EUROPEAN
SPALLATION
SOURCE

Document Type	System Architecture Description
Document Number	ESS-0045067
Date	Mar 25, 2019
Revision	5 (7)
State	Review
Confidentiality Level	Internal
Page	1 (26)

TSS System Architecture Specification

	Name	Role/Title
Owner	Mikael Olsson	Control Engineer, Target Controls and Safety, Target Division
Reviewer	Ola Ingemansson	Electrical and Instrumentation Engineer, Target Controls and Safety, Target Division
	Anders Malm	Electrical Engineer, Engineering and Integration Support Division
	Thomas Hansson	Senior Radiation Safety Engineer, ES&H Division
Approver	Linda Coney	Group Leader Target Controls and Safety, Target Division

TABLE OF CONTENT **PAGE**

1. SCOPE

The scope of this document is the system architecture of the Target Safety System (TSS).

The document does not cover detailed system design, such as choice of components, operational modes, response times, etc.

To get a more general overview and overall understanding of TSS, see ESS-0037596 [1].

This document is written to accommodate lifecycle phase 4 (clause 11) of IEC 61511-1 [2], see Figure 1.

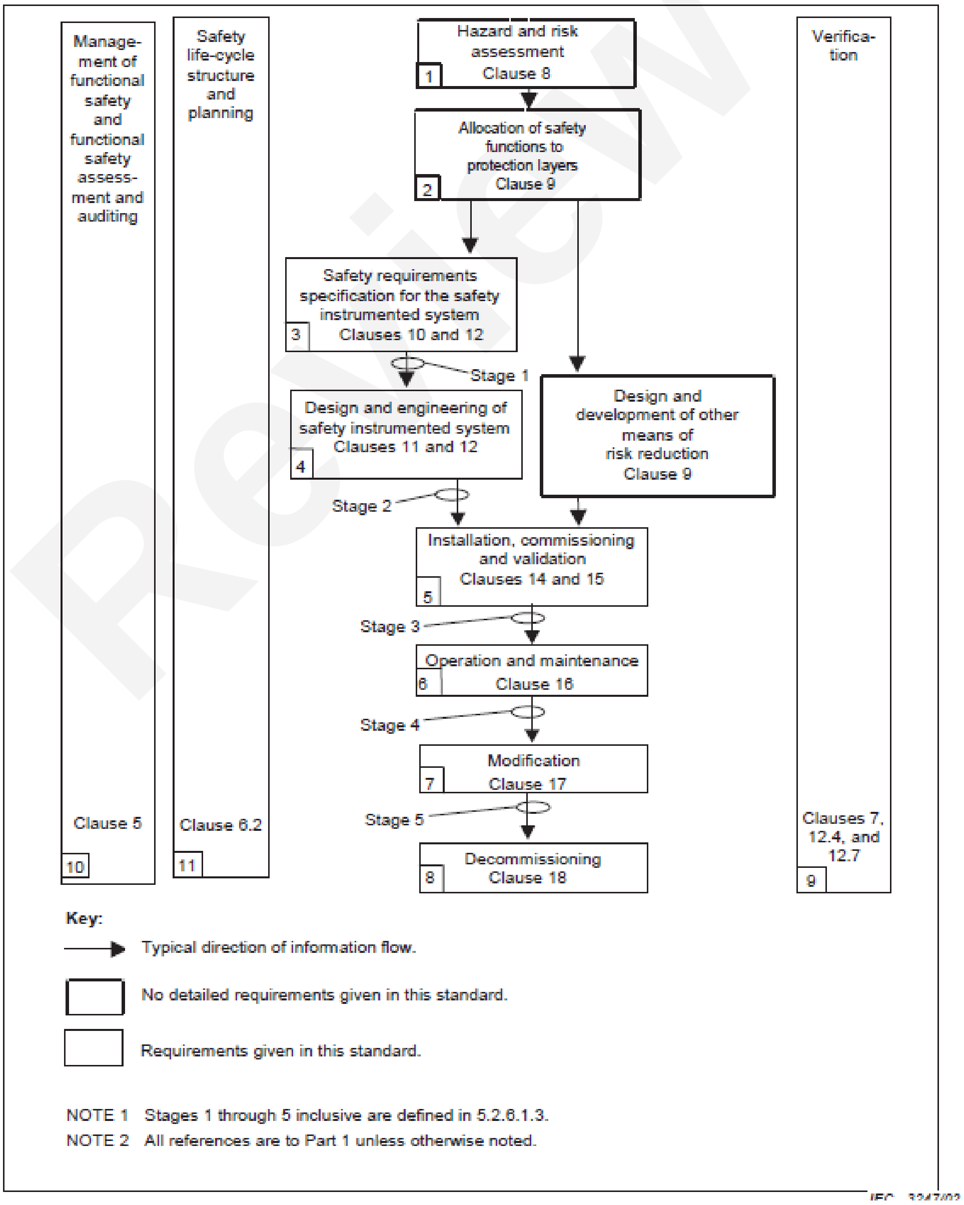

Manage-ment of functional safety and functional safety assess-ment and auditing
Clause 5
10
Safety life-cycle structure and planning
Clause 6.2
11
Hazard and risk assessment
Clause 8
1
Allocation of safety functions to protection layers
Clause 9
2
Safety requirements specification for the safety instrumented system
Clauses 10 and 12
3
Stage 1
Design and engineering of safety instrumented system
Clauses 11 and 12
4
Design and development of other means of risk reduction
Clause 9
Stage 2
Installation, commissioning and validation
Clauses 14 and 15
5
Stage 3
Operation and maintenance
Clause 16
6
Stage 4
Modification
Clause 17
7
Stage 5
Decommissioning
Clause 18
8
Verifica-tion
Clauses 7, 12.4, and 12.7
9
Key:
Typical direction of information flow.
No detailed requirements given in this standard.
Requirements given in this standard.
NOTE 1 Stages 1 through 5 inclusive are defined in 5.2.6.1.3.
NOTE 2 All references are to Part 1 unless otherwise noted.
IEC 3247/02

Figure 1 IEC 61511 system safety life-cycle

2. ISSUING ORGANISATION

This document is issued by target control (WP7) within Target Division.

3. CONTEXT

3.1. Objective

The objective of this document is to define the system architecture for TSS according to IEC 61226 [6] and IEC 61513 [5]. The system architecture describes

- Allocation of TSS functions to separate subsystems
- Interface between subsystems
- Logic implementation of TSS functions
- Implementation of redundancy, separation, and diversity on a conceptual level
- Basic layout of the subsystems in the ESS facility

3.1. Purpose

The purpose of this document is to contribute to the following requirements in ESS-0002776 [3]:

- TSS-TSS-001 (TSS safe state)
- TSS-TSS-101 (RSF, He cooling mass flow)
- TSS-TSS-102 (RSF, He cooling pressure)
- TSS-TSS-103 (RSF, He cooling inlet temperature)
- TSS-TSS-104 (RSF, Target wheel rotational speed)
- TSS-TSS-105 (RSF, Monolith atmosphere pressure)
- TSS-TSS-201 (permit static beam)
- TSS-TSS-202 (manual safety stop)
- TSS-TSS-203 (operational monitoring)
- TSS-TSS-204 (operational start and stop)
- TSS-TSS-205 (safety monitoring)
- TSS-TSS-401 (design standards and rules)
- TSS-TSS-403 (redundancy)
- TSS-TSS-404 (diversity)
- TSS-TSS-405 (functional separation)
- TSS-TSS-406 (physical separation)

The purpose of this document is also to act as base for:

- TSS system design
- TSS electrical design
- TSS application software design

- TSS deterministic and probabilistic analysis of safety reliability

4. ARCHITECTURAL VIEWPOINTS

4.1. TSS architecture overview

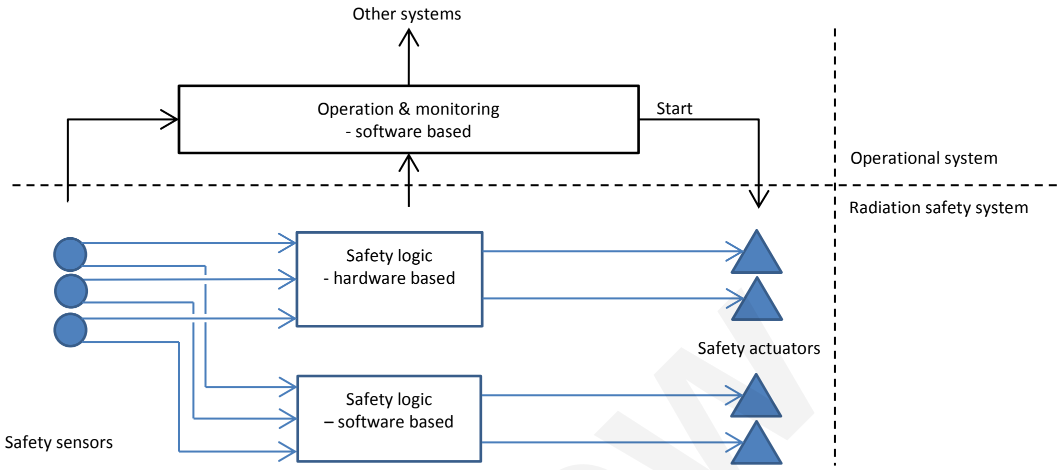


Figure 2 TSS subsystems

The complete TSS consists of two main subsystems (see Figure 2):

- the operational system, that performs functions classified as EIC0, see ESS-0218018 [4]
- the radiation safety system, that performs functions classified as EICPA or EICPB, see ESS-0218018 [4]

The architecture of the radiation safety system is based on Example 3 and Example 5 in section C.2 in IEC 61513 [5]. The standard states that these examples are “typical situations” which both have “Low potential causes of CCF”. See Figure 3 and Figure 4.

Example 3

Safety group consisting of a system with two channels operating differently the same protection action*

* It supposes the operator has sufficient time and information to react

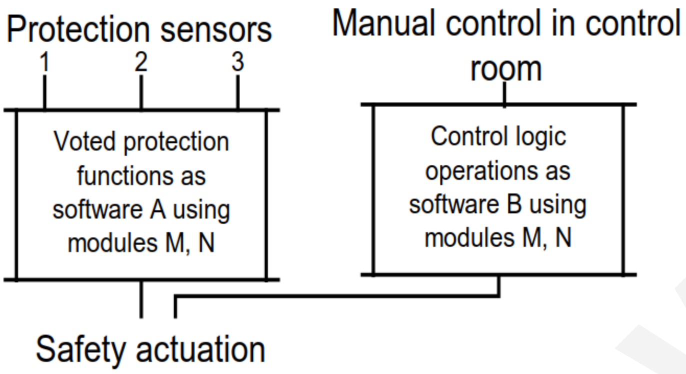

Protection sensors
1
2
3
Manual control in control room
Voted protection functions as software A using modules M, N
Control logic operations as software B using modules M, N
Safety actuation

Figure 3 Example of architecture for manual control, based on IEC 61513

The example describes two functions; one automatic protection function and one manual control function. The manual control in the control room does not use redundancy, it is not included in the automatic protection voting, it uses its own control logic (application software functions A and B which are based on common firmware modules M and N), and it uses the same actuation method as the voting function. The design of the TSS manual safety stop is based on this example.

Example 5

Safety group consisting of diverse protection functions W and Y distributed in two different systems (diverse hardware and system software with possible similarities, for example possible similar algorithms, similar timing, similar documentation, common staff)

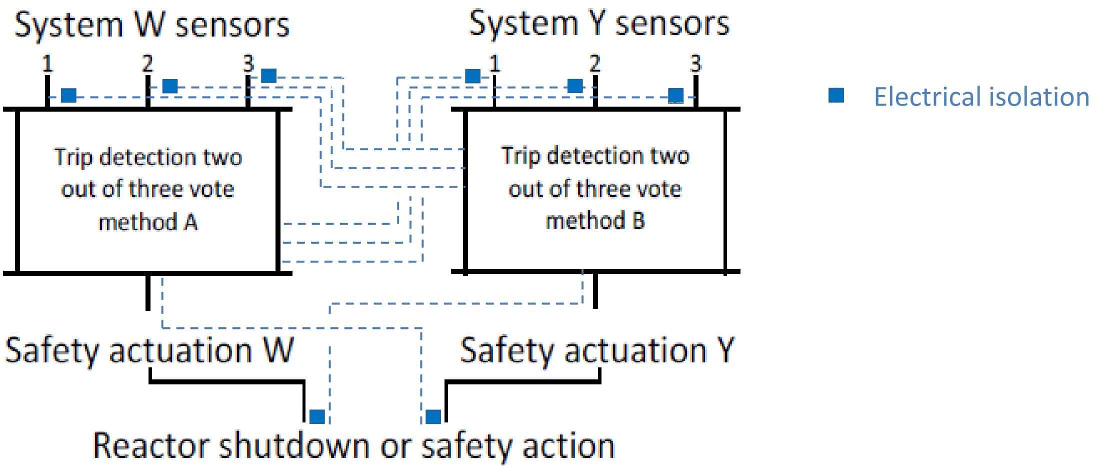

System W sensors
1
2
3
System Y sensors
1
2
3
Electrical isolation
Trip detection two out of three vote method A
Trip detection two out of three vote method B
Safety actuation W
Safety actuation Y
Reactor shutdown or safety action

Figure 4 TSS architecture for radiation safety functions, based on IEC 61513

The example, with black solid lines, describes two diverse functions (W and Y), 2oo3 voting of sensors, diverse voting systems (method A and B), and diverse actuation (W and Y). The design of the TSS radiation safety functions is based on this example.

TSS specific add-ons are highlighted as blue dotted lines. Each sensor has two outputs; one for each voting system. Each voting system uses both actuations. Electrical isolation is used to achieve functional separation.

The purpose is to increase the reliability. For any accident that demands TSS, both 2oo3-voting systems (A and B) and both actuation systems W and Y are used. That means, if any of system A, system B, actuation W or actuation Y fails, then still both W sensors and Y sensor can trip the system.

5. ARCHITECTURAL DESIGN

5.1. Radiation safety system

The architecture of the radiation safety system is described in Figure 5 and in the sections below.

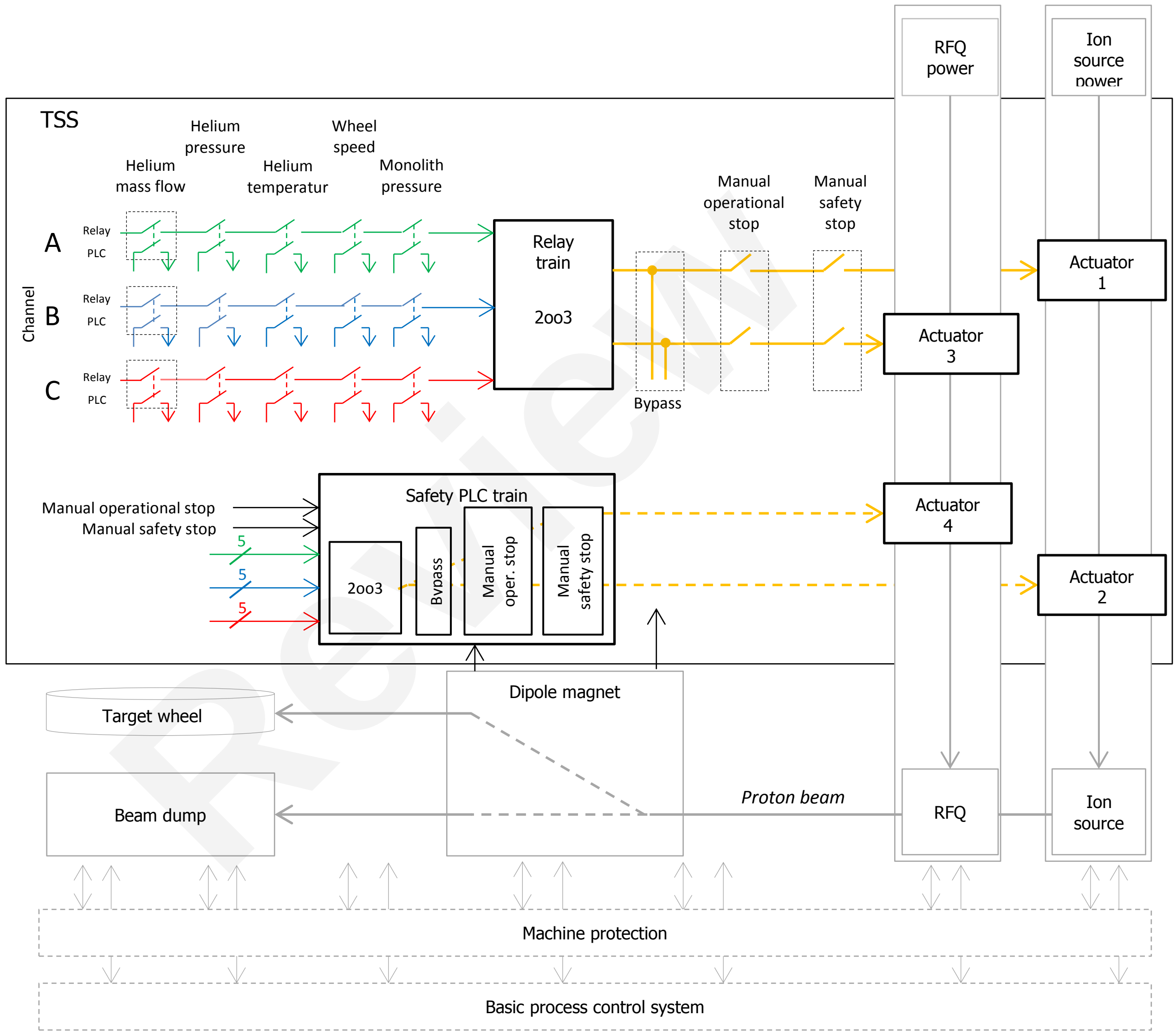


Figure 5 TSS architecture – radiation safety functions, bypass function and manual stop functions.

5.1.1. Sensors

Each TSS process parameter refers to a specific radiation safety function, and is measured by three redundant sensors (A, B and C). Each sensor has dual functionally separated (electrically isolated) outputs; one for each train. A sensor indicates a trip if the monitored process parameter is beyond a predefined trip limit.

5.1.2. Channels

The sensors are allocated to three redundant, functionally separated and physically separated channels (A, B and C). One channel includes sensors, sensor cables, and the treatment of sensors in series. Any sensor can, by itself, trip the channel.

In the relay train all A-sensors are connected hardwired in series to the channel A, B-sensors to channel B, and C-sensors to channel C.

In the PLC train all sensor indications are available in the software and the channel logic is generated by the software.

5.1.3. Trains

The channels are distributed into two redundant and functionally separated 2oo3 voting systems; trains. One train is based on relay technology, and the other on PLC technology, i.e. they are diverse.

The 2oo3 voting function is visualized in Figure 8 and is identical in the two trains; at least two of the three channels have to indicate a trip in order for the system to trip. The channels do not necessarily have to be tripped by the same process parameter.

As each train has dedicated actuators on both the ion source and the RFQ, the trains can trip the beam independent of each other.

The reasons for 2oo3 voting of the channels are:

- Resistance to independent single failure in one channel
- Increased availability (avoid spurious trips due to failure in one channel)

5.1.4. Actuation

The trains stop beam production by removing active control signals to the actuators, which switch off the electrical supply to the ion source and to the RFQ.

It is enough to act on either the ion source or the RFQ to prevent beam from reaching target, i.e. these are redundant mechanisms. Since the ion source and RFQ are different systems along the accelerator to produce the proton beam, the mechanisms are also claimed to be diverse.

Each train has one dedicated actuator at each of the ion source and the RFQ. The two serial-connected actuators at the ion source are diverse (different technology) from the two serial-connected actuators at the RFQ.

Any actuator can trip the beam independent of the others.

5.1.5. Bypass

In order to have a static permit for beam production from TSS, the 2oo3 voting of the channels can be bypassed. This means that even if the 2oo3 voting results in a trip, the system will keep allowing beam production.

The bypass is activated based on a set of control conditions, where all conditions must be fulfilled in order to have all actuators allowing beam production. See Table 1. The disconnectors at the dipole magnet and the switches at the ion source and RFQ are diverse (different technology).

Both the disconnectors and the switches have functionally separated outputs to indicate their position. The positions are monitored, evaluated and communicated by the trains. See Figure 6.

This function does not prevent any other system from stopping beam production.

Table 1 Bypass conditions for each actuator

	Actuators			
Control condition	**A1** *- ion source, relay train*	**A2** *- ion source, PLC train*	**A3** *- RFQ, relay train*	**A4** *- RFQ, PLC train*
DM1 *- disconnector #1 at electrical supply to dipole magnet set in off position (assures beam direction to dump)*	X	X	X	X
DM2 *- disconnector #2 at electrical supply to dipole magnet set in off position (assures beam direction to dump)*	X	X	X	X
Switch 1 *– switch at ion source set in “bypass” position*	X	X		
Switch 2 *– switch at RFQ set in “bypass” position*			X	X

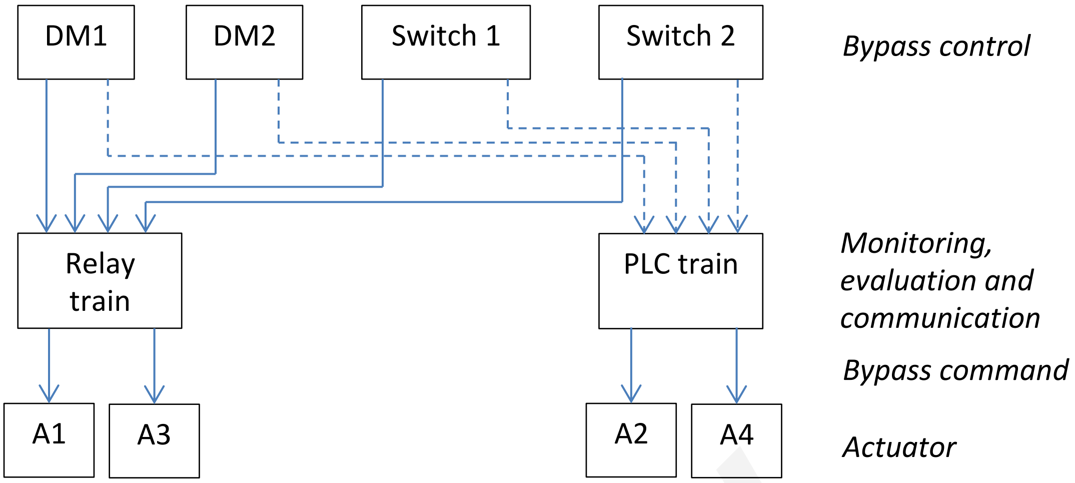


Figure 6 Bypass architecture

5.1.6. Manual stop

Two options for manual stop are available: one operational stop (intended for normal operation of TSS) and one safety stop (intended for potentially emergency situations). They are clearly divorced so that is obvious to the operator which one to use in case of an emergency (safety) situation.

The two manual stop controls (e.g. buttons) are functionally separated, i.e. they cannot prevent each other from functioning. Both have functionally separated outputs to indicate their position. The positions are monitored and communicated by the trains. See Figure 7.

They are also functionally separated from the 2oo3 voting and the bypass, i.e. they can remove the active control signal to the actuators independently of these.

The safety stop is monitored and communicated by the radiation safety system.

The operational stop is also monitored and communicated by the radiation safety system, for availability reasons. A failure in the monitoring or communication could lead to a spurious stop. As a part of the radiation safety system this failure is less probable.

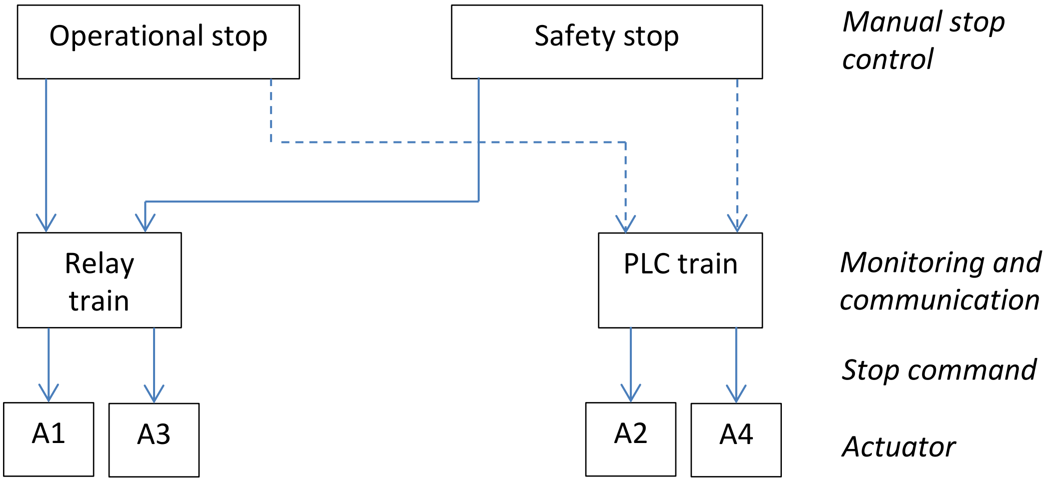


Figure 7 Manual stop architecture

5.1.7. Fail-safe

The radiation safety system architecture is built on a fail-safe concept. Each component in the system has a predefined acceptable mode for safety (safe state) that either indicates a trip (e.g. a sensor which cannot cause a system trip by itself) or actuates a system trip (e.g. an actuator) in case of these failures

- loss of power, or
- loss of communication

Other failures may not lead to a safe state. One example is an independent failure in a sensor, which forces the sensor output signal to always indicate that the process parameter monitored by the sensor is within acceptable limits.

The sensors are fail-safe in the sense that they will enter a safe state, indicting a trip, if they lose electrical supply.

The relays, the fibre communication components in the relay train, and the PLC components will enter a safe state, indicating or actuating a trip, if they lose electrical supply or communication. The PLC also has internal diagnostic (provided by the PLC supplier as predefined functions in the firmware) that can force it to the safe state due internal hardware or software failures.

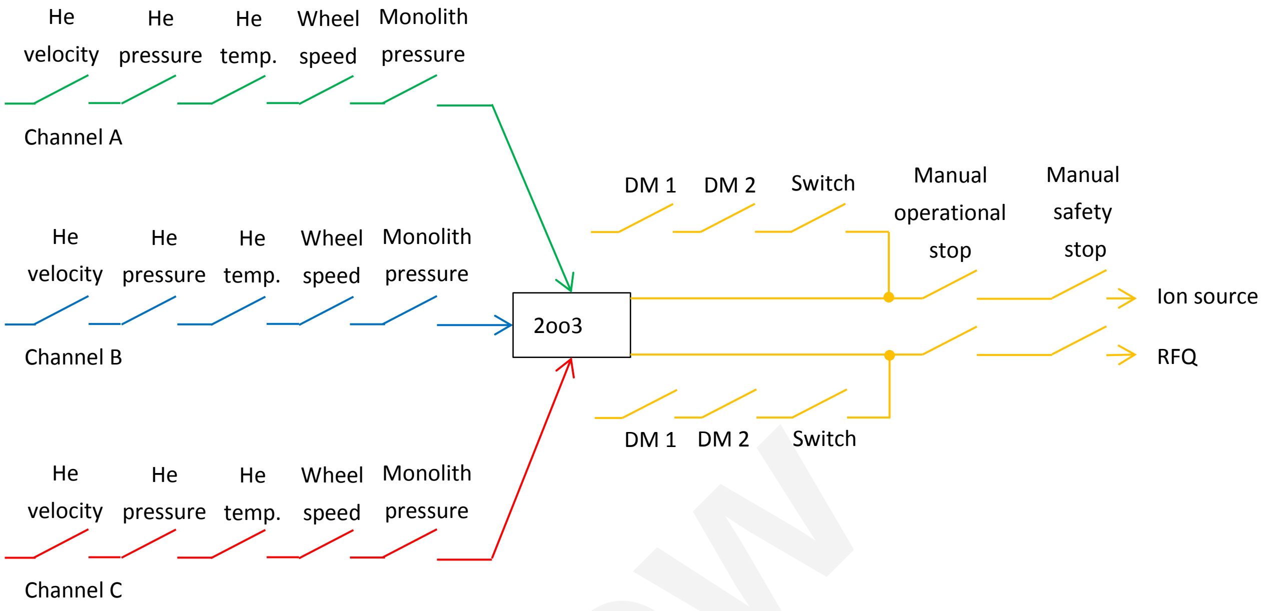
The control signals to the actuators must remain active in order to allow proton beam production; i.e. the actuator setup is fail-safe. The actuators are chosen such that the predefined state in case of lost control signal is the safe state.

5.1.8. Logic summary

The logic of the system described in the earlier sections can be summarized as

- redundant sensors for the different radiation safety functions are allocated to three channels
- 2oo3 voting is performed on the three channels
- the voting result can be bypassed by fulfilling a set of conditions
- both the voting and the bypass can be superseded by a manual stop
- the logic is identical in the two trains

The logic for one train is illustrated in Figure 8.



He velocity: relates to TSS-TSS-101

He pressure: relates to TSS-TSS-102

He temp.: relates to TSS-TSS-103

Wheel speed: relates to TSS-TSS-104

Monolith pressure: relates to TSS-TSS-105

Manual operational stop: relates to TSS-TSS-204

Manual safety stop: relates to TSS-TSS-202

DM1, DM2 and Manual switches: relates to TSS-TSS-201

Figure 8 Logic in one TSS train.

5.2. Operational system

The operational system is based on PLC technology and is functionally separated from the radiation safety system. It does not perform any radiation safety function. It does not include redundancy or diversity, and it has separate control components and cables.

As the operational system is functionally separated from the radiation safety system, it is independent of the channels, trains, bypass, and manual stops. It has no impact on the radiation safety functions or other functions performed by the safety system.

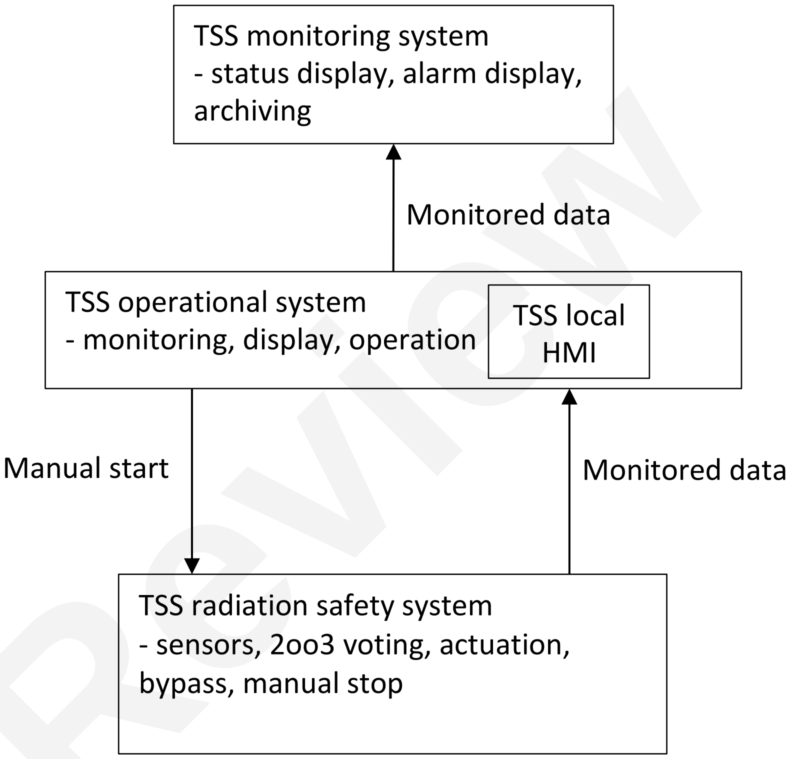

TSS monitoring system
- status display, alarm display, archiving
Monitored data
TSS operational system
- monitoring, display, operation
TSS local HMI
Manual start
Monitored data
TSS radiation safety system
- sensors, 2oo3 voting, actuation, bypass, manual stop

Figure 9 Radiation safety system vs. operational system architecture

The operational system performs the manual start and the monitoring functions.

The manual start function allows activation of the control signal to the actuators, provided that conditions for the radiation safety functions, manual stops and the bypass are fulfilled.

The monitoring function reads status from the radiation safety system components and display this status at a graphical user interface connected to the PLC. A more critical subset of the status is also displayed by separate indicators separate from the graphical user interface.

The operational system also acts as a gateway to the TSS monitoring system (see section 5.2.1), and other systems (e.g. machine protection). The communication to these systems is one-way; the operational system solely sends data to other systems.

The operational PLC communicates via fibre cables. Fibre cables do not contain energy and are not considered as a source of external failure. As such they share cable paths with the radiation safety system without risk for interference.

5.2.1. TSS monitoring system

The TSS monitoring system is based on the EPICS platform and out of scope for this document. The TSS operational system communicates data (one-way communication) to this TSS monitoring system, which supports performing the TSS operational monitoring function by providing general ESS services such as operator workstations and data archiving.

5.3. Systems behaviour

Based on the functions in the radiation safety system and the operational system, the overall system behaviour is summarized in Figure 10.

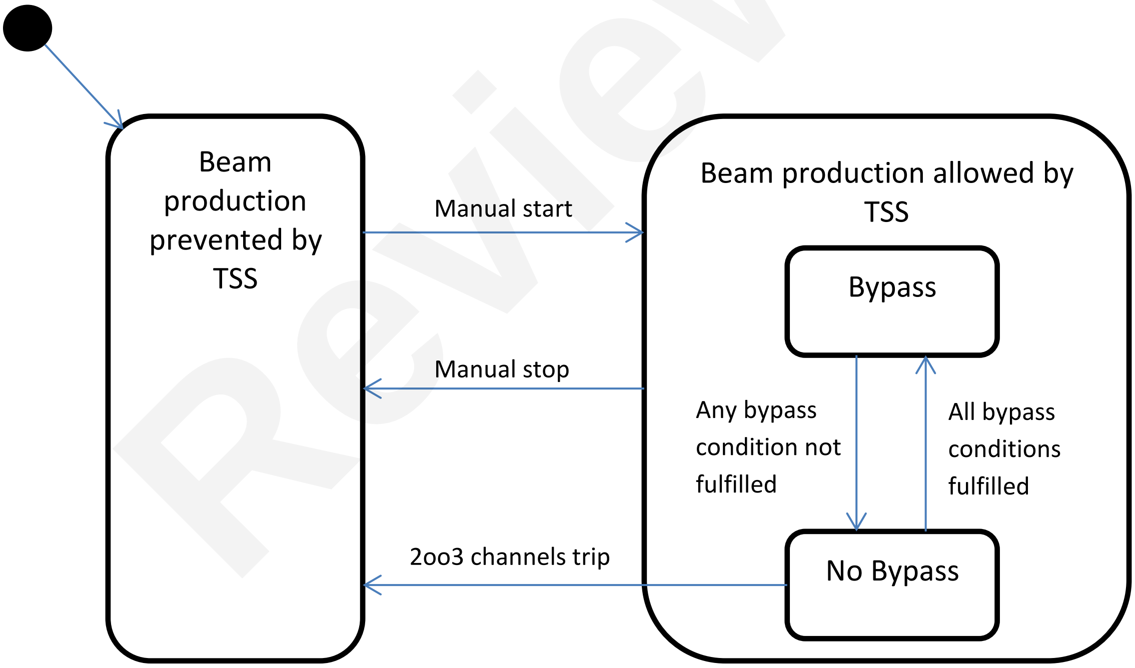

Beam production prevented by TSS
Manual start
Manual stop
2oo3 channels trip
Beam production allowed by TSS
Bypass
Any bypass condition not fulfilled
All bypass conditions fulfilled
No Bypass

Figure 10 Behavior of the complete TSS

5.4. Systems layout

Figure 11 describes the TSS main areas and cable paths in the ESS facility.

Figure 12 describes the TSS architecture and the layout of the main TSS components of the radiation safety system; sensors, control equipment, actuators, bypass conditions and manual safety stop. It also indicates that the redundant channels are routed via separate cable paths, and where these paths are placed. The manual stops are not routed through the Target utility area.

Figure 13 describes the layout of TSS equipment inside the Target utility area where all process parameters of the TSS radiation safety functions are monitored. It also indicates the physical separation between control equipment and cable routes for the redundant channels in this area. The yellow dashed boxes represent separate fire zones.

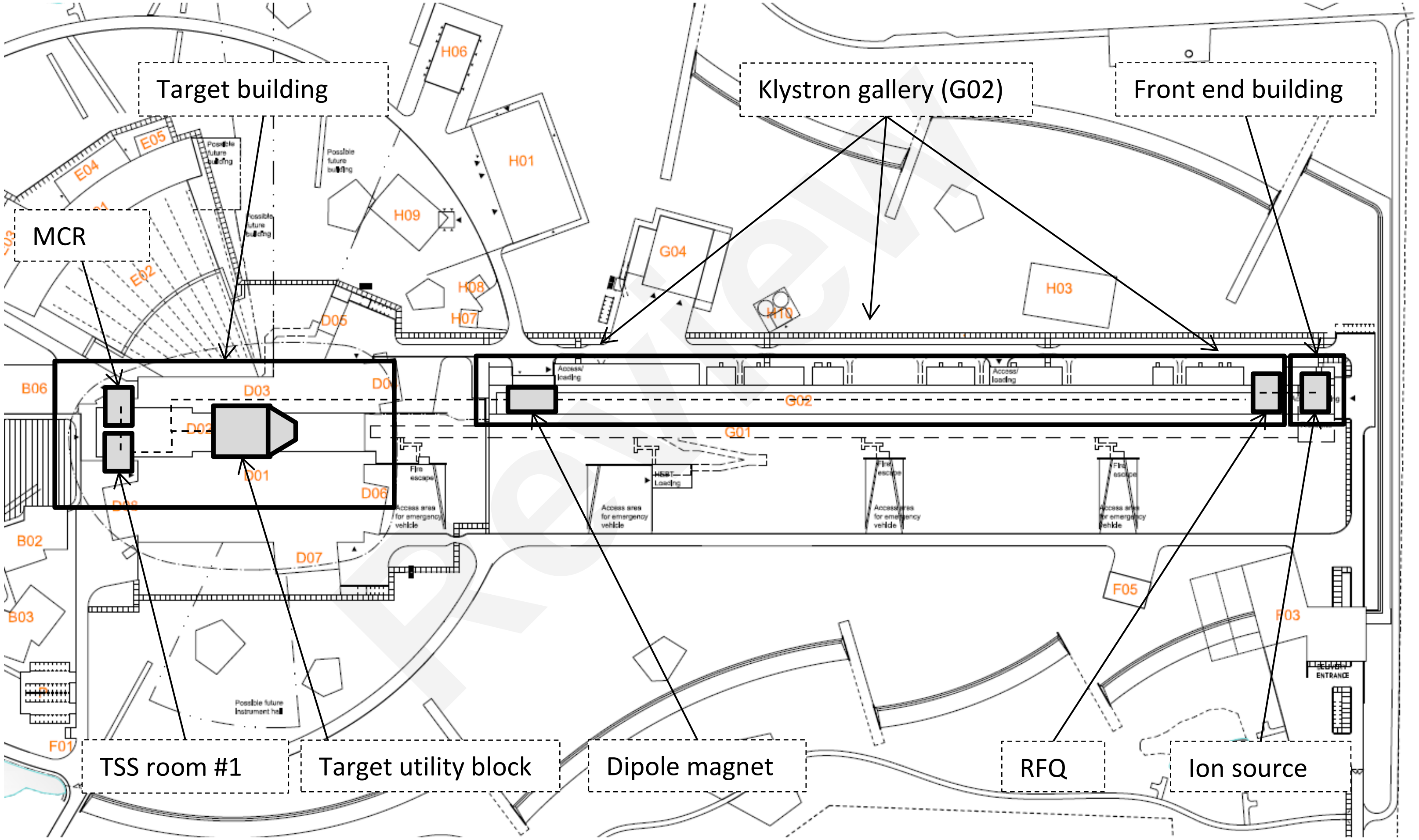


Figure 11 ESS facility layout, and TSS main areas and cable paths

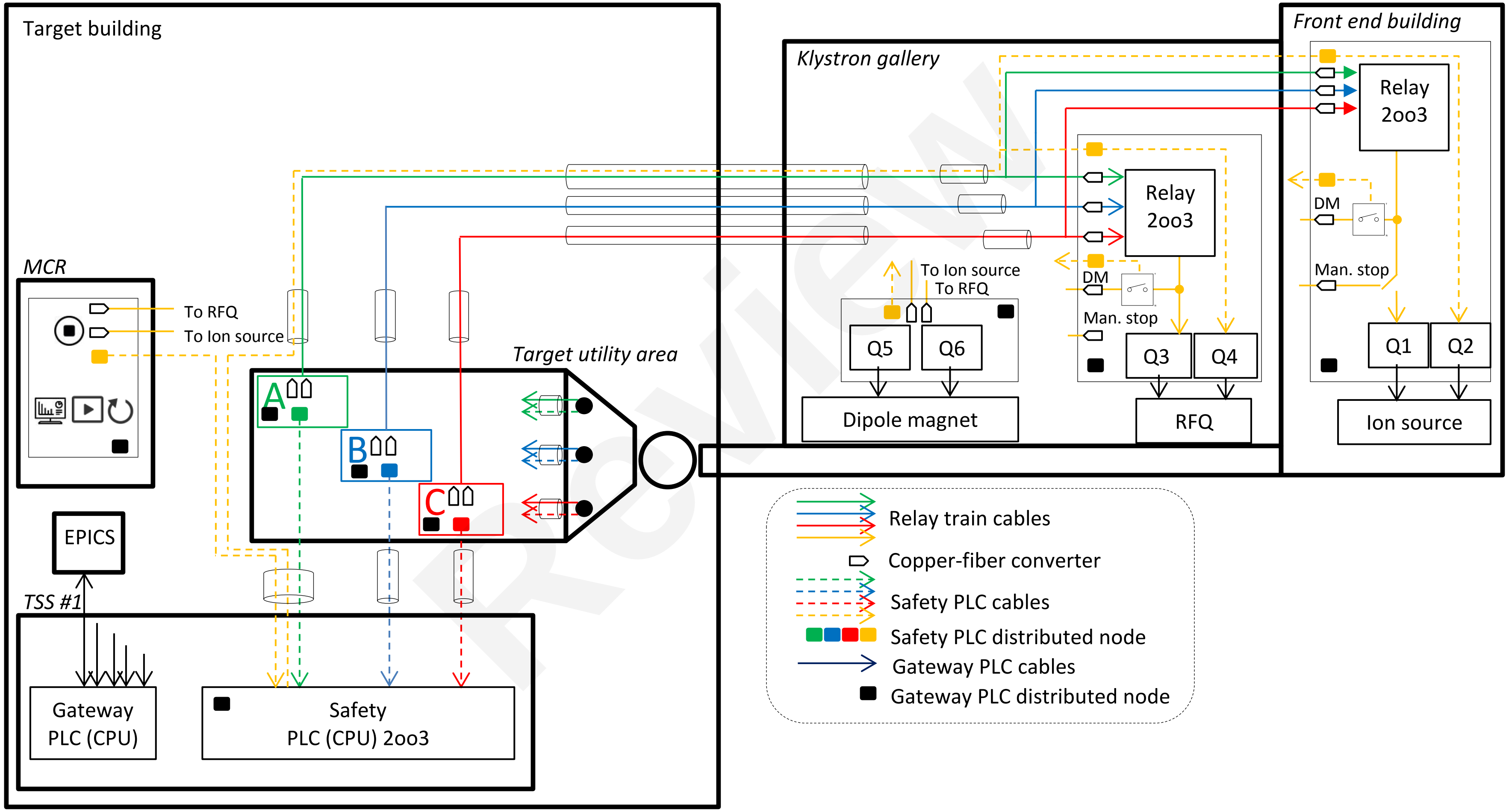


Figure 12 Layout of TSS main components at the ESS facility

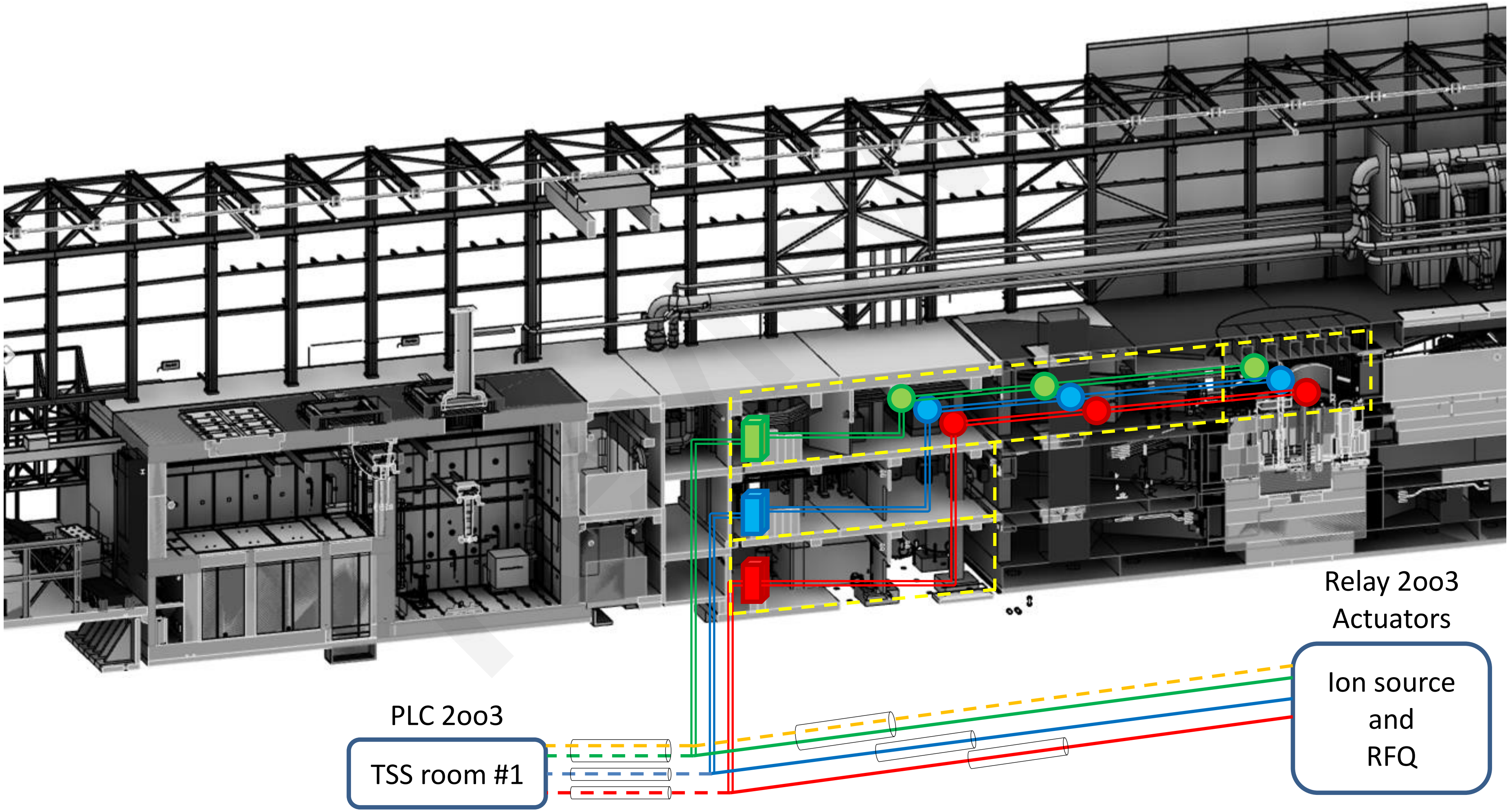


Figure 13 Principle layout of TSS in the Target utility area

5.4.1. Sensors

The sensors are located in the Target utility area. They may be placed

- Close to the measured process. Redundant sensors are then placed in the same area, i.e. fire zone. The cables connecting a sensor to the control equipment are routed cable paths dedicated to TSS; each channel has one separate cable path.
- Distanced from the measured process and close its control equipment. Each sensor is connected to the measured process by a dedicated metallic impulse pipe (sensing line). Redundant sensors are then physically separated as they are placed on different levels, i.e. in separate fire zones.

The choice of sensor location is based on the radiation environment where the process parameter is located, and if it is physically possible to use sensing lines to support monitoring of the process parameter.

5.4.2. Channels

Each of the redundant channels (A, B and C) has a separate cable path from sensors in the Target utility area to the 2oo3 voting in each train.

Inside the Target utility area the channel specific control equipment and cable paths are allocated to different levels (fire zones). The purpose is to achieve enough physical separation to withstand common cause failures due to consequences (e.g. missiles, non-electrical induced fires, pipe failures, as exemplified in IEEE 384 [7]) related to accidents that demand TSS radiation safety functions.

Outside the Target utility area the separate cable paths may be routed in the same area, i.e. same fire zone. The reason is that these areas are treated as excluded from consequences (e.g. missiles, non-electrical induced fires, pipe failures, as exemplified in IEEE 384 [7]) related to accidents that demand TSS radiation safety functions.

5.4.3. Trains

The diverse 2oo3 voting components are located in physically separated areas (fire zones):

- PLC 2oo3 voting is placed in TSS room #1 in the Target building
- Relay 2oo3 voting is placed in the:
  - Frontend Building close to the actuator for the ion source
  - Klystron Gallery close to the actuator for the RFQ

The relay 2oo3 voting is aimed to be performed as close as possible to the actuators. The purpose is to keep physical separation of the channels as far as possible, and to simplify cabling between voting and actuator. Therefore the voting is split and placed at both the ion source and the RFQ.

5.4.4. Actuation

The actuators are located in physically separated areas (fire zones):

- Inside TSS cabinets in the Frontend building (disconnecting the Ion source electrical supply)
- Inside TSS cabinets in the Klystron gallery (disconnecting the RFQ electrical supply)

5.4.5. Bypass

The manual settings for the conditions of bypass (static permit of beam) are located outside the MCR.

The manual disconnectors for the electrical supply to the dipole magnets are located in a TSS cabinet in the test stand area of the Klystron gallery, close to the dipole magnets. The manual switches are located in a TSS cabinet at the ion source and in a TSS cabinet at the RFQ, respectively.

5.4.6. Manual safety stop

The manual safety stop is located in the TSS cabinet in main control room. It is monitored and communicated via components in the radiation safety system to the actuators.

As part of the radiation safety system it is functionally separated from the operational system in the cabinet.

5.4.7. Safety monitoring

Dedicated indicators for critical status (for example position of the actuators) are located in the TSS cabinet in the main control room. The status is monitored and communicated via components in the operational system.

As part of the operational system it is functionally separated from the radiation safety system in the cabinet.

5.4.8. Operational start, stop and monitoring

The operational system is distributed in all TSS cabinets. The reason is that the operational system monitors status of components in the radiation safety system, and needs access to these. There is functional separation between the operational system and the radiation safety system. In general the components in the radiation safety system has dedicated, electrically isolated, outputs used by the operational system. Furthermore the operational system uses fiber communication between the different cabinets, and thereby prevents electrical interference to the radiation safety system.

The control (e.g. buttons, screens) for operational start, stop and monitoring functions are located in the TSS cabinet in the main control room.

Since the operational manual stop is monitored and communicated via the radiation safety system (see section 5.1.6), it is functionally separated from the operational functions in the cabinet.

Operational data, such as status, alarm indications and data for archiving, are communicated through a separate connection on the operational PLC to the TSS monitoring system via the EPICS network.

Since the operational PLC is functionally separated from the radiation safety system, the EPICS network is prevented from affecting the radiation safety functions or any function performed by the radiation safety system.

6. GLOSSARY

Term	Definition
HMI	Human Machine Interface
MCR	Main Control Room
PLC	Programmable Logic Controller
RSF	Radiation Safety Function
SSC	Structures, Systems and Components

7. REFERENCES

[1] ESS-0037596, Concept specification of Target Station Safety System
[2] IEC 61511-1:2003, Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and software requirements
[3] ESS-0002776, TSS system requirements specification
[4] ESS-0218018, TSS classification report
[5] IEC 61513, Nuclear power plants - Instrumentation and control important to safety - General requirements for systems
[6] IEC 61226:2009, Nuclear power plants - Instrumentation and control important to safety - Classification of instrumentation and control functions
[7] IEEE 384, IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits

DOCUMENT REVISION HISTORY

Revision	Reason for and description of change	Author	Date
1	Approved as baseline before PDR	Mikael Olsson	2016-02-08
2	Approved for PSAR	Mikael Olsson	2016-03-24
3	Approved for updated PSAR	Mikael Olsson	2017-02-20
4	Approved for updated PSAR Added • architectural viewpoints on subsystem level • definition of three channels • stop button • facility layout Updated • more details of 2oo3 voting • more details in system architecture figures • Relay and PLC connected to both ion source and RFQ respectively Removed • detail design information	Mikael Olsson	2018-03-01
5	Approved for TSS CDR2 Added • examples from IEC 61513 • galvanic isolated outputs on sensors • manual stop and bypass in Figure 5, and specific figures for architecture Figure 6-7. • details of sensors, channels, trains, etc • details of bypass conditions • details of operational system • details of layout, including picture of target utility block	Mikael Olsson	2019-03-25