 1, or 2, or all items in 3 , or 4	EOH4-SDS ground switch closed	EOH4-SDS-1 line switch open	ESV1-SB07 and ESV2-SB09		
PF4U/L	device 1, or 2, or all items in 3 , or 4	EEF2-SDS ground switch closed	EEF2-SDS-1 line switch open	ESV1-SB06 and ESV2-SB05		
PF5U/L	device 1, 2, 3, or 4	EOH6-SDS ground switch closed	EOH6-SDS-1 line switch open	ESV1-SB09		

table A-1 continued next page -->

System	Safe criteria	device 1	device 2	device 3 (open)	device 4 (open)	device 5 (open)
NB1A	device 1, or 2, or all items in 3, or 4, or 5	Pringle ground switch closed	Ross ground switch closed	ESF1-SB10 and ESV2-SB11	ESF2-SB05	ESF1-SB01
NB1B		Pringle ground switch closed	Ross ground switch closed			
NB1C		Pringle ground switch closed	Ross ground switch closed			
NB2A		Pringle ground switch closed	Ross ground switch closed	ESF1-SB10 and ESV2-SB10		
NB2B		Pringle ground switch closed	Ross ground switch closed			
NB2C		Pringle ground switch closed	Ross ground switch closed			

Table A-2 The conditions which present a SAFE condition for the Cable Spread Room and the Test Cell Basement caged area..

- At a minimum, for each system, at least one device must be in its safe position to prevent a hazard within the area.
- All systems must be safe for the area to be considered safe.

System	Safe criteria	device 1	device 2	device 3 (open)	device 4 (open)
TF Coil	device 1, 2, 3, or 4	ETF1-SDS ground switch closed	ETF1-SDS-1 line switch open	ESV1-SB01	ESF1-SB01
	device 1, 2, 3, or 4		ETF1-SDS-2 line switch open	ESV1-SB02	
	device 1, 2, 3, or 4		ETF1-SDS-3 line switch open	ESV1-SB03	
	device 1, 2, 3, or 4		ETF1-SDS-4 line switch open	ESV1-SB04	
OH coil	device 1, or 2, or all items in 3, or 4	ETF2-SDS ground switch closed	ETF2-SDS-1 line switch open	ESV2-SB01 and ESV2-SB02 and ESV2-SB03	
PF1AU	device 1, 2, 3, or 4	EOH1-SDS ground switch closed	EOH1-SDS-1 line switch open	ESV1-SB08	
PF1AL	device 1, 2, 3, or 4	EEF1-SDS ground switch closed	EEF1-SDS line switch open	ESV2-SB07	
PF1BU	device 1, 2, 3, or 4	EHF-SDS ground switch closed	ETF2-SDS-2 line switch open	ESV2-SB05	

table A-2 continued next page -->

System	Safe criteria	device 1	device 2	device 3 (open)	device 4 (open)
PF1BL	device 1, 2, 3, or 4	EF/OH-SDS ground switch closed	ETF2-SDS-4 line switch open	ESV2-SB04	ESF1-SB01
PF1CU	device 1, or 2, or all items in 3, or 4	EEF4-SDS ground switch closed	EEF4-SDS-1 line switch open	ESV2-SB07 and ESV2-SB12	
PF1CL	device 1, or 2, or all items in 3, or 4	EEF3-SDS ground switch closed	EEF3-SDS-1 line switch open	ESV2-SB06 and ESV2-SB12	
PF2U	device 1, or 2, or all items in 3, or 4	EOH5-SDS ground switch closed	EOH5-SDS-1 line switch open	ESV1-SB09 and ESV2-SB09	
PF2L	device 1, 2, 3, or 4	EOH3-SDS ground switch closed	EOH3-SDS-1 line switch open	ESV1-SB12	
PF3U	device 1, or 2, or all items in 3, or 4	EOH2-SDS ground switch closed	EOH2-SDS-1 line switch open	ESV1-SB07 and ESV1-SB12	
PF3L	device 1, or 2, or all items in 3, or 4	EOH4-SDS ground switch closed	EOH4-SDS-1 line switch open	ESV1-SB07 open and ESV2-SB09 open	
PF4U/L	device 1, 2, 3, or 4	EEF2-SDS ground switch closed	EEF2-SDS-1 line switch open	ESV1-SB06 open	
PF5U/L	device 1, 2, 3, or 4	EOH6-SDS ground switch closed	EOH6-SDS-1 line switch open	ESV1-SB09 open	