|  |
| --- |
|  |
|  |
|  |
| SOFTWARE Safety Requirements Specification for Personnel Safety System 0 |
|  |

|  | Name | **Role/Title** |
| --- | --- | --- |
| **Owner** | Stuart Birch | Senior Engineer – Personnel Safety Systems, ICS |
| **Author** | Denis Paulic | Deputy Group Leader for Protection Systems Group, ICS |
| **Reviewer** | Morteza Mansouri  Thilo Friedrich  Fan Ye | Lead Integrator Engineer for Safety Critical Systems, ICS  Systems Engineering and Engineering Process Coordinator/Engineer, ICS  PSS Safety Engineer, Isograph Expert, Engineering Safety Consultants Limited, UK |
| **Approver** | Annika Nordt | Group Leader for Protection Systems Group, ICS |

|  |  |
| --- | --- |
| Table of content | Page |

1. Introduction 5

1.1. Scope 5

1.2. Objectives 5

1.3. Inputs 5

1.4. Implementation 5

1.5. Verification and validation strategy 5

2. The Overall Description 6

2.1. Input signals for implementing safety functions and procedures 6

2.2. Actuators for implementing safety functions 8

2.2.1. HV PS contactors 8

2.2.2. HV grounding relay 9

2.2.3. Key exchange solenoid 9

2.3. PSS0 controlled area status 10

2.4. PSS0 Modes of Operation 12

2.4.1. Internal signals for alarm conditions 13

2.4.2. Mode transition diagram 14

2.5. Systems Interfaces 16

2.5.1. Interface between two SIS logic solvers 16

2.5.2. Interface between PSS0 and Interlock PLC 17

2.6. Operator interfaces 17

3. Safety instrumented functions 17

3.1. Safety integrity functional requirements 18

3.2. SIF01 18

3.2.1. Description 18

3.2.2. Hardware setup 19

3.2.3. Requirements 19

3.2.3.1. SIL and response time requirements 19

3.2.3.2. Acknowledgment requirements 19

3.2.3.3. Time delays requirements 19

3.2.3.4. Diagnostic test requirements – inputs 20

3.2.3.5. Diagnostic test requirements – outputs 20

3.2.4. Cause and effect matrix 20

3.2.5. Modes 20

3.2.6. Formal description 20

3.3. SIF02 21

3.3.1. Description 21

3.3.2. Hardware setup 21

3.3.3. Requirements 22

3.3.3.1. SIL and response time requirements 22

3.3.3.2. Acknowledgment requirements 22

3.3.3.3. Time delays requirements 22

3.3.3.4. Diagnostic test requirements – inputs 22

3.3.3.5. Diagnostic test requirements – outputs 22

3.3.4. Cause and effect matrix 22

3.3.5. Modes 23

3.3.6. Formal description 23

3.4. SIF03 23

3.4.1. Description 23

3.4.2. Hardware setup 24

3.4.3. Requirements 24

3.4.3.1. SIL and response time requirements 24

3.4.3.2. Acknowledgment requirements 24

3.4.3.3. Time delays requirements 24

3.4.3.4. Diagnostic test requirements – inputs 24

3.4.3.5. Diagnostic test requirements – outputs 24

3.4.4. Cause and effect matrix 25

3.4.5. Modes 25

3.4.6. Formal description 25

3.5. SIF04 26

3.5.1. Description 26

3.5.2. Hardware setup 27

3.5.3. Requirements 27

3.5.3.1. SIL and response time requirements 27

3.5.3.2. Acknowledgment requirements 27

3.5.3.3. Time delays requirements 27

3.5.3.4. Diagnostic test requirements – inputs 27

3.5.3.5. Diagnostic test requirements – outputs 27

3.5.4. Cause and effect matrix 28

3.5.5. Modes 28

3.5.6. Formal description 28

4. Tools for software development 29

5. Access protection to safety software 29

6. Abbreviations 30

7. References 31

Document Revision history 31

list of tables

Table 1: Input signals for PSS0 SIFs 6

Table 2: HV PS contactor 1 diagnostic signals truth table. 8

Table 3: Output signals for actuating HV PS contactors. 9

Table 4: Output signal for actuating the HV grounding relay. 9

Table 5: Output signal for actuating the Fortress lock solenoid. 10

Table 6: Internal variables for calculating the PSS0 controlled area status. 10

Table 7: PSS0 Modes. 12

Table 8: Internal variables for storing the alarm conditions. 13

Table 9: Transitions between the PSS0 modes. 15

list of Figures

Figure 1: Interconnections between PSS0 modes (mode transition diagram). 15

Figure 2: Signals exchange between red and blue trains. 16

Figure 3: Logical representation of PSS0 SIFs. 18

Figure 4: Hardware setup for PSS0 SIF01. 19

Figure 5: Cause and effect matrix for PSS0 SIF01. 20

Figure 6: Hardware setup for PSS0 SIF02. 21

Figure 7: Cause and effect matrix for PSS0-SIF02. 22

Figure 8: Hardware setup for PSS0 SIF03. 24

Figure 9: Hardware setup for PSS0 SIF04. 27

# Introduction

## Scope

The scope of this document is limited to the Personnel Safety System 0 (PSS0). It addresses the safety requirements for the application program according to IEC 61511-1 [1] and is specified for all programmable safety instrumented system (SIS) devices necessary to implement required safety instrumented functions (SIFs).

## Objectives

The objectives of this document are:

* To specify the software safety requirements:
  + for each SIS necessary to implement the required safety function;
  + for each safety function allocated to that SIS.
* To specify software performance requirements and design constraints.
* To specify the functional software requirements for the SIS and each SIF.

## Inputs

The inputs to this document are defined in following documents:

* Safety requirement specification (SRS) for PSS0 [2].
* Safety integrity level (SIL) assessment report [3].
* Hardware design specification [4].

## Implementation

To implement the objectives, the following items shall be included:

* The SIFs to be implemented;
* Safety integrity level (SIL) requirements;
* All modes of operation for each SIF;
* Equipment and operator interfaces for each SIF;
* Program sequences and time delays (if applicable in this phase);
* Requirements on response time, self-diagnostic/monitoring, support for proof test, monitoring/validating process variables, response in case of detected faults of equipment.
* Actions to be taken on bad process variable such as sensor value out of range, excessive rate of change, frozen value, detected open circuit, detected short circuit, etc.

## Verification and validation strategy

The verification activities for PSS0 application program are covered in the validation and verification plan document [5].

# The Overall Description

The functional requirements for each safety instrumented function (SIF) are described in the SRS [2]. All hardware devices (sensors, logic solvers, actuators) are described in the Hardware design specification document . This chapter gives an overview of required input and output signals, states of the actuators and PSS0 controlled area, a description of PSS0 modes of operation and description of interfaces that shall be included in designing the safety software. A list of internal signals that should be included in software design to facilitate understanding of certain conditions is also provided in this chapter.

## Input signals for implementing safety functions and procedures

The table below shows the input signals that shall be used for implementing the PSS0 safety instrumented functions. They are extracted from the I/O list in the PSS0 electrical circuit diagrams [6]. As described in [4], the PSS0 SIS logic solver is a two-train system, meaning that the safety system is realised through two technically independent PLC chains called red and blue system. The red train runs complete PSS0 software, including all non-safety functions, whilst the blue system only includes the safety part. If the signal is used only by one train, it is marked accordingly with red or blue colour.

Table 1: Input signals for PSS0 SIFs

| Variable | Description | Source |
| --- | --- | --- |
| AccesDoorClosed | This signal indicates the position of Access door.  **AccesDoorClosed = TRUE** 🡪 Access door is closed | Mechanical and magnetic safety position switches |
| HVOFFButton | This signal indicates the status of the ISrc HV OFF button.  **HVOFFButton = TRUE** 🡪 ISrc HV OFF button is not pressed | Contacts inside the ISrc HV OFF button |
| FortressLock | This signal is called the safety circuit and indicates the status of mechanical and electronic locks for the Access door.  **FortressLock = TRUE 🡪** Access door is mechanically and electronically locked. | Fortress proLok |
| AccessKey | This signal indicates the position of the Access key in the key exchange box.  **AccessKey = TRUE** 🡪 Access key is in ON position. | Key exchange box position monitoring switches |
| HVGroundingRelay | This signal indicates the position of the HV grounding relay.  **HVGroundingRelay = TRUE** 🡪 The HV grounding relay is connected to earth. | HV grounding relay |
| HVGroundingRelayContactor | This signal indicates the status of the relay for controlling the HV grounding relay.  **HVGroundingRelayContactor = TRUE** 🡪 The grounding relay is not requested to disconnect from earth. | Contactor relay for moving the HV grounding relay |
| IsrcHVPSContRelay1Status | This signal indicates the status of the relay for controlling the HV PS contactors from the red train.  **IsrcHVPSContRelay1Status = TRUE** 🡪 The HV PS contactors are not requested to energise from red system. | Contactor relay 1 for energising the HV PS contactors |
| IsrcHVPSContRelay2Status | This signal indicates the status of the relay for controlling the HV PS contactors from the blue train.  **IsrcHVPSContRelay2Status = TRUE** 🡪 The HV PS contactors are not requested to energise from blue system. | Contactor relay 2 for energising the HV PS contactors |
| ISrcHVPSContactor1NO | These signals indicate the status of the HV PS Contactor 1.  **ISrcHVPSContactor1NO = TRUE and**  **ISrcHVPSContactor1NC = FALSE\* 🡪** The HV PS contactor 1 is energised | HV PS contactor 1 |
| ISrcHVPSContactor1NC |
| ISrcHVPSContactor2NO | These signals indicate the status of the HV PS Contactor 2.  **ISrcHVPSContactor2NO = TRUE and**  **ISrcHVPSContactor2NC = FALSE\* 🡪** The HV PS contactor 2 is energised | HV PS contactor 2 |
| ISrcHVPSContactor2NC |
| SearchButton1 | This signal indicates that the search button 1 is pressed.  **SearchButton1 = TRUE** 🡪 Search button 1 pressed. | Search button 1 |
| SearchButton2 | This signal indicates that the search button 2 is pressed.  **SearchButton2 = TRUE** 🡪 Search button 2 pressed. | Search button 2 |
| GroundingRod | This signal indicates that the grounding rod is in its place, behind the Access door.  **GroundingRod = TRUE** 🡪 Grounding rod in place. | Mechanical position switch |

\*Note: Other combinations are described in next section.

## Actuators for implementing safety functions

The operating states of the actuators are used as conditions to calculate the active mode of operation for PSS0 system. Below are listed the SIS actuators, with corresponding output signals and important functional specifications to be included in the software design.

### HV PS contactors

These devices are power contactors controlled by both SIS logic solvers (red and blue train) through control coils (one per contactor). It is assumed that each contactor has a unique and non-variable safe state, which is the open (de-energised). If any contactor is out-of-order, the maintenance shall be allowed only if both contactors are in the safe state. The red logic solver shall read two diagnostic feedback signals from each contactor (four in total), whilst the blue one shall read one signal from each contactor, as shown below (see Table 1 for description of signals):

* To red train:
  + Normally closed contact from contactor 1 (ISrcHVPSContactor1NC)
  + Normally open contact from contactor 1 (ISrcHVPSContactor1NO)
  + Normally closed contact from contactor 2 (ISrcHVPSContactor2NC)
  + Normally open contact from contactor 2 (ISrcHVPSContactor2NO)
* To blue train:
  + Normally open contact from contactor 1 (ISrcHVPSContactor1NO)
  + Normally open contact from contactor 2 (ISrcHVPSContactor2NO)

Table 2 shows all possible combinations of feedback signals for HV PS contractor 1. Analogously, the same is valid for HV PS contactor 2 and relevant diagnostic feedback signals.

Table 2: HV PS contactor 1 diagnostic signals truth table.

|  |  |  |
| --- | --- | --- |
| **ISrcHVPSContactor1NC** | **ISrcHVPSContactor1NO** | **HV PS contactor 1** |
| TRUE | TRUE | Unexpected combination.\* |
| TRUE | FALSE | Open, de-energised. |
| FALSE | TRUE | Closed, energised. |
| FALSE | FALSE | Unexpected combination.\* |

\*Note: This combination is only possible in case of a failure of the HV PS contactor 1.

This means that at any point both trains shall know the status of both HV PS contactors, which is used to calculate the state of PSS0 controlled area, as described in section 2.3. The contactors are actuated through contactor relays (one per train), using the output signals listed in table below.

Table 3: Output signals for actuating HV PS contactors.

|  |  |  |
| --- | --- | --- |
| **Variable** | **Description** | **Diagnostic feedback signals** |
| ISrcHVPSContactRelay1 | This signal energises the contactor relay 1, which is used for actuating the HV PS contactors from the red train.  **ISrcHVPSContactRelay1** **= TRUE** 🡪 The request to energise the HV PS contactors is active from red system. | HV PS contactors energised (closed):  **ISrcHVPSContactor1NC = FALSE**  **ISrcHVPSContactor1NO = TRUE**  **ISrcHVPSContactor2NC = FALSE**  **ISrcHVPSContactor2NO = TRUE** |
| ISrcHVPSContactRelay2 | This signal energises the contactor relay 2, which is used for actuating the HV PS contactors from the blue train.  **ISrcHVPSContactRelay2** **= TRUE** 🡪 The request to energise the HV PS contactors is active from blue system. |

### HV grounding relay

This device is a gravity-return type of a high voltage relay. It is controlled by the red train logic solver within the SIS, through the contactor relay using the output signal described in Table 4. Its default position (i.e. in case of power failure) is closed position (connected to earth), and it is assumed to be a unique and non-variable safe state. Required maintenance is allowed only if the HV PS contactors are in safe state. Diagnostic feedback is delivered to both trains, through the normally closed signal “HVGroundingRelay”, and is used for calculating the state of PSS0 controlled area.

Table 4: Output signal for actuating the HV grounding relay.

|  |  |  |
| --- | --- | --- |
| **Variable** | **Description** | **Diagnostic feedback signals** |
| HVGroundingRelayContactor | This signal energises the contactor relay, which is used for actuating the HV grounding relay from the red train.  **HVGroundingRelayContactor = TRUE** 🡪 The request to disconnect the HV grounding relay is active. | HV grounding relay disconnected:  **HVGroundingRelay = FALSE** |

### Key exchange solenoid

For locking the Access door, a heavy duty, solenoid-controlled switch interlock unit is used. The unit has two layers of locking mechanisms: one purely mechanical, using the trapped key interlock sequence; and an electronic lock which can be applied by acting on the solenoid inside the unit. This solenoid is controlled only by the red train logic solver, using the output signal described in Table 5. It is assumed that it has a unique safe state, which is when mechanical tounge from the Access door is inserted in the lock, the Safety key is in place (see [7]) and solenoid is de-energised. In this state the Access door is considered electronically and mechanically locked. The diagnostic feedback is read by both trains, through the normally closed signal “FortressLock”, and is used for evaluating the state of the PSS0 controlled area in different operating modes.

Table 5: Output signal for actuating the Fortress lock solenoid.

|  |  |  |
| --- | --- | --- |
| **Variable** | **Description** | **Diagnostic feedback signals** |
| FortressLockSolenoid | This signal energises the key exchange solenoid from the red train.  **FortressLockSolenoid = TRUE** 🡪 The request to electronically unlock the Access door is active. | Access door locked mechanically and electronically:  **FortressLock = TRUE** |

## PSS0 controlled area status

The PSS0 controlled area status shall be calculated in the software in two different ways, based on safety and functional requirements. From a safety point of view it can be either safe or unsafe to access, whilst from procedural point of view it can be either searched or not searched, as required by the formalised search procedure (see [7]). To calculate and store the status of the PSS0 controlled area, the following internal variables should be defined:

Table 6: Internal variables for calculating the PSS0 controlled area status.

|  |  |  |
| --- | --- | --- |
| **Variable** | **Description** | **Main conditions** |
| SearchButton1Armed  SearchButton2Armed | These variables indicate that the specific button has been pressed in correct order\* (see [7]), whilst the search procedure is on-going.  **SearchButton1Armed = TRUE** 🡪 The search button one is pressed and the search process has started.  **SearchButton2Armed = TRUE** 🡪 The search process is ongoing and search button 2 has been pressed. | * Search mode (see section 2.4) |
| AreaSearched | This variable indicates that the formalised search process has been carried out and there are no people left in PSS0 controlled area.  **AreaSearched = TRUE** 🡪 The PSS0 controlled area is searched. | * Search buttons armed.   **SearchButton1Armed = TRUE**  **SearchButton2Armed = TRUE**   * Grounding rod in place.   **GroundingRodPosition = TRUE**   * Access door closed.   **AccesDoorClosed = TRUE** |
| AreaSafeToAccess | This variable represents the safe state of the PSS0 controlled area, meaning that no hazard is present and it can be accessed.  **AreaSafeToAccess = TRUE** 🡪 The PSS0 controlled area is safe to access. | * HV PS contactors de-energised.   **ISrcHVPSContactor1NC = TRUE**  **ISrcHVPSContactor1NO = FALSE**  **ISrcHVPSContactor2NC = TRUE**  **ISrcHVPSContactor2NO = FALSE**   * HV grounding relay connected to earth.   **HVGroundingRelay = TRUE**   * Contactor relays for actuating HV PS contactors and HV grounding relay de-energised.   **ISrcHVPSContactRelay1 = TRUE**  **ISrcHVPSContactRelay2 = TRUE**   * Access key not in the key exchange box position ON.   **AccessKey = FALSE** |
| AreaReadyForPermit | This variable represents the unsafe state of the PSS0 controlled area, meaning that the area is ready for allowing operation of HV PS.  **AreaReadyForPermit = TRUE** 🡪 The PSS0 controlled area is not safe to access. | * HV grounding relay not connected to earth.   **HVGroundingRelay = FALSE**   * Area searched.   **AreaSearched = TRUE**   * Access door mechanically and electronically locked.   **FortressLock = TRUE** |

\*Note: If the search buttons are not pressed in correct order, i.e. Search button 2 pressed before the Search button 1, the system shall not react. This means that the Search button 1 shall always armed (pressed) first and pressing of Search button 2 shall be enabled 15 seconds (see [7]) after the Search button 1 is armed. This should be included software tests.

## PSS0 Modes of Operation

The PSS0 operates in five modes (see Table 7) to ensure safe access to PSS0 controlled, and that required procedures (see [7]) are carried out in a controlled way and in the right order.

Table 7: PSS0 Modes.

| **Mode** | **Description** | **Main conditions** |
| --- | --- | --- |
| **HV ON** | In this mode, a permit is issued from the PSS0 system to energise the HV PS (ISrc and LEBT test stand operation is allowed). This means that the PSS0 controlled area has been searched to make sure there is nobody left inside, the Access door is locked, warning lights are on to alert people about existing hazards and all hazardous equipment is allowed to be energised. | * Area searched   **AreaSearched = TRUE**   * Area ready for permit (unsafe to access)   **AreaReadyForPermit = TRUE**   * HV PS contactors energised (actuated)   **ISrcHVPSContactor1NC = FALSE**  **ISrcHVPSContactor1NO = TRUE**  **ISrcHVPSContactor2NC = FALSE**  **ISrcHVPSContactor2NO = TRUE**   * Warning lights |
| **Transition** | This is a transition mode between Search and HV ON modes in the process of energising the HV PS [7] to ensure that the PSS0 controlled area is ready for energising the HV PS and that a permit to energise the HV PS is issued.  It is also used in the other direction when transitioning between HV ON and Access mode, to ensure that the procedure for enabling access to the PSS0 controlled area is followed. | * Area searched   **AreaSearched = TRUE**   * Area unsafe for access and Access door not locked through the solenoid.   **HVGroundingRelay = FALSE**  **FortressLock = FALSE**   * Access key not in position ON   **AccessKey = FALSE** |
| **Access** | This is a mode where the PSS0 controlled area is considered safe and access is allowed. A permit to energise the HV PS is removed, search is broken upon entry and all warning lights are off. | * Area safe to access   **AreaSafeToAccess = TRUE**   * Area not searched   **AreaSearched = FALSE**   * Access key not in position ON   **AccessKey = FALSE** |
| **Search** | This mode is used to control the formalised search procedure (see [7]) and is required every time before starting the HV PS if the PSS0 controlled area has been accessed. | * Area safe to access   **AreaSafeToAccess = TRUE**   * Access key not in position ON   **AccessKey = FALSE**   * Search button 1 armed   **SearchButton1Armed = TRUE**   * Search button 2 can be armed after a delay of 15 seconds upon the button 1 is being armed. |
| **Alarm** | This is a fall-back mode of the system in case something unexpected has happened, e.g. internal PSS0 PLC dangerous error, PSS0 PLC re-start, ISrc HV OFF button pressed in any mode, intrusion into PSS0 area, etc. | * Start-up OR Active alarm (see section below) * Permits to energise HV PS contactors removed   **ISrcHVPSContactor1NC = TRUE**  **ISrcHVPSContactor1NO = FALSE**  **ISrcHVPSContactor2NC = TRUE**  **ISrcHVPSContactor2NO = FALSE** |

### Internal signals for alarm conditions

Table 8: Internal variables for storing the alarm conditions.

|  |  |  |
| --- | --- | --- |
| **Variable** | **Description** | **Main conditions** |
| CriticalAlarm | This variable indicates that a specific condition occurred that required the system to transition to the alarm mode and remove the permits to allow operation.  **CriticalAlarm = TRUE** 🡪 A critical alarm condition is active. | One of following conditions is active:   * ISrc HV OFF button pressed (see SIF01) * Intrusion detected (see SIF02) * PSS0 SIS hardware error |
| StartUp | This variable indicates that system has been powered up (started) or restarted.  **StartUp = TRUE** 🡪 The PSS0 system has just been started-up or restarted. | * System restart variable active (this variable shall be TRUE by default upon system restart). |
| AlarmAckRequired | This variable shows if the alarm acknowledgment is required. The acknowledgment is enabled only if the alarm is not active anymore.  **AlarmAckRequired = TRUE\*** 🡪 The active alarm shall be reset by the operator. | * Critical alarm has been active. |
| SearchError | This variable indicates that a formalised search procedure took too long and needs to be re-done. It will bring the system back to Access mode and acknowledgment is not required.  **SearchError = TRUE\*\*** 🡪 Search procedure time limit exceeded. | * Search on-going and timer for search procedure exceeded 60 seconds. |

\*Note: Resetting of “AlarmAckRequired” signal shall be included in software tests.

\*\*Note: This variable shall not be treated as an alarm and shall not trigger transition to Alarm mode. It shall be used to notify the operator that search procedure should be re-done.

### Mode transition diagram

Figure 1 shows transitions between the PSS0 modes, where green arrows represent the direction from the HV ON to Access mode, and blue arrows show the opposite direction. All unexpected events that require safe state of the PSS0 controlled area shall bring the system to Alarm mode and these transitions are marked red. If the system is in Alarm mode, upon removing the alarm condition, it can only transition to Access mode, which is a safe system’s mode. This diagram shall be used as a basis for developing a detailed PSS0 state machine diagram used in PSS0 software, and the required transition conditions between the modes are shown in Table 9.

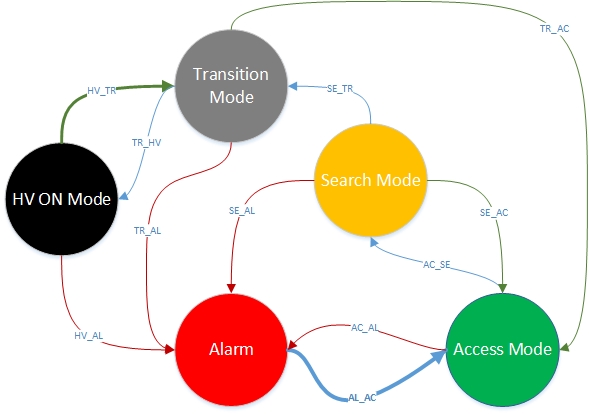


Figure 1: Interconnections between PSS0 modes (mode transition diagram).

Table 9: Transitions between the PSS0 modes.

|  |  |
| --- | --- |
| Transition | Description / Conditions |
| Startup | Upon start-up, the system shall be in the Alarm mode  **StartUp = TRUE** |
| AL\_AC | No active alarms AND  Alarms and start-up acknowledged AND  Area safe to access  **CriticalAlarm = FALSE AND AlarmAckRequired = FALSE AND AreaSafeToAccess = TRUE** |
| AC\_SE | Search button 1 pressed (armed) AND  Area safe to access  **SearchButton1Armed = TRUE AND AreaSafeToAccess = TRUE** |
| SE\_TR | Area searched  **AreaSearched = TRUE** |
| TR\_HV | Area ready for permit AND  Access key in ON position  **AreaReadyForPermit = TRUE AND AccessKey = TRUE** |
| HV\_TR | Access key removed from ON position  **AccessKey = FALSE** |
| TR\_AC | Area not searched - Access door opened  **AccesDoorClosed = FALSE(**AreaSearched = FALSE**)** |
| AC\_AL | Area not safe to access OR  ISrc HV OFF button pressed OR  Alarm in the other train (see section below)  **AreaSafeToAccess = FALSE OR CriticalAlarm=TRUE OR Red/BlueSystemOK = FALSE** |
| SE\_AL | Area not safe to access OR  ISrc HV OFF button pressed OR  Alarm in the other train (see section below)  **AreaSafeToAccess = FALSE OR CriticalAlarm=TRUE OR Red/BlueSystemOK = FALSE** |
| HV\_AL | Area not ready for permit OR  ISrc HV OFF button pressed OR  Alarm in the other train (see section below)  **AreaReadyForPermit = FALSE OR CriticalAlarm=TRUE OR Red/BlueSystemOK = FALSE** |
| TR\_AL | ISrc HV OFF button pressed OR  Alarm in the other train (see section below)  **CriticalAlarm=TRUE OR Red/BlueSystemOK = FALSE** |
| SE\_AC | Search error  **SearchErrror = TRUE** |

## Systems Interfaces

### Interface between two SIS logic solvers

Although the red and blue trains do not communicate directly with each other, there should be the possibility to know if the interlock is active or if the status is ok in the other train. For that purpose red and blue trains shall exchange the data through hard-wired signals, which shall be connected to standard DI/DO modules in each train, as shown below:

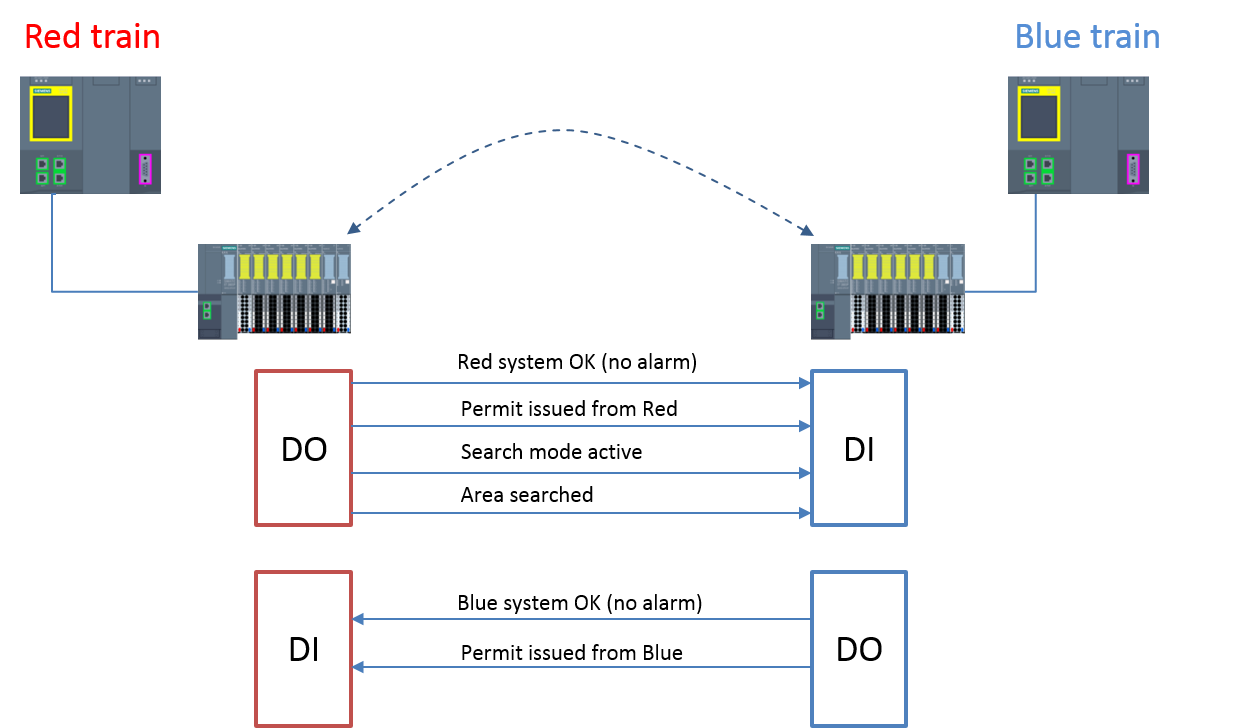


Figure 2: Signals exchange between red and blue trains.

If one train is in alarm mode, the other train shall be informed through the “Red/blue system OK“ signal and transition immediately to alarm mode upon detecting it, independently of currently active mode.

The permit to energise the HV PS contactors shall be considered active only if it is active in both trains, which is communicated between the trains through “Permit issued from Red/Blue” signals (see picture above).

### Interface between PSS0 and Interlock PLC

This interface is described in the Interface control document for PSS0 and Ion source [9]. To inform the Interlock PLC that PSS0 permit is issued the “ToInterlockPLCPSSpermit” shall used. It shall be TRUE if the permit from both trains is issued.

## Operator interfaces

Each train has its own operator interface, realised through Siemens human machine interface (HMI) touch panels (see [4]). As part of this interface, the status of the SIS critical to maintain the SIL shall be available. This includes the following as a minimum:

* current PSS0 mode of operation for each train;
* indication that SIS protective action (SIF) has occurred;
* feedback about automatic actions in PSS0 procedures;
* status of sensors and final elements;
* the results of diagnostics.

The operator interfaces shall prevent changes to PSS0 software. Where safety information needs to be transmitted to the SIS (i.e. alarm acknowledgment), it shall be documented and tested to make sure it cannot lead the system to an unsafe state.

# Safety instrumented functions

This chapter is focused on important requirements from a whole set of SIFs that are necessary for developing PSS0 software. As a main principle, all permits for powering the hazardous equipment shall be removed if the presence of personnel in the PSS0 controlled area is not compatible with current PSS0 operating mode. Analogously, the system shall not issue the permit to energise any hazardous equipment when people are working in the controlled area. The figure below illustrates an overview of the SIFs for PSS0 (see [2]), showing the logical interconnections between the SIFs and SIS actuators.



Figure 3: Logical representation of PSS0 SIFs.

## Safety integrity functional requirements

Below are listed some functional requirements that shall be included in software design to satisfy the system’s safety integrity described in [2]:

* No combination of the interlocks shall prevent the actuators to reach their safe states when requested (when the inputs are valid).
* No combination of the interlocks shall delay the commands to SIS actuators by more than 1 second.
* No combination of the interlocks shall result in an undefined or unstable state of the system.

## SIF01

### Description

The main scope of this function is to ensure that energising the HV PS is not permitted if the ISrc HV OFF button is pressed. Upon detecting input from ISrc HV OFF button, the SIS logic solver shall send the command to switch-off the HV PS and the system shall transition to Alarm mode.

The ISrc HV OFF button control device is monitored by the logic solver. The feedback status from each HV PS contactor is monitored, and if a discrepancy is detected between this feedback and the command sent to switch-off, the system shall report a feedback error on the operator interface.

### Hardware setup

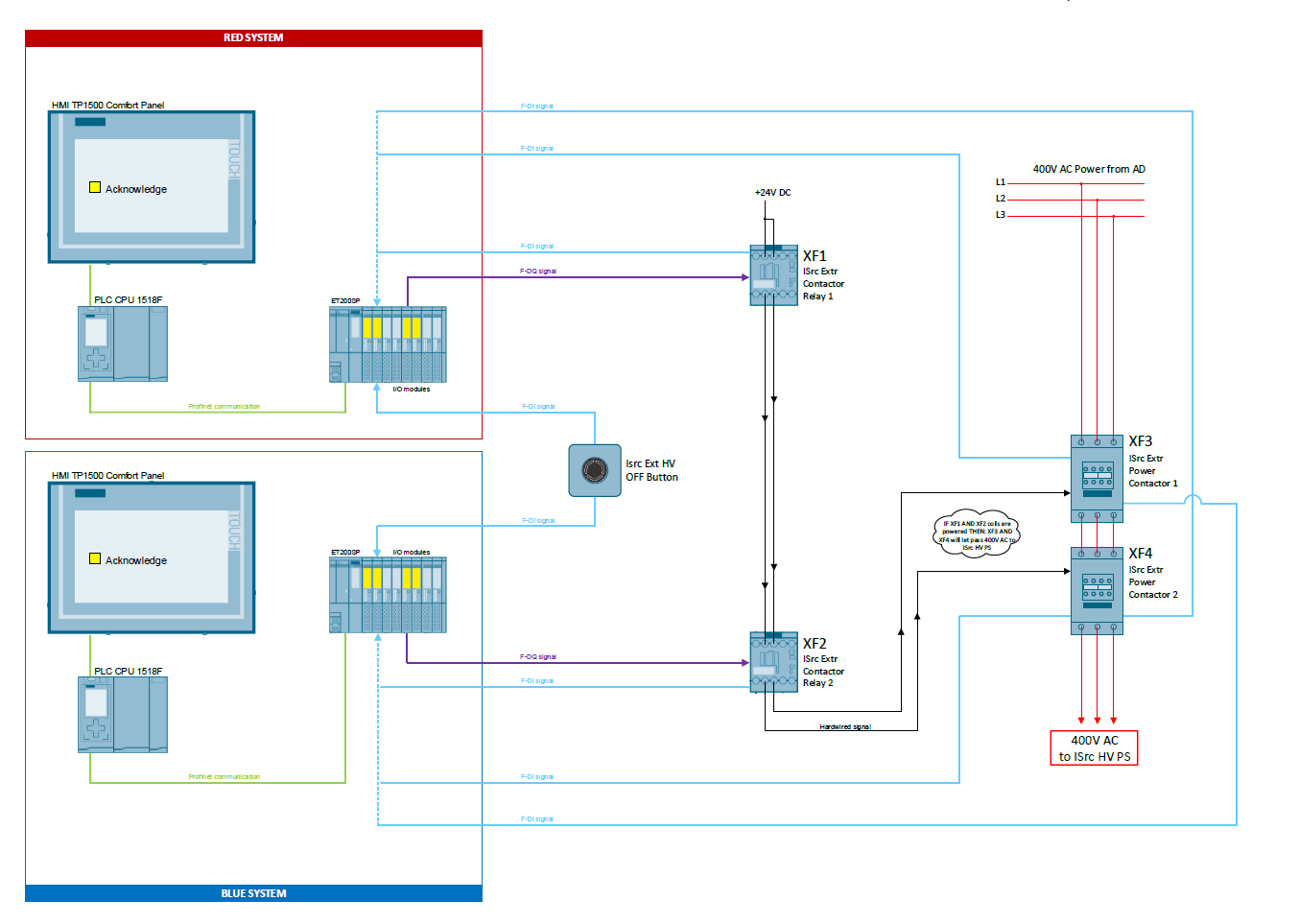


Figure 4: Hardware setup for PSS0 SIF01.

### Requirements

#### SIL and response time requirements

* SIL and response time requirements are defined in the SRS [2].

#### Acknowledgment requirements

* This function shall be manually acknowledged from the operator interface.
* Before acknowledging the alarm, it shall be confirmed whether the contacts of ISrc HV OFF button control device are closed, alarm conditions are ok, and the actuators are switched off.
* A procedure shall be developed to make sure only authorised personnel are allowed to acknowledge alarms and bring the system to Access mode (i.e. alarm acknowledgment shall be password protected).

#### Time delays requirements

* If the ISrc HV OFF button is pressed, the permit to energise the HV PS shall be removed with a delay of 500 ms to avoid damaging the HV PS.

#### Diagnostic test requirements – inputs

* Discrepancy time between reading 2 switches from the ISrc HV OFF control device shall not be greater than 50 ms.
* The short circuit tests on sensor supplies shall be carried out in less than 5 ms.

#### Diagnostic test requirements – outputs

* The following diagnostic test shall be activated for output signals:
  + Wire-break test,
  + Dark test with a read-back time of 1 ms.

### Cause and effect matrix



Figure 5: Cause and effect matrix for PSS0 SIF01.

### Modes

* This function shall be enabled in all PSS0 modes of operation.

### Formal description

|  |
| --- |
| **Formal Description using Plain Text and Boolean formulas:**  *Activation of the Alarm mode and removing the permit to power the HV PS by pressing the ISrc HV OFF button:*   * IF any of 4 NC contact modules inside a ISrc HV OFF button is detected open, indicating that the button has been pressed; * THEN   + Send a command to Interlock PLC to request switching-off of the HV PS (notification that a PSS0 permit is going to be removed).   + Start a timer to count 500 ms for a required time delay.   + Remove the command for energising the HV PS contactors after a time delay exceeds.   + Set the Alarm mode and require acknowledgment.   + Activate the internal signal for critical alarm.   **IF** (HVOFFButton == FALSE) **THEN** (StartTimer500ms = TRUE AND ToInterlockPLCPSSpermit = TRUE)  **IF** (Timer500ms.OK == TRUE)  **THEN** (AlarmMode = TRUE AND CriticalAlarm = TRUE AND ISrcHVPSContactRelay1 = FALSE AND ISrcHVPSContactRelay2 = FALSE AND HVMode = FALSE AND AccessMode = FALSE AND SearchMode = FALSE AND TransitionMode = FALSE) |

## SIF02

### Description

The scope of this function is to monitor the position of the Access door by checking the status of the safety position monitoring switches, for purpose of protecting people from entering the hazardous area. If the function is activated, a permit to energise the HV PS shall be removed, as in case of SIF01.

### Hardware setup

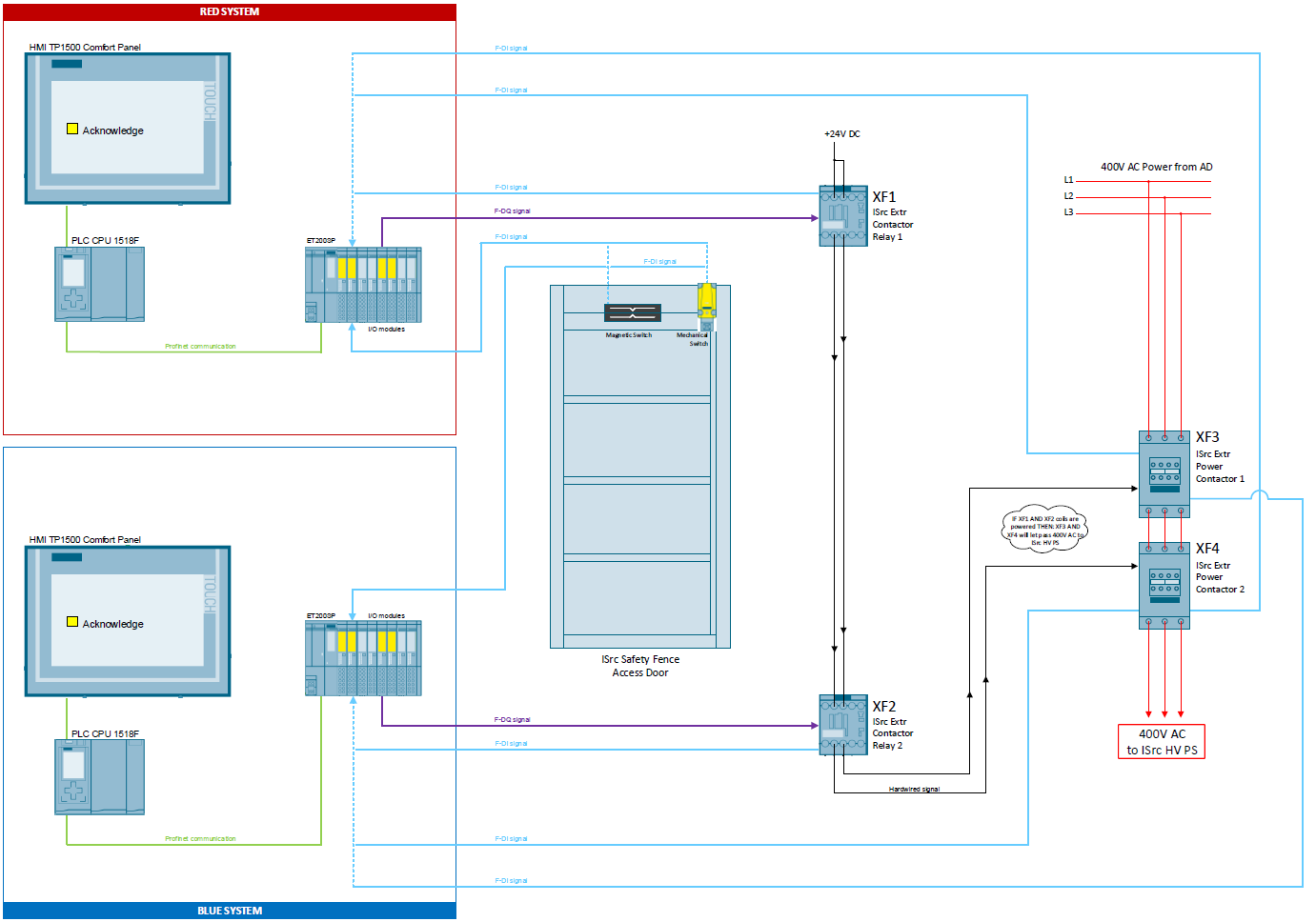


Figure 6: Hardware setup for PSS0 SIF02.

### Requirements

#### SIL and response time requirements

* SIL and response time requirements are defined in the SRS [2].

#### Acknowledgment requirements

* Same as for SIF01.

#### Time delays requirements

* If the intrusion is detected through safety position switches, the permit to energise the HV PS shall be removed with a delay of 500 ms to avoid damaging the HV PS.

#### Diagnostic test requirements – inputs

* Discrepancy time between reading two switches shall not be greater than 700 ms.
* The short circuit tests on sensor supplies shall be carried out in less than 5 ms.

#### Diagnostic test requirements – outputs

* Same as for SIF01.

### Cause and effect matrix



Figure 7: Cause and effect matrix for PSS0-SIF02.

### Modes

This function shall only be valid if the system is in HV ON mode, when any opening of the Access door is considered as an intrusion.

In other modes, the status of the Access door shall only be shown on the operator interface and detection of door opening shall not cause an alarm.

### Formal description

|  |
| --- |
| **Formal Description using Plain Text and Boolean formulas:**  *Activation of the Alarm mode and removing the permit to power the HV PS by opening the Access door in HV ON mode:*   * IF the system is in HV ON mode AND any of the two position monitoring switches is detected open; * THEN   + Send a command to Interlock PLC to request switching-off of the HV PS (notification that a PSS0 permit is going to be removed).   + Start a timer to count 500 ms for a required time delay.   + Remove the command for energising the HV PS contactors after a time delay exceeds.   + Set the Alarm mode and require acknowledgment.   + Activate the internal signal for critical alarm.   **IF** (HVONMode == TRUE AND AccesDoorClosed == FALSE) **THEN** (StartTimer500ms = TRUE AND ToInterlockPLCPSSpermit = TRUE)  **IF** (Timer500ms.OK == TRUE)  **THEN** (AlarmMode = TRUE AND CriticalAlarm = TRUE AND ISrcHVPSContactRelay1 = FALSE AND ISrcHVPSContactRelay2 = FALSE AND HVONMode = FALSE) |

## SIF03

### Description

The Access key is the main input for transitioning to and from the HV ON mode. This function monitors the position of the Access key in the key exchange box and, upon detecting it is removed from the position ON, a permit to energise the HV PS shall be removed and HV PS shall be connected to earth (grounded). The function shall also ensure that a permit can be issued again only if the PSS0 controlled area is ready for permit and the Access key is in position ON.

### Hardware setup

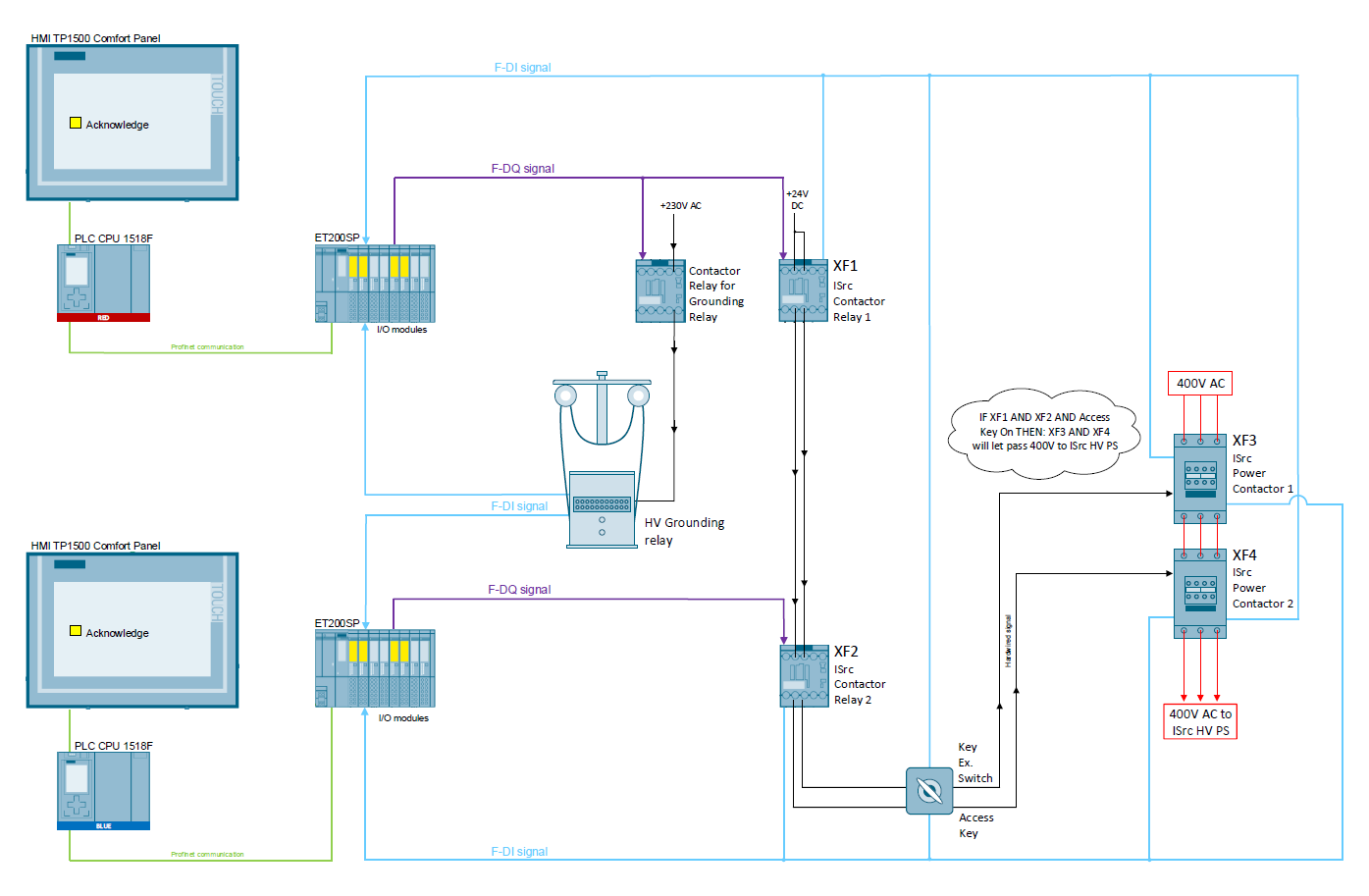


Figure 8: Hardware setup for PSS0 SIF03.

### Requirements

#### SIL and response time requirements

* SIL and response time requirements are defined in the SRS [2].

#### Acknowledgment requirements

* No requirements for acknowledgment upon activating this function.

#### Time delays requirements

* If the Access key is removed from position ON, a permit to energise the HV PS shall be removed with a delay of 500 ms to avoid damaging the HV PS.
* The HV grounding relay shall be connected to earth 500 ms after the HV PS contactors are detected de-energised to avoid having the HV PS grounded whilst the permit to energise is issued.

#### Diagnostic test requirements – inputs

* The short circuit tests on sensor supplies shall be carried out in less than 5 ms.

#### Diagnostic test requirements – outputs

* Same as for SIF01.

### Cause and effect matrix



### Modes

This function shall be enabled in all PSS0 modes of operation.

If the system is in HV ON mode, it follows the standard procedure for de-energising the HV PS by removing the Access key from the position ON in the key exchange box and triggers the system’s transition to Transition mode.

If the Access key is out of position ON, it shall not be possible to issue the permit to energise the HV PS contactors in any PSS0 mode.

### Formal description

|  |
| --- |
| **Formal Description using Plain Text and Boolean formulas:**  *Removing the permit to power the HV PS and connecting the HV PS to earth by removing the Access key from position ON in the key exchange box:*   * IF the system is in HV ON mode AND the Access key is detected removed from position ON in the key exchange box; * THEN   + Send a command to Interlock PLC to request switching-off of the HV PS (notification that a PSS0 permit is going to be removed).   + Start a timer to count 500 ms for a required time delay to remove the permit.   + Remove the command for energising the HV PS contactors after a time delay exceeds.   + Set the Transition mode.   + Start a timer to count 500 ms for a required time delay to connect the HV PS to earth.   **IF** (HVONMode == TRUE AND AccessKey == FALSE) **THEN** (StartTimer1\_500ms = TRUE AND ToInterlockPLCPSSpermit = FALSE)  **IF** (Timer1\_500ms.OK == TRUE)  **THEN** (TransitionMode = TRUE AND ISrcHVPSContactRelay1 = FALSE AND ISrcHVPSContactRelay2 = FALSE AND HVONMode == FALSE)  **IF** (ISrcHVPSContactor1NC == TRUE AND ISrcHVPSContactor1NO== FALSE AND ISrcHVPSContactor2NC == TRUE AND ISrcHVPSContactor2NO == FALSE)  **THEN** (StartTimer2\_500ms = TRUE)  **IF** (Timer2\_500ms.OK == TRUE)  **THEN** (HVGroundingRelayContactor = FALSE)  *Ensuring that a permit to energise the HV PS cannot be issued if the PSS controlled area is not ready and Access key is in position ON:*  **IF** (TransitionMode == TRUE AND AccessKey == TRUE AND AreaReadyForPermit == TRUE)  **THEN** (HVONMode = TRUE AND TransitionMode = FALSE)  **IF** (HVONMode == TRUE)  **THEN** (ISrcHVPSContactRelay1 = TRUE AND ISrcHVPSContactRelay2 = TRUE AND ToInterlockPLCPSSpermit = TRUE)  **IF** (AccessMode == TRUE OR SearchMode == TRUE OR AlarmMode == TRUE) AND (AccessKey == TRUE)  **THEN** (AlarmMode = TRUE AND AccessMode == FALSE AND SearchMode == FALSE) |

## SIF04

### Description

This function has the same input device as SIF03, but different reaction. Upon detecting the Access key is in position ON in the key exchange box, the Access door shall be locked electronically.

### Hardware setup

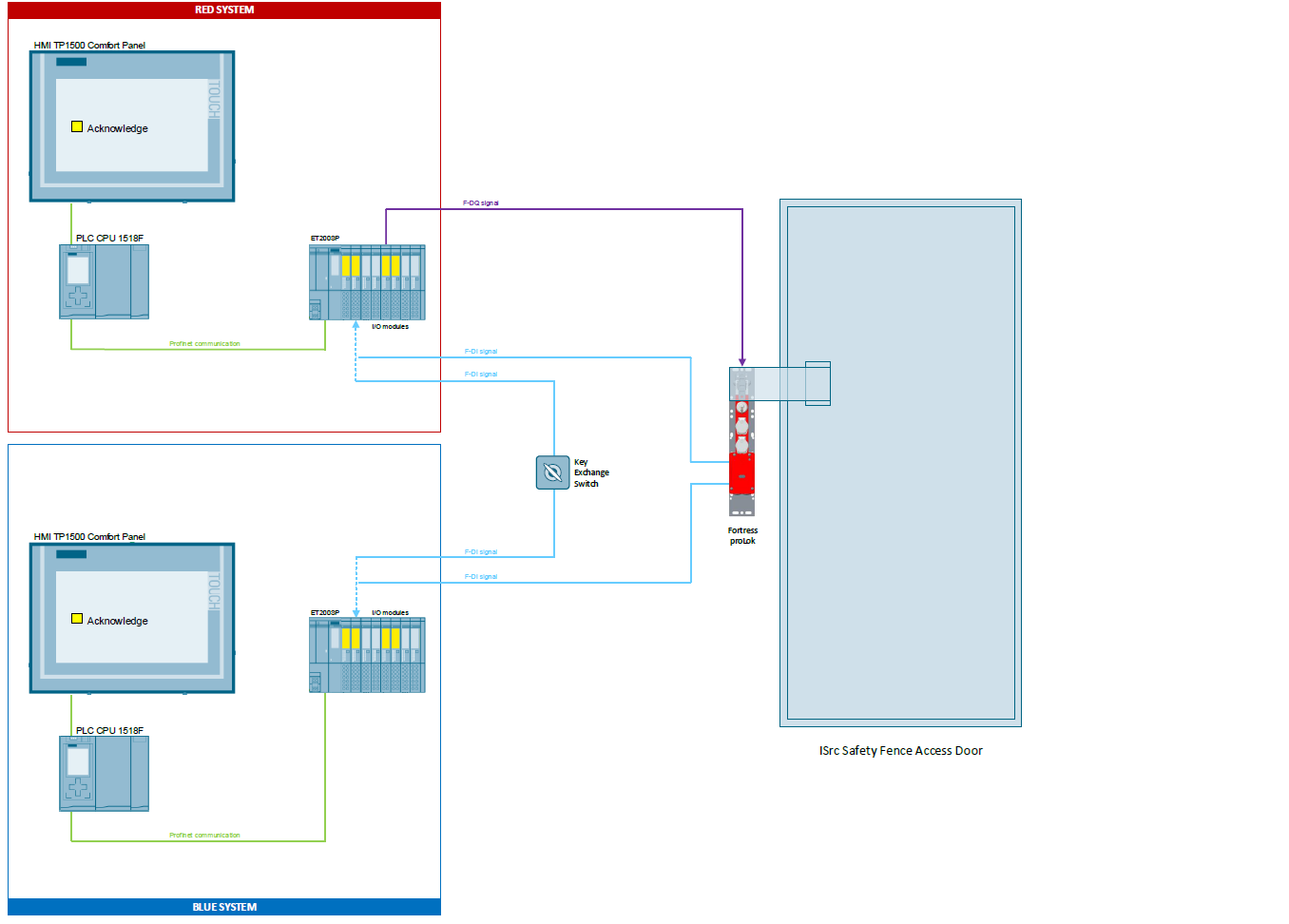


Figure 9: Hardware setup for PSS0 SIF04.

### Requirements

#### SIL and response time requirements

* SIL and response time requirements are defined in the SRS [2].

#### Acknowledgment requirements

* No requirements for acknowledgment upon activating this function.

#### Time delays requirements

* No specific time delay requirements.

#### Diagnostic test requirements – inputs

* Same as for SIF03.

#### Diagnostic test requirements – outputs

* The wire-break test shall be activated.

### Cause and effect matrix



### Modes

This function shall be enabled in all PSS0 modes. Even the action of putting the Access key in position ON if the system is in Access or Search modes shall put the system in Alarm mode, the locking of the Access door shall be carried out independently.

### Formal description

|  |
| --- |
| **Formal Description using Plain Text and Boolean formulas:**  *Locking the Access door electronically by putting the Access key in position ON in the key exchange box and ensuring that locking of Access door cannot be bypassed in procedure for energising the HV-PS:*   * IF the Access key is detected in the position ON in the key exchange box; * THEN   + Send a command to activate the solenoid inside the lock on the Access door. * IF the safety circuit feedback from the Fortress lock is not active; * THEN   + Do not consider PSS0 controlled area ready for issuing a permit.   **IF** (AccessKey == TRUE) **THEN** (FortressLockSolenoid = FALSE)  **IF** (FortressLock == FALSE) **THEN** (AreaReadyForPermit = FALSE) |

# Tools for software development

Below are listed the software tools that shall be used (as a minimum) for implementing the PSS0 software:

* Siemens SIMATIC Step 7 Totally Integrated Automation (TIA) Portal version 14, service pack 1 (v14 SP1)
  + Including the Step 7 Safety Advanced v14 SP1, for programming the safety program.
  + Fulfils all the recommendations from the IEC 61511 standard for software development tools.
* Siemens WinCC Comfort v14 SP1 for developing the HMI.

The engineering workstation for development and maintenance of the PSS0 software shall be a Windows station with one of the following Windows versions (required to run WinCC Comfort v14 SP1):

* + Windows 7 Professional SP1 or Windows 8 Professional
  + Windows 7 Enterprise SP1 or Windows 8 Enterprise
  + Windows 7 Ultimate SP1 or Windows 8 Ultimate
  + Windows 10 Professional Version 1607
  + Windows 10 Enterprise Version 1607

# Access protection to safety software

It is essential to provide access protection in operation mode for the access to the safety part of the software. The access to PSS0 safety software shall be protected by two password prompts: one for the safety program and another for the safety PLC. To optimise the access protection, the passwords for safety PLC and safety program shall be different. To prevent the misuse, the system shall automatically check the collective signature of the safety program (Checksum test) and in case of the software misuse; the system shall go to Alarm mode and PSS0 software developer shall be informed immediately. Note that checksum shall change after any error-free safety software re-generation.

The access protection shall be implemented as soon as the system is considered ready for the site integration test (SIT).

# Abbreviations

ESS European Spallation Source

ES&H Environmental Safety and Health

HMI Human Machine Interface

HV High Voltage

IEC International Electrotechnical Commission

I/O Inputs and Outputs

ICS Integrated Control Systems

ISrc Ion Source

LEBT Low Energy Beam Transport

PLC Programmable Logic Controller

PS Power Supply

PSS Personnel Safety Systems

PSS0 Personnel Safety System 0

SIF Safety Instrumented Function

SIL Safety Integrity Level

SIS Safety Instrumented System

SIT Site Integration Test

SRS Safety Requirement Specification

TIA Totally Integrated Automation

# References

|  |  |
| --- | --- |
| [1] | *IEC 61511:2016 Functional safety - Safety instrumented systems for the process industry sector,* 2016. |
| [2] | F. Ye, “Safety Requirements Specification Document for PSS0 (ESS-0238059),” 2018. |
| [3] | F. Ye, “Safety Integrity Level Assessment Report for PSS0 (ESS-0231390),” 2018. |
| [4] | M. Mansouri, “PSS0 Hardware Design Document (ESS-0237967),” 2018. |
| [5] | P. Skog, “Verification and validation for PSS0 (ESS-0233615),” 2018. |
| [6] | A. Toral, “PSS0 Electrical Circuit Diagrams (ESS-0151602),” 2018. |
| [7] | M. Mansouri, “Concept of Operations For the Accelerator Personnel Safety System 0 (PSS0) (ESS-0134492),” 2018. |
| [8] | E. Sargsyan, “Technical Description of the ESS Normal Conducting Front End (ESS-0159957),” 2018. |
| [9] | M. Mansouri, “Accelerator Personnel Safety System 0 and Ion Source Interface Control Document (ESS-0237562),” 2018. |

Document Revision history

| Revision | Reason for and description of change | Author | Date |
| --- | --- | --- | --- |
| 1 | Template  First version | Paulina Skog  Denis Paulic | 2018-09-21 2018-10-26 |
|  | Implemented comments from F. Ye and updated references. | Denis Paulic | 2018-10-29 |