
ICS Handbook

	Name	Role/Title
Owner	Timo Korhonen	Chief Engineer, Integrated Control System Division
Reviewer	Annika Nordt Daniel Piso Fernandez Susanne Regnell Hector Novella	ICS Protection Systems Group Leader ICS Hardware and Integration Group Leader ICS Software Group Leader ICS Deputy Project Manager
Approver	Henrik Carling	ICS Head of Division

TABLE OF CONTENT

PAGE

1. INTRODUCTION.....	9
1.1. Purpose.....	9
1.2. Scope	9
1.3. Definitions	9
1.4. Related Documents.....	9
2. ICS DIVISION MISSION STATEMENT	10
2.1. Scope	10
2.2. Responsibilities	11
2.3. Documentation structure and references	11
3. SYSTEM DESIGN PHILOSOPHY.....	11
3.1. Introduction.....	11
3.2. Operation of the ESS Facility	12
3.3. System mandatory functional requirements.....	12
4. SYSTEM LIFE CYCLE	14
4.1. Introduction.....	14
4.2. Roles	14
4.3. Lifecycle Phases	14
4.4. System Development.....	16
4.4.1. CS Deliverables Management	16
4.4.2. Deliverables for CS technical specifications.....	17
4.4.3. Deliverables and requirements for CS Manufacture	18
4.4.4. Deliverables and requirements for CS Factory Acceptance Tests.....	21
4.4.5. Deliverables and requirements for CS Installation on ESS site	22
4.4.6. Deliverables and requirements for CS Site Acceptance Test	22
4.4.7. CS Integrated Commissioning	23
4.4.8. CS Operation and Maintenance	23
4.4.9. Deliverables and requirements for CS Obsolescence Management.....	23

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

4.4.10. CS Decommissioning	23
4.4.11. Requirements for CS Documentation	23
5. SYSTEM ARCHITECTURAL DESCRIPTION	25
5.1. Introduction	25
5.2. Integrated Control System Architecture.....	25
5.2.1. Connections between subsystems	25
5.2.2. EPICS and the Control System Network	26
5.2.3. Timing Distribution	28
5.2.4. Beam Interlock system network.....	29
5.3. Control System Services	30
5.3.1. Archiving service	30
5.3.2. Alarms Strategy and Management.....	30
5.4. Operator tools	31
5.4.1. User Interface tools.....	31
5.4.2. Machine setup management	33
5.5. Accelerator physics applications and support	33
5.6. Control System Configuration Management.....	33
5.7. Naming Convention	34
5.7.1. Scope of the Naming Convention.....	35
5.7.2. Responsibility and Support	35
6. SYSTEM SOFTWARE STANDARDS AND SPECIFICATIONS.....	36
6.1. Computing Infrastructure	36
6.1.1. Architecture of Services	38
6.2. ESS Software Development Environment	39
6.2.1. The Development Environment Architecture.....	39
6.2.2. EPICS development workflow	41
6.2.3. IOCs (Input Output Controllers)	41
6.2.4. Management of the Software Development Environment.....	41
6.2.5. The ICS Virtual Development Environment	42
6.3. EPICS development	43
6.4. ICS Configuration Management Tools and Services	45
6.4.1. Naming Service	45
6.4.2. Controls Configuration Database (CCDB)	45
6.4.3. Cable Database, CDB.....	45

6.4.4.	IOC Factory	46
6.4.5.	Lattice Database	47
6.4.6.	Channel Finder	47
6.4.7.	Other supporting applications.....	48
6.5.	EPICS Services	48
6.5.1.	Archiver	48
6.5.2.	Alarm Service	49
6.5.3.	Logbook	49
6.5.4.	Other EPICS services	49
6.6.	User Interface and other end user tools	49
6.6.1.	Control System Studio.....	49
6.6.2.	Role-Based Access Control (RBAC)	50
6.6.3.	Kameleon	50
6.6.4.	Other tools.....	51
7.	SYSTEM HARDWARE STANDARDS AND SPECIFICATIONS	52
7.1.	Hardware platforms.....	52
7.1.1.	MicroTCA	52
7.1.2.	EtherCAT	52
7.1.3.	PLCs	53
7.1.4.	Other hardware and fieldbuses.....	53
7.2.	Global Timing System Specification.....	53
7.3.	ICS Network and Server Infrastructure specifications	55
8.	INTERFACE SPECIFICATIONS.....	57
8.1.	Introduction	57
8.2.	Functional Interfaces	57
8.3.	Physical Interfaces	58
8.3.1.	Connecting I/O signals to ICS equipment	58
8.3.2.	Standards for signal interfaces	58
8.3.3.	I/O through fieldbuses	59
8.3.4.	Timing trigger standards	59
8.3.5.	Beam interlock system I/O	60
8.4.	Division of responsibilities related to interfaces	60
9.	MACHINE PROTECTION SPECIFICATION	61
9.1.	Introduction	61

9.1.1.	The Role of Machine Protection at the ESS	61
9.1.2.	Achieving High Operational Availability of the ESS	61
9.1.3.	The Machine Protection Equipment under control (EUC)	61
9.1.4.	Machine Protection Goals.....	62
9.1.5.	Relation of ESS Machine Protection to ESS Safety.....	62
9.1.6.	Means to achieve Machine Protection.....	62
9.1.7.	Machine Protection and EUC design	63
9.1.8.	Machine Protection and dedicated technical protection systems	63
9.1.9.	Machine Protection and operational and preventive maintenance procedures.....	63
9.1.10.	Machine Protection support systems	63
9.1.11.	The Machine Protection mandate at the ESS.....	64
9.1.12.	Tasks of the ESS Machine Protection Committee (MPC).....	64
9.1.13.	Composition of the MPC.....	64
9.1.14.	Relation of the MPC to other ESS decision making bodies.....	65
9.1.15.	Related Machine Protection venues	65
9.2.	ESS Machine Protection Systems Engineering Management Plan	65
9.3.	Machine Protection Systems Requirements Architectural Framework	65
9.3.1.	Machine Protection Capability Objectives.....	65
9.3.2.	Machine Protection General Requirements	65
9.3.3.	Machine Protection System-of-Systems Architectural Framework	68
9.3.4.	Local MP-related Systems	68
9.3.5.	MP-related Proton-Beam Monitoring Systems	71
9.3.6.	MP-related Proton Beam Monitoring versus Beam Instrumentation Protection Systems	72
9.3.7.	Beam Interlock System.....	72
9.3.8.	MP-related Beam Switch-Off Actuation Systems	72
9.3.9.	MP Management Systems	73
9.3.10.	MP Event Logging and Diagnostics System	74
9.3.11.	MP Operating Mode Configuration System	74
9.3.12.	MP Status and Configuration Monitoring System.....	74
9.3.13.	Higher Level Safety Systems	74
9.3.14.	Timing System	74
9.3.15.	Interfaces between the Constituent Systems	75

9.4. Software Specifications	75
9.5. Hardware Specifications	76
10. PERSONNEL SAFETY SYSTEMS SPECIFICATION	78
10.1. PSS Introduction	78
10.2. PSS Standards and lifecycle	78
10.3. Personnel Safety System Software Specifications	79
10.3.1. PSS Software Strategy	79
10.3.2. PSS Cyber Security Plan – Defence-in-Depth	80
10.3.3. PSS Software Architecture	81
10.3.4. PSS Software Virtual Commissioning	83
10.4. Personnel Safety Hardware Specification.....	83
10.4.1. PLC modules	83
10.4.2. PSS enclosures.....	83
10.4.3. Beam-off stations	84
10.4.4. Monitoring doors in PSS controlled areas.....	84
10.4.5. Access control system	85
10.4.6. Key exchange system.....	86
10.4.7. PSS blue/red lights.....	86
10.4.8. Message display system	87
10.4.9. Public address system	87
10.4.10. PSS cable routes	87
10.4.11. PSS cables.....	87
10.4.12. PSS interfaces	87
10.4.13. Radiation monitors.....	88
10.4.14. ODH monitors.....	88
10.5. Personnel Safety Configuration Management and Quality Assurance Plan	88
10.5.1. PSS Configuration Management Plan	88
10.5.2. PSS Development and Quality Assurance Plan	93
11. DEVIATIONS POLICY	96
11.1. Introduction	96
11.2. Handling of Deviations and Non-Conformances.....	96
11.2.1. Event detection	96
11.2.2. Deviation categorization.....	97
11.2.3. Deviation treatment	98

11.2.4. Root cause investigation	99
11.2.5. Corrective and preventive actions	99
12. APPENDICES	100
13. GLOSSARY	101
14. REFERENCES.....	101
DOCUMENT REVISION HISTORY	102

LIST OF TABLES

Table 1 Acronyms and definitions	9
Table 2 Copper communication cable requirements	55

LIST OF FIGURES

Figure 1 Control System life cycle from design to operation	16
Figure 2 Connections between I/O Controllers.....	26
Figure 3 Connections between EPICS servers and clients.....	27
Figure 4. The ESS control system (Technical) network and its relation to other networks.....	28
Figure 5 Schematic view of the timing distribution.	29
Figure 6 Example of a BOY graphical user interface screen, also known as OPI, or HMI	32
Figure 7. Example of a DataBrowser plot.	32
Figure 8. Example BEAST alarm display.....	32
Figure 9. A graph illustrating the flow of configuration data.....	34
Figure 10. Schematic view of the Development Environment.....	40
Figure 11. Completing the development loop through the GIT repository.	41
Figure 12 Ansible is used for the configuration of virtual and physical machines.....	42
Figure 13. Ansible playbooks used to configure ICS systems are stored and versioned in Git	42
Figure 14 Vagrant uses the playbooks stored in Git to populate the virtual machines.....	43
Figure 15. IOC Factory deployment.....	47

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

Figure 16. End device patch panel physical network topology 55

Figure 17 Conceptual drawing ESS Network 57

Figure 18 Decision making process for deviation classification 97

1. INTRODUCTION

The Integrated Control System Division (ICS) is responsible of defining and providing control systems for the ESS facility. This Handbook defines standards for the ESS Integrated Control System (ICS) that are to be followed by all of the contributors, internal ESS/ICS staff, in-kind collaborators and companies delivering systems or services to ESS.

1.1. Purpose

These standards are essential in order to achieve an integrated, maintainable and affordable control system to operate ESS. These standards are applicable to the development process and comprise deliverables and quality assurance requirements as well as descriptions of standard software and hardware components.

In most areas this handbook will not be a catalogue listing the details of components or standards because details may be subject to frequent updates. Instead, guidelines and the philosophy are described. For details, links to online documentation or CHESS documents are provided.

1.2. Scope

The standards defined in this Handbook consider the Integrated Control System (ICS); the standards are applicable to all work that the ICS Division and related organizations deliver to ESS ICS. Related organisations include the in-kind partner laboratories, commercial contractors and similar entities, regardless of the work having been initiated or contracted by the ICS Division or another division of ESS.

1.3. Definitions

Table 1 Acronyms and definitions

Acronym	Definition
ICS	Integrated Control System
ICS Division	Integrated Control System Division in the ESS Machines Directorate
In-kind contribution	Contribution of a member country to ESS that is not in the form of money but a defined deliverable, in form of physical devices or components, software, service or labour.

1.4. Related Documents

This document is intended to give an overview of the described topics. Detailed descriptions of each subject are in separate documents stored in CHESS, and when appropriate by the nature of the subject (e.g., frequent updates), available online on the

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

ICS website (Confluence WIKI.) A list of the references is provided in the last chapter of this document.

2. ICS DIVISION TECHNICAL MISSION

2.1. Scope

The ICS Division develops, supports, maintains and enforces the standards specified herein. Well-established industrial standards, commercial off-the-shelf (COTS) and open source products are promoted, while custom-built solutions are strongly discouraged. Design choices and the prescribed standards are based on independent market surveys, prototype activities, benchmarking and evaluations.

The ICS division provides control system integration for ESS stakeholders. ICS staff works together with the subsystem engineers of other divisions to integrate the subsystems into the EPICS-based control system.

ICS provides a set of generic control system services to the other divisions. ICS is responsible for defining the systems based on user requirements, providing, operating and maintaining the services and supporting the users of the services.

Modern control systems are based on technology that undergoes continuous, rapid improvement in capability and possibilities. Control systems have to follow this development to remain maintainable but at the same time they can also benefit from this development to realize dramatic cost, performance, availability, user-experience, safety and efficiency improvements for the whole ESS facility. The integrated control system is thus a dynamic system that evolves over the facility lifetime with the evolution providing significant benefits in addition to normal maintenance activities.

ICS defines the standards for the control system hardware (in cooperation with the E2H2C) and software. Software standards are described in chapter 6, hardware standards are described in chapter 7 and the references in both respective chapters.

ICS commits to provide technical advice for the hard- and software it is supporting.

ICS provides the networking and server infrastructure required to connect the systems together and to operate them. Network and server infrastructure is described in 7.3 and references therein.

ICS is responsible of designing, equipping and delivering the ESS Main Control room (MCR).

ICS does **not** provide

- Office computing support

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

- Software license management, etc.
- Telephony services
- Website services (outside ICS service applications)
- Any other services that are out of the technical scope of the ICS division

2.2. Responsibilities

The ICS Division is responsible of operating, support and maintenance of the systems and standard solutions specified herein. The interface agreements between ICS and different divisions are documented in [3],[4],[5] and [6].

2.3. Documentation structure and references

As defined by ESS policy, the source for official documents is the CHES document repository. For rapidly changing and developing things some documentation will be available in Confluence wiki:

<https://ess-ics.atlassian.net/wiki/display/ID/Integrated+Control+System+Home>.

ICS Documentation structure is described in [1].

3. SYSTEM DESIGN PHILOSOPHY

3.1. Introduction

The guiding design principles of the Integrated Control system are those of performance, cost-efficiency, safety, reliability and maintainability. The system has to perform to the specifications set by the ESS performance goals and also provide the flexibility to cope with modifications that arise during commissioning and as experience is accumulated from the operation.

The long lifetime of the facility both mandates and gives the opportunity to introduce new technologies that will provide a basis for good performance and easy upgrades. Technologies that are already now foreseen to be obsolete by the time ESS goes into regular operation shall be avoided, except as intermediate solutions when required for prototyping and development.

At the same time, there is a strong need for standardisation. Without defining standards that are used by all the parties involved in the project, integration of systems that have been developed in a distributed collaboration of institutes would be costly and inefficient and will lead to lowered quality, higher costs and even safety risks. Following the standards that are set by ESS is mandatory, if there is a strong reason to deviate from the standards, it shall always be negotiated with the relevant stakeholders and the ICS team before the deviation can be accepted.

Standardisation shall be understood as managed introduction of new solutions, that is, new technologies can be introduced when there is a well-founded reason for the

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

introduction (replacement of an obsolete technology, improvement in performance through a new technology etc.) and the necessary resources have been secured.

3.2. Operation of the ESS Facility

The ICS shall enable operation of the ESS facility (accelerator and target) from a single control room. ICS shall provide the necessary means for the operating staff to operate the ESS in all agreed modes and pulse repetition rates up to the nominal frequency of 14 Hz. The control system shall provide control system facilities that are needed to bring up the facility from an initial state to the specified regular operating state of 5 MW average beam power at 14 Hz repetition rate.

ICS shall also enable the integration of the neutron instruments in a coherent and cost efficient way that ensures efficient operation of the instruments and helps them in the mission of producing world-class science.

ICS shall also provide facilities to analyse the performance of the facility and its components by acquiring and archiving vital data from the facility and providing the necessary tools to retrieve the data for analysis.

3.3. System mandatory functional requirements

ICS System requirements are listed in [2]. The most central requirements are listed here for convenience.

[Scope] ICS division shall provide control system integration to all relevant ESS divisions and facilities (Accelerator, Target, Site Infrastructure, Neutron Instruments.)

[Integration] The ICS shall support operation of the ESS Accelerator, target and the relevant Site Infrastructure from a single control room. Neutron instruments are typically operated individually from their own locations, and the operating of the instruments is the responsibility of DMSC. However, ICS shall provide the necessary support that is required to operate the instruments from the locations decided by DMSC and the instrument responsible staff.

[Timing] ICS division shall provide a timing and synchronisation facility for the ESS that is able to deliver trigger pulses, synchronised clock signals, synchronised software actions and synchronous timestamps for the components connected to the ICS.

[Operation] All ICS systems shall be able to support operation of the facility at 14 Hz. Lower rates than 14 Hz shall also be possible.

[Reliability] ICS systems shall provide a level of reliability that is commensurate with the general reliability and availability requirements of the ESS.

[Safety] ICS shall deliver Personnel Safety Systems (PSS), protecting personnel from harm arising from conventional hazards or ionizing radiation hazards where radiation exposure beyond allowable limits could occur as defined in chapter 10.

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

Other than PSS, the control system shall not be relied on to provide any kind of safety against harm to people working with the equipment under control.

[Machine protection] ICS shall provide systems to protect the ESS accelerator and Target from beam-induced hazards. The global Machine Protection (or Target Protection) systems shall be built in cooperation with the relevant stakeholders.

[Data Handling and Storage] ICS shall set up a data archiving system to collect, store and retrieve data that is relevant to the machine operation. This data shall be acquired via EPICS records. Storage of the data will be provided according to the ESS rules and (when appropriate) record-keeping requirements set to scientific facilities.

[Subsystem integration support] ICS division shall provide the control system users with integration support and a set of (software) tools to support the activities of the users. The tools include (but are not limited to) graphical user interface (GUI) building tools, tools to retrieve and visualize archived data and support for scripting languages.

4. SYSTEM LIFE CYCLE

4.1. Introduction

This chapter specifies the system life cycle and development process. It defines the required inputs, the methodology and rules applicable and the resulting deliverables for each phase in the life cycle. The application of this development process will ensure that the system is fully compliant with ICS Handbook and reference documents as shown in section 1.4.

This chapter also defines roles and responsibilities, but not the assignment of those to in-kind contributors or other parties. The assignment of roles shall be defined in each particular in-kind agreement.

4.2. Roles

- **System Responsible Officer.** Provides input throughout the design process. They review the control system design as well as approve system factory acceptance tests (FAT) and site acceptance tests (SAT).
- **ICS Responsible Officer.** Develops, supports, maintains and enforces control development standards, development processes and design conventions. They also provide hardware and software support to control system suppliers. They review the control system design and participate to factory acceptance tests and site acceptance tests.
- **Control System Designer.** Designs the control system according to ESS specifications for a system.
- **Control System Supplier.** Supplies any equipment or component including spare units for a control system. If provided by an in-kind partner, the boundary of the supply is defined in the in-kind schedule specifications.
- **System Operator.** Operates the system controls. They work mainly in the MCR (Main Control Room) and, use control and monitoring tools delivered by the Control System Supplier. They have received the necessary training based on information provided by the Control System Supplier.
- **Control System Maintenance Operator.** Maintains the system controls. They conduct preventive and routine maintenance, as well as unplanned maintenance in case of breakdown. They manage spare units.

4.3. Lifecycle Phases

As a part of system implementation, the implementation process of control systems shall comply with the general scheme and procedures used for the ESS project.

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

This scheme foresees an implementation process in three main phases as illustrated below in Figure 1:

- A **design phase** in two steps, control system design followed by a project review. The two steps are repeated for preliminary and critical design.
- A **manufacture phase** in two steps, system manufacture and factory acceptance test. Individual tests of controls equipment shall be performed during manufacture.
- An **integration phase** in three steps, system installation on ESS site followed by site acceptance test and integrated commissioning. Site acceptance test includes integration of control (sub-)systems and acceptance tests of the whole control system if applicable.

The implementation process is followed by:

- **Operation and maintenance phases.** These two phases are merged together as they are closely linked; they are not in the current scope of ICS Handbook.
- **Decommissioning phase.** Completes the system life cycle, but is outside the scope of ICS Handbook.

Each phase is characterized by its outputs, which are the deliverables at completion of the phase. The outputs from one phase are used as inputs to the next together with controls requirements and guidelines provided by ESS handbooks.

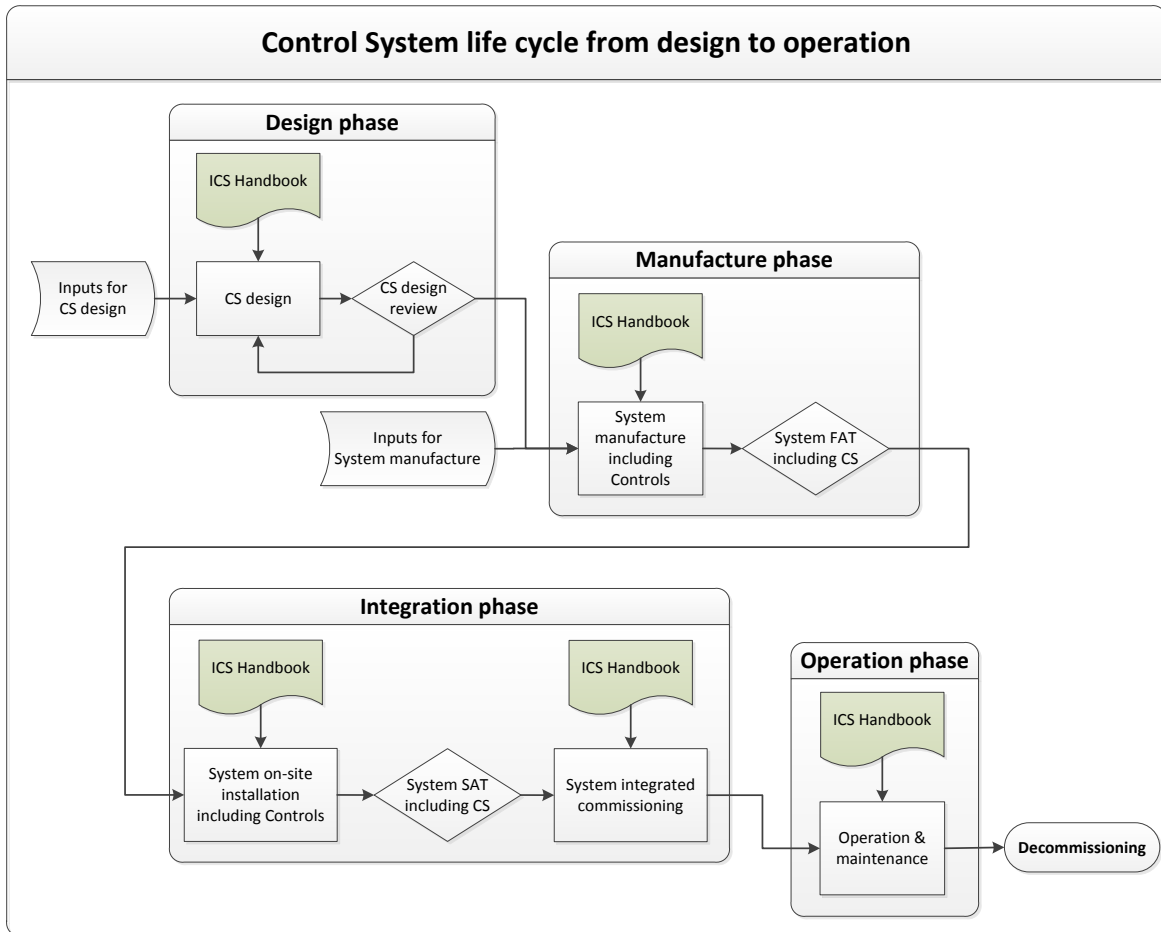


Figure 1 Control System life cycle from design to operation

4.4. System Development

This section details the control system (CS) development process introduced in the previous section. For each phase, the required inputs [Ixx], applicable rules and methodology in order to generate the outputs required for the next phase are defined.

The deliverables identified in this section as [Dxx] are delivered at completion of each life cycle phase considered. They are required depending on the configuration of the in-kind schedule.

4.4.1. CONTROL SYSTEM Deliverables Management

- Outputs or deliverables shall be identified and managed to ensure that ESS know that they have the correct version and shall be advised of any changes and/or deficiencies. Each output shall be recorded with at least the output identifier/name, the type, the description, the current version and the status (not built, built, reviewed and approved).

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

- All deliverables shall be traceable to their parent output as well as to their relevant specification and design item.
- All deliverables in electronic format shall be backed up after the acceptance phase in order to secure a functional restore state.
- All deliverables shall be kept updated along the whole lifecycle up to the SAT by the Control System Supplier. All deliverables shall be approved by ESS.

4.4.2. Deliverables for Control System technical specifications

Deliverables for Control System design:

At completion of the control system critical design, the specifications issued of the control system shall include the following items:

- [D1] Control System function and architecture. This includes a high level functional analysis (D1A), a detailed functional breakdown with functional links and the characterization of functions (D1B), and the physical and functional architecture (D1C).
- [D2] Specifications of Control System controller type (slow/fast, conventional/interlock, safety) and network interface configuration. The details of these specifications will be determined by the Control System Supplier.
- [D3] List of signals connected to the Control System including name, type, sampling rate, allocation to cubicle/rack.
- [D4] List of the data at Integrated Control System (ICS) interface.
- [D5] Hardware configuration of Control System cubicles showing the cubicle interfaces with ICS infrastructure, buildings, power supply and HVAC.
- [D6] Description of control system state machines with transitions and state variables. The deliverable includes the control system state machine mapping table.

System inputs recommended for Control System design:

The system responsible officer provides these inputs during the design process:

- [I1] Control system operation and control philosophy. This includes operation concepts, high-level operational procedures and system operating states.
- [I2] High level system functional analysis.
- [I3] System process flow diagrams (PFDs), piping and instrumentation diagrams (P&IDs) mechanical and electrical drawings related to Control System preliminary design.

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

- [14] List and short description of main states for system operation.
- [15] System risk analysis and RAMI requirements.
- [16] System Interface Control Documents (ICDs) relevant for the control system.
- [17] List and specifications of the main protection functions to implement within the system or with respect to other systems. The specifications include a risk analysis to identify the interlock (i.e. machine protection) functions from amongst all of the protection functions.
- [18] List and specifications of the main personnel safety functions and safety related measurements to be implemented within the system or with respect to other systems. Distinguish between radiation and occupational relevant functions.

Rules and guidelines required for Control System Design:

Rules are defined in the related sections of this document. Some topics may be further detailed; in such a case refer to the dedicated satellite document.

- General architecture, methods, standards for the whole Control System: chapter 5.
- Conventional controls: chapter 5.
- Interfaces with integrated control system (ICS): chapter 8.
- Specific rules and guidelines applicable to beam interlock controls (Machine Protection System): chapter 9.
- Specific rules and guidelines applicable to radiation and occupational safety controls: chapter 10.

4.4.3. Deliverables and requirements for Control System Manufacture

Control system manufacturing is assumed to be performed as part of an integrated process for the manufacture of the whole system. However, in some cases, for procurement sharing purposes, systems may be split in several procurements distributed among ESS partners. In this case, the system Control System manufacturing phase must cope with such configurations in order to avoid any major issues during on-site integration at ESS.

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

The manufacturing phase should include a manufacture design and construction activity, in which there shall be checkpoints. The final checkpoint at completion of manufacture is followed by a Factory Acceptance Test (FAT) for each TA.

Deliverables for Control System manufacture:

Outputs requested at completion of the manufacturing phase are as follows:

Hardware:

- [D7] Control System cubicles with internal wiring and all internal instrumentation and control (I&C) equipment. Sensitive equipment shall be packed separately for shipping and shall be mounted and wired on site in order to provide cubicles with all internal I&C equipment ready to be installed on ESS site and connected to:
 - ICS interfaces (see chapter 8).
 - Main supply and earth.
- [D8] Control System spare parts list with appropriate specifications of storage space and conditions.

Software:

- [D9] Source code of any software developed for the control system for operation, factory acceptance test, site acceptance test, integrated commissioning and maintenance, in the scope of the TA. Configuration data for any Control System controller to be downloaded.
- [D10] Control System configuration data (see chapter 6.4).
- [D11] IOC: configuration developed in ESS EPICS Environment (EEE, see chapter 6.3) required for factory acceptance test, site acceptance test and integrated operation.

Manufacturing documents or data:

- [D12] Detailed descriptions (text documents including structured lists in IO Layers) of:
 - Process control for any system operational state.
 - Process failure detection and strategy for process control.
 - I/O treatments.
 - Data exchanges required for slow and fast controls.
 - Feedback controls.
 - HMI, alarms and events.

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

- Software architecture for these items with identification of related software modules and data exchange links.

- [D13] Full software and configuration documentation as generated by the ESS prescribed engineering tools.
- [D14] Any document required for cubicle mounting, air conditioning, assembly, external and internal wiring, earthing and powering. Inventory of any equipment or component used for cubicle manufacturing (including I&C equipment), with supplier identification and a supplier procurement reference.

ESS on-site installation documents:

- [D15] Cabling documents for cubicle connection with I/O cabinets, Control System Networks, earth and power supplies.
- [D16] Procedure of installation, configuration, starting up and software and hardware completeness checks for the control system; in particular for system specific components (nonstandard components).

Maintenance documents:

- [D17] Original technical documentation for each piece of equipment or component (including software) used to manufacture the systems in an I&C cubicle.
- [D18] Schematic diagrams of the full signal path from the sensors/actuators to the I/O boards of the controllers including powering and conditioning, with identification of test points for fault analysis or calibration and identification of the terminal blocks. Trouble shooting procedures and functions.
- [D19] Calibration factors for each sensor-actuator-conditioner-I/O board and procedures for recalibration of these components.
- [D20] Technical documents, manuals and procedures required for maintenance of any I&C component.
- [D21] Maintenance plan: detailed warranty and/or maintenance periods and their possible extensions, licensing requirements.
- [D22] Tools required for maintenance of any I&C component.

Conformity reports:

- [D23] Certificates of conformity for Control System implementation to any regulation applicable on ESS site and proof of compliance to ESS ICS standards.

4.4.4. Deliverables and requirements for Control System Factory Acceptance Tests

System factory acceptance tests (FAT) are intended to check the conformity of the implemented system to the approved design. Control system FAT is a part of the system FAT. All instrumentation and control (I&C) components in the implementation shall be powered and tested during FAT. The FAT scenario for I&C will be adjusted depending on configuration of the Control System implementation with the policy to test as much as possible as soon as possible.

- The leading guideline of FAT scenario is to test I&C performance and functionality as much as reasonable achievable.
- For every test (unit testing; system and integration testing; acceptance testing) the version of the equipment being tested, the version of the test specifications being used and, for acceptance testing, the version of the design specification being tested against, shall be recorded.
- The Control System Supplier shall provide all necessary hardware and software tools and configuration files for FAT.
- It is recommended that compliance with I&C standards and design rules is checked throughout the manufacturing process for the FAT to run smoothly.

Deliverables for Control System Factory Acceptance Tests:

[D24] A single report collecting all Control System FAT results related to I&C will be issued. The report shall include tracing to all requirements from the approved design which are fulfilled, not fulfilled and not testable.

Rules required for Control System Factory Acceptance Tests:

- The results of FAT shall be recorded and retained in the lifetime records of EES
- Any failures during FAT shall be investigated and the cause and rectification of the failure documented in the FAT report. A complete bug report (problems and fixes) must be provided and maintained during all life cycle phases.

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

4.4.5. Deliverables and requirements for Control System Installation on ESS site

ESS site installation includes ESS site reception of I&C cubicles and equipment, damage checking at reception, installation of cubicles, mounting of I&C equipment within the cubicle, cubicle cabling and cubicle powering.

4.4.6. Deliverables and requirements for Control System Site Acceptance Test

The system site acceptance test (SAT) is intended to check conformity with ESS requirements of the system implemented first as a stand-alone. Control System SAT is part of the system SAT. All I&C equipment shall be powered and tested during SAT.

Control System SAT is first a repeat of FAT for each implementation involved in. In addition, the SAT will include a performance test of the whole system where possible. Attention shall be paid to checking of system interlock (machine protection) and personnel safety functions as they may be integrated with the whole control system for the first time. During SAT, the control system will be connected to Integrated Control System (ICS).

Deliverables for Control System SAT:

[D25] A single report collecting all SAT results related to I&C will be issued.

Rules required for Control System SAT:

- The results of SAT shall be recorded and retained in the lifetime records of ESS. Any failures during SAT shall be investigated and the cause and rectification of the failure documented in the SAT report.
- SAT is performed with EEE. EEE may be complemented by specific tools for the MPS and PSS.
- Data links with EEE not tested during FAT shall be tested during SAT.
- For process control and performance test purpose, the system shall be tested under a scenario and acceptance criteria provided by the System Responsible Officer. This scenario shall include the individual tests of every system control function with the real process connected to the control system and the test of the system as a complete autonomous system as close as possible. This process control and performance test is out of scope of ICS Handbook.

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

4.4.7. Control System Integrated Commissioning

This phase is not in the scope of ICS Handbook.

4.4.8. Control System Operation and Maintenance

This phase is not in the scope of ICS Handbook.

4.4.9. Deliverables and requirements for Control System Obsolescence Management

It shall be possible to replace control system equipment to cope with maintenance issues, control system upgrades, hardware or software obsolescence, or as a result of it becoming increasingly expensive to operate and maintain.

Deliverables for Control System obsolescence management:

[D26] A proactive management plan for obsolescence describing the strategies for identification and mitigation of the effects of obsolescence throughout all stages of Control System life cycle. This management plan shall be produced during the design phase and maintained through all the phases.

Rules required for Control System obsolescence management:

- The latest ICS Handbook version available shall be applicable when the TA is signed.
- ESS is committed to support old versions of ICS Handbook standards, including the obsolescence management of those standards.
- Every new I&C equipment shall be documented in the same way as was required for the initial procurement.
- Training for operation and maintenance teams shall be included in the process of replacement, if required.
- The System Responsible Officers shall define requirements for their control system backup and storage by successive evolutions and the strategy to adopt in case of obsolescence.

4.4.10. Control System Decommissioning

This phase is not in the scope of ICS Handbook.

4.4.11. Requirements for Control System Documentation

- All documentation shall be in the English language.

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

- All documentation shall be available in electronic format (PDF, Open Document XML format or Microsoft Word) and in an online version which is accessible using ESS product lifecycle management system.
- All documentation shall be under version control.
- For every item (including 3rd party and COTS) the original documentation shall be delivered.

5. SYSTEM ARCHITECTURAL DESCRIPTION

5.1. Introduction

This chapter outlines the architecture of the ESS Integrated Control System (ICS). However, the Personnel Safety System (PSS) is out of the scope of this explanation and will be defined in chapter 0.

The technical implementation of the functions described in this section is described in the respective sections that follow (6,7, 9 and 10).

5.2. Integrated Control System Architecture

The ICS is a distributed, network-based control system that allows the ESS facility to be operated as an integrated unit from a single central control room. More specifically, the ICS provides:

- A control system based on EPICS [8] for the accelerator, conventional facilities, NSS, and target subsystems,
- A timing system for synchronization of the machine components,
- A control system infrastructure including a technical network, computing, and data storage capacity and a main control room,
- A machine protection system inhibiting beam operation upon the detection of a non-nominal condition that would lead to beam-induced damage of equipment
- Software tools and support to efficiently manage configuration, operation and maintenance of the control system

As the system is highly distributed, a large number of connections between the system components are required for the system to function as an integrated unit.

5.2.1. Connections between subsystems

The control system comprises a number of computing nodes that are attached to facility subsystems to perform input and output, thus called I/O controllers (IOC). A number of networks connect these computing nodes together. In addition the control system also provides a set of services running on server computers and software for client workstations to access the control system for operation.

A computer network based on Ethernet carries the data and control information between the nodes of the distributed system, i.e., the IO controllers, server computers and client workstations. This network, the Technical Network, is the backbone of data transport in the control system. It is described in more detail in chapter 7.3.

Several components of the ESS facility need to be synchronised to each other. In the control system, this is done by a timing system that can distribute synchronous triggers

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

and data to the control system nodes, and also distribute exact timestamps. Details about the timing system can be found in chapter 7.2.

The proton beam can cause damage to the facility components if it is not steered properly. For that reason, a machine protection system (MPS) is also an integral part of the control system. A physical component of machine protection is the beam interlock system (BIS) that stops beam operation if a potentially harmful condition is detected. The machine protection system is explained in more detail in chapter 9.

The interconnections of the IOCs are shown in Figure 2. **All** ICS systems that use EPICS are connected to the Technical network. **Most** systems receive timing signals from the central timing system and are thus connected to the Timing Distribution Network. **Many** systems, mostly in the accelerator, are connected to the Beam Interlock System.

Connections from the IOCs to the physical I/O can be directly from the IOC via either I/O cards (as in MTCA.4 AMCs) or via a fieldbus (e.g., EtherCAT, Serial RS-232 port or regular Ethernet). In many cases, I/O is connected to a PLC using the PLC vendor's I/O modules and the PLC and EPICS IOC communicate via a dedicated Ethernet link.

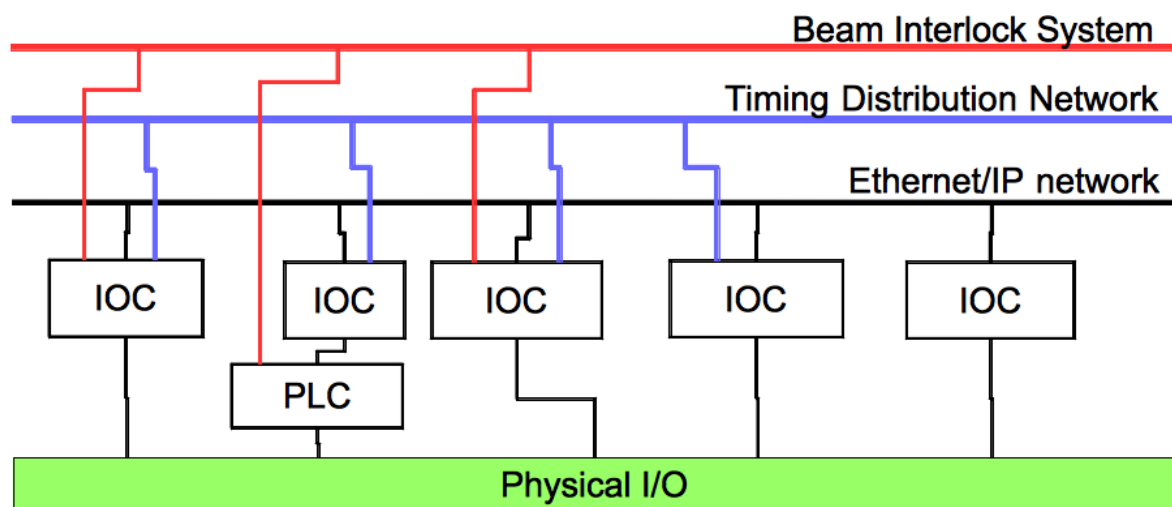


Figure 2 Connections between I/O Controllers

5.2.2. EPICS and the Control System Network

The control system is built based on the EPICS (Experimental Physics and Industrial Control System) software toolkit. EPICS is a client-server system where the servers provide an interface to access data, for example reading physical data from sensors, monitoring status information or sending commands to devices. These servers are called Input/Output Controllers, or IOCs. A server can also provide data from other types of data sources than physical I/O, for instance databases or computed physics models. The

servers can also perform automation tasks independently from any central entities or applications.

The clients in an EPICS system access (read or write) data from servers. Examples of client software are operator GUI panels to monitor or manipulate parameters of physical devices, software that does data acquisition or monitors the status of the facility, or scripts or other software that manipulates the state of the facility, for instance setting the accelerator up when starting operation.

Data and command exchange in the system happens over the computer network, over so called EPICS channels, i.e., connections that carry process variables between the server and client computers.

Thus, all components in the control system that serve or access EPICS process variables shall be connected to the Technical Network and use the EPICS Version 4 pvAccess protocol [9] for communication. This setup is schematically shown in Figure 3. Please note that this picture is accelerator-centric. It does not describe all services and components that ICS will support but provides just a schematic overview of the architecture.

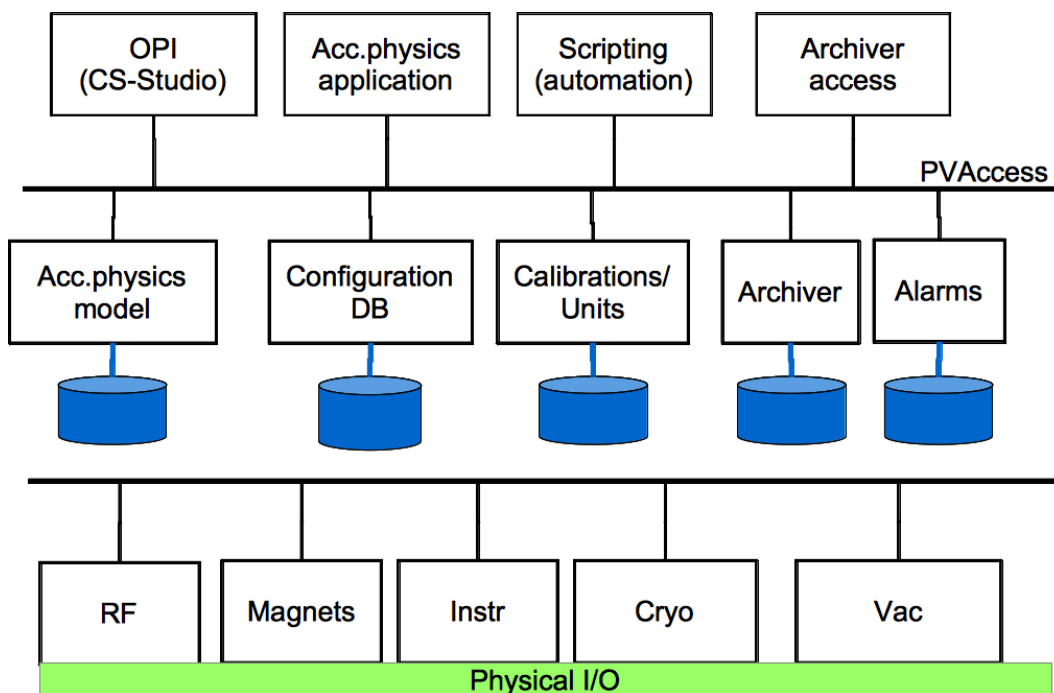


Figure 3 Connections between EPICS servers and clients.

The Technical Network shall be isolated from other networks that are used for general data traffic or office computing, as illustrated in Figure 4.

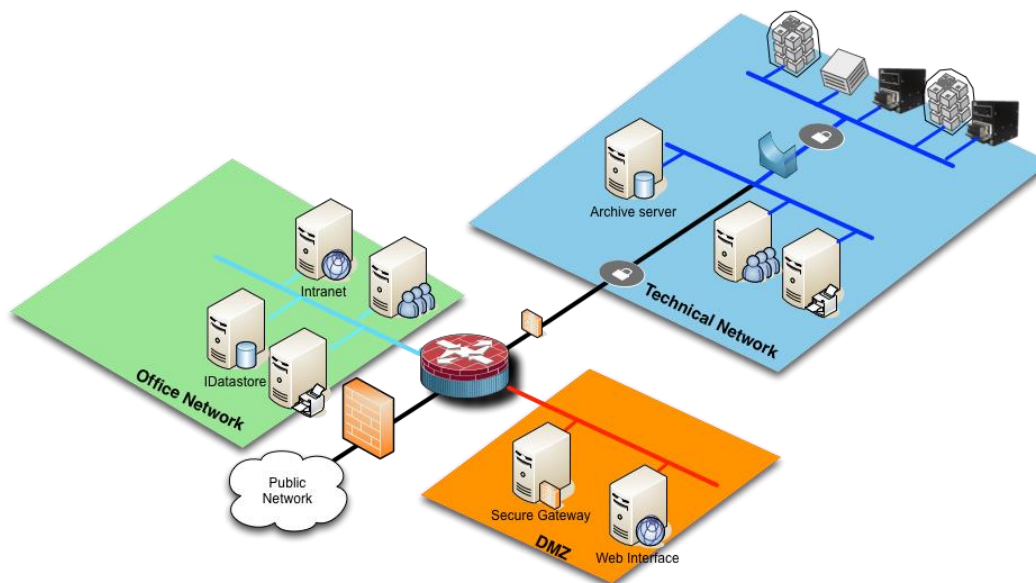


Figure 4. The ESS control system (Technical) network and its relation to other networks.

5.2.3. Timing Distribution

The ESS facility operates with a 14 Hz cycle. In normal operation (up to) 2.86 milliseconds long proton beam pulses are generated, accelerated and steered to the target station at a frequency of 14 Hz. Many of the facility components have to work synchronously with this operating cycle. The Technical Network carries the bulk of the data in the control system but is by its nature not alone sufficient for precisely synchronized and centralized control of the facility. The ESS thus has a timing system that provides a precise synchronisation of the distributed control system (and thus accelerator, target and neutron instrument) components. The timing system is synchronised to the central RF and is able to simultaneously broadcast data and trigger events to a large number of receivers with a deterministic latency.

The timing system provides the following services:

- Trigger signals to subsystems in the facility, for example triggering the RF systems appropriately for beam acceleration
- Clock signals that are synchronous and in phase over the whole facility
- Synchronous transmission of beam-related parameters to all relevant controllers in the facility. These parameters can include things like the beam destination, expected beam mode (beam current, pulse length, repetition rate) and also information from measurements of the past pulse
- Timestamps (“wall clock time”) that are synchronised all over the facility and can be attached to the data collected by the EPICS software
- Repeated distribution of sequences of events that happen in one beam cycle.

The timing distribution is a tree topology network with a mainly downstream information flow is from the central master unit (Event Generator) down to the receivers. The single signal from the master unit is multiplied in fan-out modules to several receivers.

A limited amount of data and events can also flow upstream, i.e., from the event receivers towards the event generator. This can be used for instance to trigger synchronous data collection based on conditions that are detected by an I/O controller down in the facility.

A more detailed description of the timing system is provided in chapter 7.2.

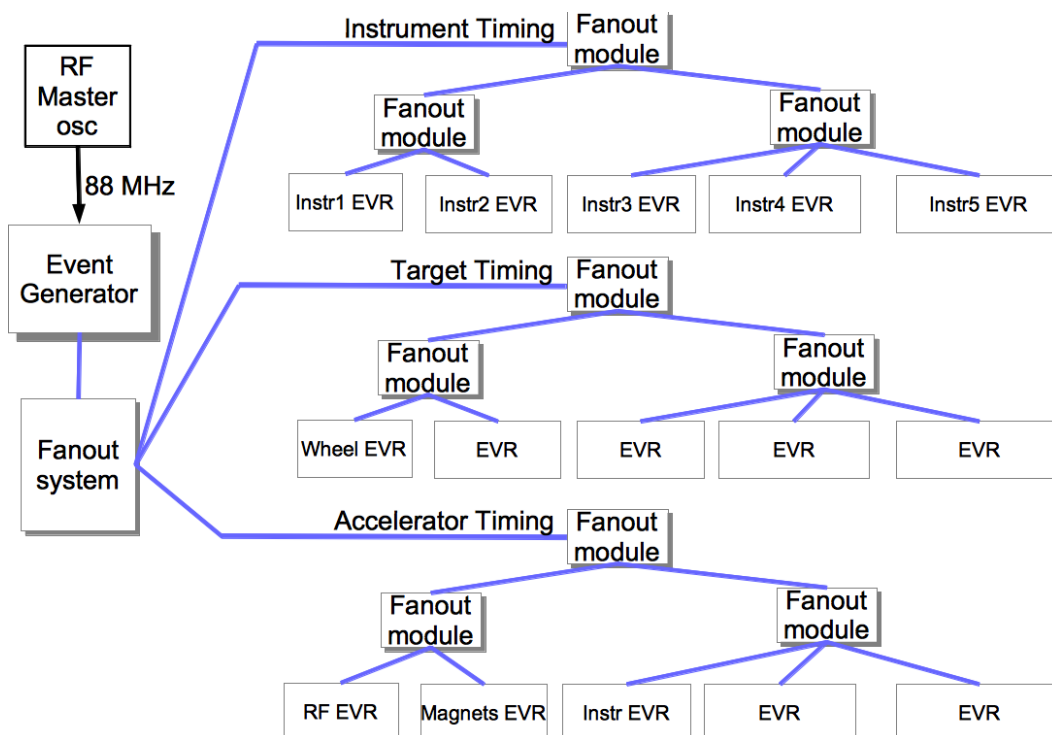


Figure 5 Schematic view of the timing distribution.

5.2.4. Beam Interlock system network

The third type of global interconnection is the Beam Interlock System (BIS). The BIS receives inputs from many sensors (or similar), has a logic unit to process the inputs and produce a signal telling to stop beam production when a condition that could damage the facility components is detected, and a connection to accelerator components that are used to switch of the beam. The BIS and the encompassing entity, Machine Protection System are described in more detail in chapter 9.

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

5.3. Control System Services

Control System Services are software-based entities that complement the functionality of the control system by providing certain centralized functions. These services are provided and maintained by ICS for the whole facility to use.

5.3.1. Archiving service

Successful operation and continuous improvement of the facility requires a means to monitor and analyse its performance over long periods of time. For this purpose, ICS provides a service for collecting and storing data from the IOCs during the facility operation and tools for retrieving and analysing the collected data. The data will be stored for periods that depend on the requirements for the data analysis. For instance, low-frequency data that can be used to analyse the facility performance as a whole will be retained for several years or even through the facility lifetime, whereas detailed high-volume data to analyse the performance of a subsystem may be discarded after a few months.

The archiving system [6.5.1] creates a time-based (in contrast to event-based) data archive, which is primarily intended for performance monitoring of the facility. The archiver is not primarily intended for data acquisition for measurements or experiments.

The data collection and handling policies will be defined in discussion with the facility operators and users. ICS is responsible for setting up and operating the service and also guaranteeing its operation.

5.3.2. Alarms Strategy and Management

One of the central services of the ICS is the alarm system. Alarm system informs system operators (operators, engineers and physicist) about conditions that may, or have already stopped beam operation or can otherwise be harmful to the facility or its components. The alarm system is primarily intended for people that operate the ESS facility from a control room. It may however also be useful for subsystem engineers to inform them about faults or potentially harmful situations in their domain of responsibility.

The alarms shall help personnel to diagnose the cause of an interlock before restarting operation or to take actions to mitigate interrupts. Thus, in difference to the protection systems (MPS, PSS and interlocks), which prevent human injuries, environmental accidents or major machine damage, alarm systems are vital for reducing downtime and maximizing availability.

ESS consists of a large number of sub-systems, which will be designed, configured and commissioned independently. These distributed systems will thereafter be integrated with the ICS. In the operational phase of the ESS project all alarms generated by the sub-systems will be collected by one dedicated ICS alarm handler and displayed to the operators. The alarms will alert operators when they need to take actions to prevent damage to equipment, to avoid unnecessary interrupts in operation and to diagnose causes of interrupts in order to restart.

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

Therefore, the EPICS alarm handler, CS Studio Beast, and other alarm management tools need to provide operators with enough information. On the other hand, the information must not overwhelm the operators, especially not in complex fault situations when alarms are needed the most.

For this reason, it is important that the same design philosophy and rules regarding alarms are imposed on all sub-systems controlled by ICS. Furthermore, this has to be initiated already in the design and configuration phase.

The usefulness of the alarm system will be determined by its *global* properties, that is, the properties shown to the operators. For example, the average rate should not exceed six alarms per hour. This can only be achieved if all the distributed systems are configured with this global goal in mind. As soon as one single sub-system allows a too high alarm rate, the global alarm goals will not be reached.

In a similar fashion, it is important that all local alarm designs use the same naming conventions for equipment, fault types, and severity. Otherwise, it may be impossible for operators to compare and prioritize between different alarms that activate simultaneously.

In short, all alarm sub-systems must be designed with the same goals in mind, or the global performance targets may not be achieved. All design, procurement, and commissioning of alarms for all systems controlled by ICS shall be performed according to the ESS Alarm Strategy [10].

5.4. Operator tools

5.4.1. User Interface tools

The standard tool for user interface applications at ESS is the Control System Studio (CS-Studio).

CS-Studio is an integrated platform for several tools, also called plugins. The most common plugins that belong to ESS standard setup are:

- A display manager, a tool that can be used to create EPICS graphical user interfaces without programming. The current ESS standard display manager is BOY.
- A trend graph display tool that is used to show control system values as a function of time, often referred to as stripcharts. Data Browser is the ESS standard tool and it is able to display both live data as well as archived data.
- An alarm display tool, part of the BEAST distributed alarm system toolkit. In addition to the display tool, BEAST comprises an alarm server plus a relational database for configuration and logging.

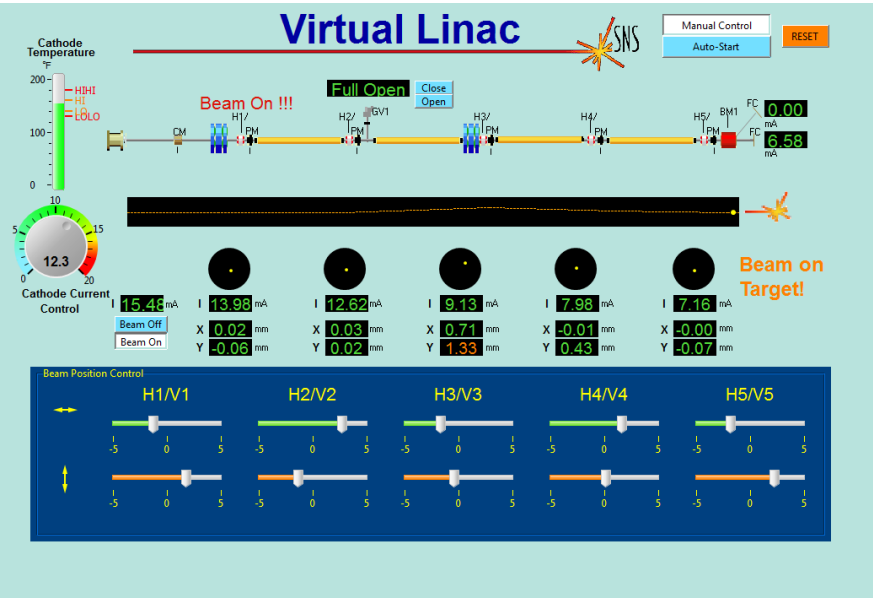
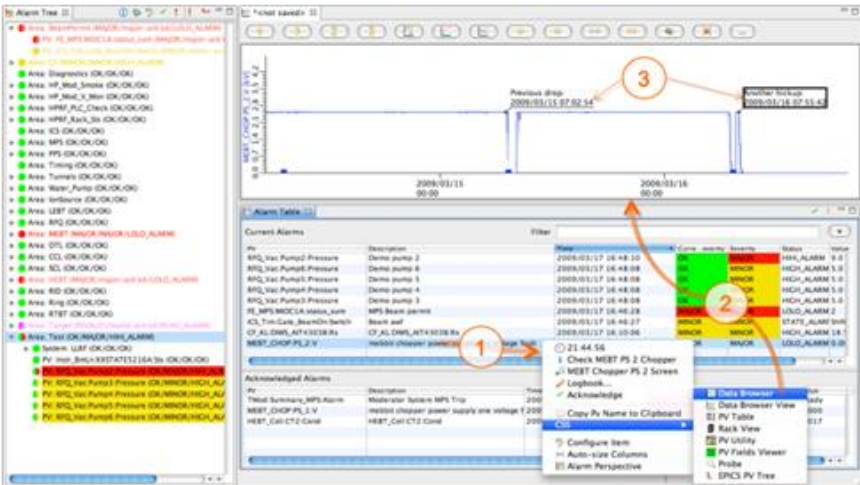


Figure 6 Example of a BOY graphical user interface screen, also known as OPI, or HMI



Figure 7. Example of a DataBrowser plot.



Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

ICS is responsible of providing the CS-Studio as the part of its standard software distribution. ICS also provides user support and participates in development of CS-Studio as part of the collaboration.

ICS system integrators typically create the graphical user interfaces but depending of the application, GUIs may also be created by other stakeholders like accelerator operators.

5.4.2. Machine setup management

For facility operation and tuning, it is essential to have a tool to save the state of the machine set points and to restore them on demand. The EPICS collaboration has developed a number of tools for this purpose. At the time of writing the final decision of the tool is still open, but there are several candidates under evaluation, for example MASAR (MACHine Snapshot, Archive and Retrieve).

For the immediate needs, a simple tool like PVTable or Channel Access SaveRestore is sufficient. ICS will provide a final solution by the time when central control room operation will start.

5.5. Accelerator physics applications and support

ICS will provide services for accelerator physics applications. In particular a physics model service based on OpenXAL and a framework that supports writing physics applications based on the model service. The supported language for writing physics applications is Python.

The input for the physics model, known as the lattice, comes from a tool called LinacLego. At a later stage (to be defined), LinacLego is planned to be replaced with a database tool.

5.6. Control System Configuration Management

For the purpose of building and maintaining the control system and also other facility components (to be defined), ICS will provide a set of configuration management tools. These tools serve the purposes of modelling the facility (plant model), providing data for maintenance and operation, documentation of the facility and configuration of software applications that are used in the facility.

A central part of these tools is a database , the Controls Configuration Database (CCDB) for storing configuration data, namely data about system components, their relations and properties. This database will provide a controls-centric model of the facility (accelerator, target, instruments) “as built”.

To support CCDB, a separate database for storing cabling information (Cable Database), is provided. This database stores the data about properties of standard cable types used at ESS and also the individual cables to connect system components.

In the control system domain, the configuration tools provide input for the EPICS control system as illustrated in Figure 9. The light blue elements belong to the configuration management, the red elements are user tools and services.

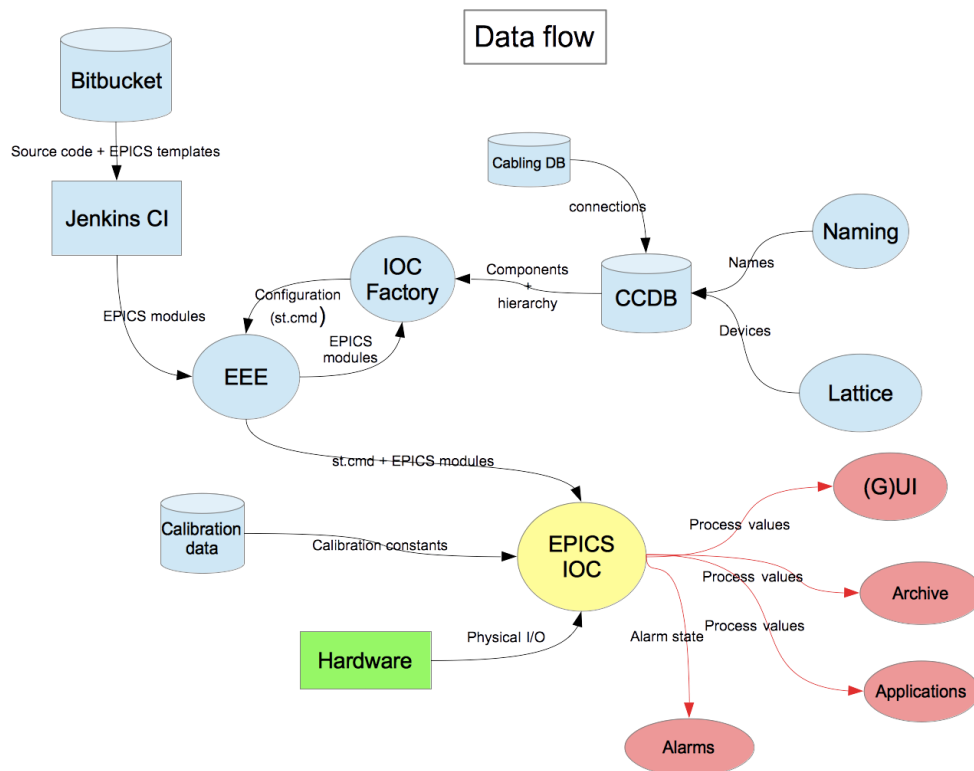


Figure 9. A graph illustrating the flow of configuration data.

5.7. Naming Convention

When built, ESS will have a very large (estimated to be around 1.5 million) number of control points, also known as process variables (PV). In EPICS, all the process variables are addressed by their names that have to be unique across the facility. Thus, proper definition and management of the names is necessary for successful operation of the facility.

The ESS Naming Convention is a standard to ensure meaningful, short and structured naming of signals and devices.

The standard originates from experience at research facilities similar to ESS and was approved at an early stage of the ESS project. The ESS Naming Convention is a controlled document available in CHESS [11].

An online reference is available in [<https://ess-ics.atlassian.net/wiki/display/NC>].

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

5.7.1. Scope of the Naming Convention

The ESS Naming convention applies to devices and signals controlled and monitored by the Integrated Control System (ICS). ICS emphasizes the importance of the naming convention, since the functionality of the system may be compromised if:

- the signal names, referred to as process variable names in EPICS based Control System, do not follow the naming convention format and rules given below.
- the associated device name of the process variable name is not registered in the web-based Naming Service provided by ICS.

Equipment outside of the ICS scope will be named if requested. For example, safety valves like pressure relieve valves and manual valves are not controlled but could nevertheless be named and also displayed on control screens.

The ESS Naming Convention names shall be used on operator screens, drawings, design schematics, computer software, project databases, equipment name tags, test procedures, and other sources of technical information at ESS.

The device names shall not be confused with identification of components in inventory since the naming convention names reflect the function of the devices and their physical (installation) location whereas inventory identification applies to a specific piece of hardware. When a component is replaced, the new component inherits the device name.

The device names shall not be confused with identification of components in inventory since the naming convention names reflect the function of the devices and their physical (installation) location whereas inventory identification applies to a specific piece of hardware. When a component is replaced, the new component inherits the device name.

5.7.2. Responsibility and Support

The responsibilities are delegated as:

- **Management:** The ICS chief engineer is responsible for the Naming Convention document and the signal list available at:
<https://ess-ics.atlassian.net/wiki/pages/viewpage.action?pageId=21758278>
- **Data:** The ICS Integration team is responsible for user access privileges, data and structures tree in the Naming Service.
- **Software:** The ICS Software team is responsible for maintenance, development and support of the Naming Service software.

6. CONTROL SYSTEM SOFTWARE STANDARDS AND SPECIFICATIONS

This section provides details about the implementation of software services and systems that have been introduced above, and the infrastructure that supports development and maintenance of those services.

The ESS control system will be built in collaboration between the central ICS division in Lund and many in-kind partners. In-kind contributors will design, develop, test and deliver software from their location. All software, be it developed in Lund or at the partner's location, has to be integrated into the control system by the central ICS team who will also be responsible of the operation and maintenance during the ESS operations phase. To make this feasible, software components, frameworks, versions, dependencies and toolkits must be agreed upon by all parties in order to guarantee that all the different pieces can be properly integrated.

6.1. Control System Computing Infrastructure

ICS defines and supports the system platforms required for control system development.

Operating environment for servers, software development and console machines:

- The operating system for server and console computers shall be Linux.
 - CentOS on Intel 86-based hardware, especially servers.
 - Embedded Linux (Yocto-based) on embedded platforms like MTCA.4, except when the architecture is Intel 86-based.
 - Embedded systems like MTCA.4 are booted from a network file system and thus will not have local disks for booting. This will make it easier to manage the large number of embedded IOCs in the integrated control system.
- Virtualization will be extensively used to reduce the amount of hardware servers, to manage obsolescence issues and to achieve a high level of availability.
- For distributed development where it is not possible to use the central services like the ESS Epics Environment (EEE), physical installations of the development environment are supported. This applies in particular to development at in-kind partners. ICS supports the configuration of the development environment but operating the development system is under responsibility of the in-kind partner.

ICS provides support for a number of programming languages to be used in the control system. By support, the following is meant:

- ICS has expertise in that language and can help other developers to solve their problems in using the supported language.
- EPICS (pvAccess) binding is provided for the language and ICS staff has the expertise to help users in solving their problems in using the binding.

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

Supported programming languages for control system client applications:

- C/C++, for EPICS server and client applications, with toolchains:
 - Gnu Compiler Collection (GCC) on Linux (server, x86-based)
 - ELDK or Yocto (with GCC) on embedded Linux platform.
- Java/JDK on backend servers (not embedded I/O controllers) and client software
- Python
 - the supported Python-EPICS interface library is pvaPy [18]

Database backend

- PostgreSQL [19] is the standard database management system of ESS for relational databases. However, every effort shall be made to minimise the dependency on any particular database management software.
- Recently several applications for “nosql” databases have emerged. As this field is new it is too early to nominate a standard. Developments in the community shall be followed and a standard defined at an appropriate point in time.

Application server

- Wildfly is the preferred application server for ICS web applications.
- Other servers e.g. Tomcat are accepted when the application comes from an “upstream” contributor, for example from the EPICS community.
- However, only Java application servers are supported.

Issue tracking

- JIRA [20] is the supported platform for reporting issues (bug reports, feature requests) for software supported by ICS.
- All issue reporting that concerns ICS software shall be done through JIRA.
- ICS division in Lund defines workflows for issue handling that are to be followed by all involved parties
- Each subgroup in ICS can define in detail how to handle the issues listed below. However, the rules towards in-kind partners and other stakeholders shall be the same as for internal developers and shall be clearly communicated. This concerns the following:
 - **Resolving and closing JIRA issues.**
 - **Assignment of JIRA issues to the responsible persons.**

Version Control

- ESS uses GIT as the backend version control system. The repositories are hosted on ESS BitBucket [21]site.
- Rules for the repository: branching, tagging, etc. (**revise or delete this: <https://ess-ics.atlassian.net/wiki/display/DE/Revision+Control+Process>**)

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

Software build system

- Continuous integration, Jenkins (**revise this:** <https://ess-ics.atlassian.net/wiki/display/HAR/Jenkins>)

Testing

- **Some info here:** <https://ess-ics.atlassian.net/wiki/display/HAR/ICS+Test+Environment>

6.1.1. Architecture of Services

Access to the Services that are defined in 6.4 shall be through a RESTful interface [22] in the case of Web applications. For data that needs to be accessed by the IO controllers or control room applications, an EPICS V4 pvAccess interface will also be provided. Direct SQL access to databases is not allowed for maintainability reasons.

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

6.2. ESS Software Development Environment

The Integrated Control System Division (ICS) has the mandate to specify and/or provide all the tools needed to build software for the commissioning and operation of the ESS and to make it available to ESS staff, in-kind partners and other external partners. This includes EPICS applications, scripting environments, physics simulators and commissioning tools among others. This set of tools is provided as an installation package for physical machines and packaged virtual machines. In both cases the system contains all the libraries, software components and frameworks that are needed to develop software for the ESS Controls Systems.

ICS uses virtualization technology and a configuration management system to provide a cutting edge development environment where the entire software infrastructure can be described as code and properly stored in a version control system, tested and tagged. Rollback to a previous setup shall be possible if problems with a new release come up.

The following components have been already identified and they are part of the software suite provided by the ICS Development Environment:

- EPICS development environment. This involves EPICS base and modules needed for the development of EPICS low level software for the IOCs.
- CS-Studio [23]. Eclipse-based collection of EPICS client tools to monitor and operate accelerators. One of the key components of this suite is BOY. BOY is an Operator interface (OPI) development and runtime environment for creating user interfaces without the need of programming.
- OpenXAL [24] is an open source development environment used for creating accelerator physics applications, scripts and services. OpenXAL contains a physics model of the ESS machine that lets the developer simulate the ESS accelerator and to communicate at the same time with the physical devices of the machine.
- Jupyter Notebook [25]. Open source interactive data and scientific environment. Jupyter Notebook is currently used by ESS to provide a scripting environment for physics applications. Currently ICS provides support for Python. It is possible to run simulations in OpenXAL and MANTID [26] (open source framework for high-performance computing and visualisation of material science data).

6.2.1. The Development Environment Architecture

The Development Environment is the software and the supporting infrastructure for development at ESS and at in-kind partners. The main constituents of this setup are the Development Machine on which all development is to be performed and a centralized file server hosting the ESS EPICS Environment (thus “EEE server”). This server needs to be accessible by Development Machines and IOCs. One Development Machine is expected per user and one EEE server per location. Both (Development Machine and EEE server) are released in numbered versions to ensure a standardized environment for all users. Servers at different locations are synchronized one way from ESS outwards to ensure stable versions of EPICS related software that are up-to-date.

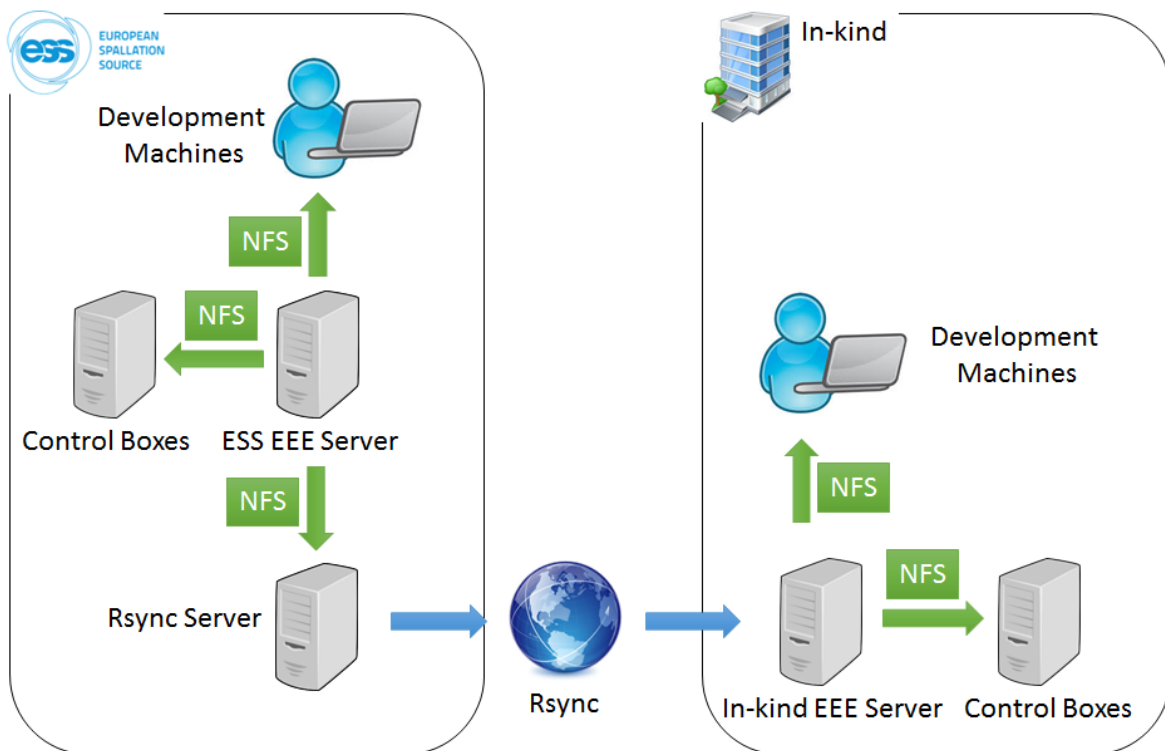


Figure 10. Schematic view of the Development Environment.

A development Machine can be a Virtual Machine (VM) or a physical machine on which all software development is performed.

EPICS deployment is managed by a system that is called the ESS EPICS Environment (EEE) [See chapter 6.3]. EEE does not reside on the Development Machine but is instead placed on a centralized physical server. It is made available to the Development Machines and IOCs through a Network File System (NFS) mount which enables them to access the same files on the server without keeping a local copy. EEE server is also a boot server enabling IOCs to boot and mount their root file systems from it. Each partner that develops EPICS IOC software or modules should have one EEE server.

When new functionality is added to the EEE server at ESS, it should not only be available to ESS but also to external developers. This is achieved by periodic one-way synchronizing of in-kind EEE servers with the ESS EEE server. Synchronization is performed over the Internet using Rsync [27]. More specifically, EEE residing on the ESS server in Lund is NFS mounted to the **Rsync Server**, which makes it accessible to Rsync client software installed on In-kind EEE servers.

6.2.2. EPICS development workflow

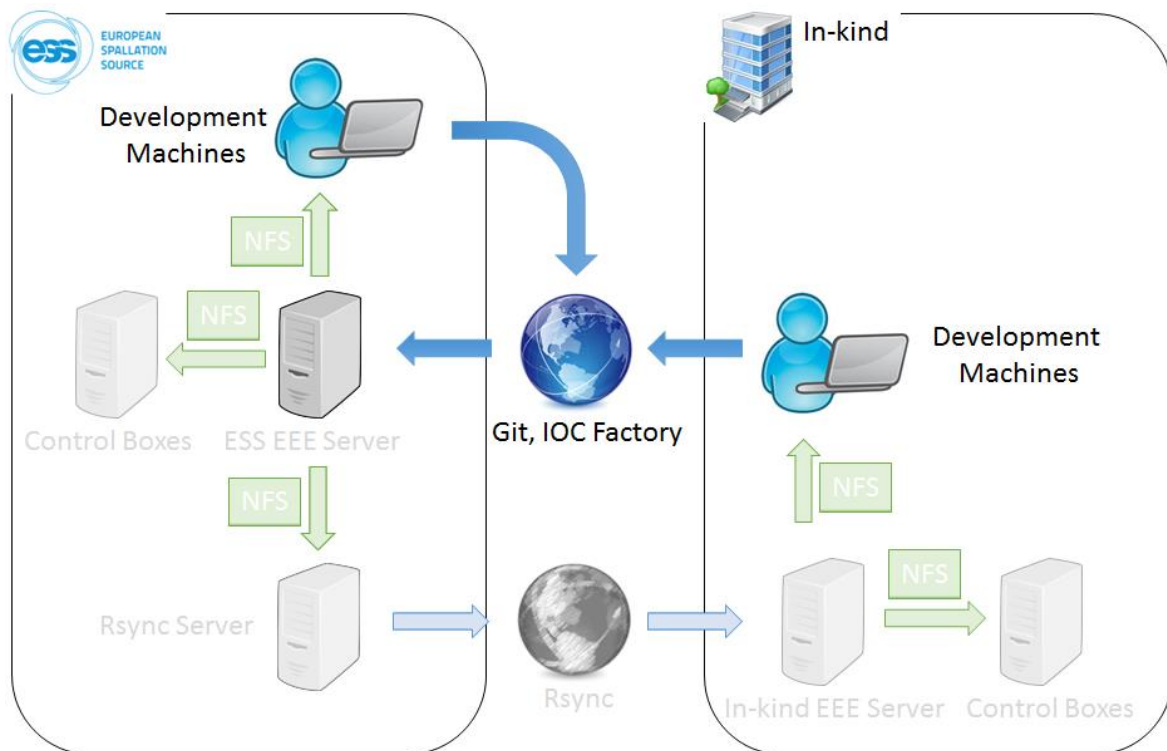


Figure 11. Completing the development loop through the GIT repository.

Pushing an EPICS module with a numbered tag into the ESS git-repository will trigger a build process that, if successful, will install the module in the ESS EEE Server with the numbered tag. This will be done by the Deployment Server, which is not shown in the image for simplification.

Modules can be installed locally [12] on the In-kind EEE server and will be tagged with the username that installed them. Note that these will not appear on the ESS EEE server. Please refer to the section 4.4.3 of this document for detailed information about the EEE.

6.2.3. IOCs (Input Output Controllers)

Developers at ESS and at in-kind partners can configure EPICS IOCs in a standardized way using **IOC Factory**, which is accessible through a browser from any machine. IOC configurations that are generated using the IOC Factory will be placed on the ESS EEE Server for immediate use. IOCs deployed directly to a local EEE server will however not be synced with any other partner sites.

Note that once changes are deployed on the ESS EEE server they will further be synced to in-kind NFS servers and therefore available to partner machines as explained in the Architecture section above.

6.2.4. Management of the Software Development Environment

Ansible [13] has been selected as the computer configuration management system for ESS. It is an open source system used to automate the configuration of IT systems, deploy applications and provision software in both new and existing systems. Ansible can also be

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

used for software orchestration, where not only the configuration of the systems is important but also the order in which they have to be configured. The basic unit of Ansible is the playbook. We can think of the Ansible playbook as a script where we can describe the configuration of our system. All the configuration of ICS servers, ICS development machines, all ICS machines in general are described in Ansible playbooks. Ansible allows ICS to describe all software infrastructures as code (IaC) and to keep such configuration in a version control system such as Git. This lets us version the current configuration of ICS systems and therefore keep control of the updates, and even perform rollbacks.

The physical and virtual machines are configured from the same source of information: a set of Ansible playbooks describing the configuration of the ICS development environment.

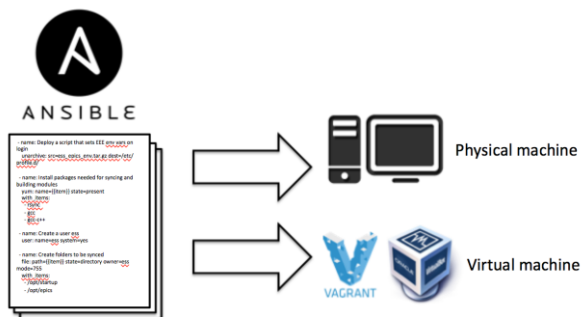


Figure 12 Ansible is used for the configuration of virtual and physical machines

ICS uses the Atlassian cloud implementation of *Git* repository called *Bitbucket* [21].

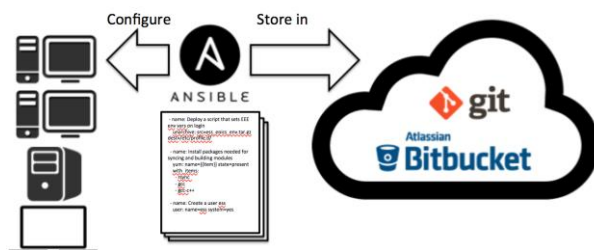


Figure 13. Ansible playbooks used to configure ICS systems are stored and versioned in Git

6.2.5. The ICS Virtual Development Environment

Vagrant[14] has been selected as the ICS standard way to create virtual environments. Vagrant lies on top of virtualization providers such as VirtualBox, VMWare, AWS and so on. At ICS, Vagrant is used on top of the VirtualBox [15] provider.

Using Vagrant, it is possible to configure a virtual environment by describing the configuration in a file that is called **Vagrantfile**. This configuration file provides all the setup needed to configure a virtual machine properly, including the reference to Ansible playbooks, which install the appropriate versioned software. This way of configuring the virtualization environment spares the end-user of doing the configuration himself. That

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

also brings a huge benefit when automating the creation and management of virtual machines. On top of all that, being able to describe the virtual machine configuration in a file allows us to keep the configuration under version control. This means that the virtual environment can be properly versioned, and previous versions can be restored easily. In Vagrant the user normally manages the virtual environment with a very simple command line interface. Typical commands are: “*vagrant up*” to start the virtual machine, “*vagrant halt*” to stop the virtual machine or “*vagrant reload*” to reload the configuration from the Vagrantfile.

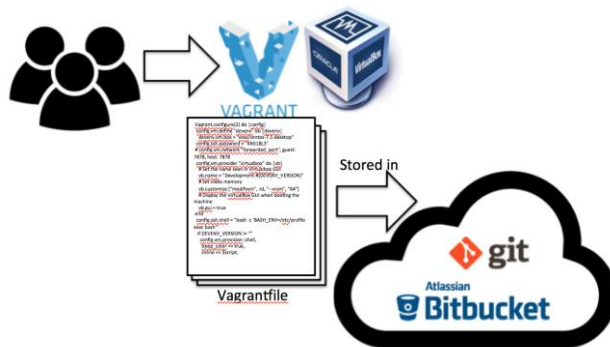


Figure 14 Vagrant uses the playbooks stored in Git to populate the virtual machines

A key benefit of using virtual machines for the development environment is that they can be treated as disposable environments. If for any reason the environment gets corrupted the virtual machine can be discarded and a new one created within seconds. That gives the user freedom to work with the environment without being worried about breaking it. For this to work, it is very important that user’s data and code are kept outside the virtual machine. Vagrant and VirtualBox provide the concept of shared folders. Using shared folders the users can maintain source code and important data in their host environment whereas the code can be also accessible from the virtual machine. Data can also be shared among virtual machines using shared folders.

The user is always able to install additional packages in the virtual machine, although we encourage keeping it as standard as possible. In most of the cases, the users just want to modify the virtual machine in order to install their preferred IDE. In that case we encourage users to install the IDE in their host (laptops or desktop computers) and to use shared folders to work on the code that later on can be run in the virtual machine. This implies that the users can use their original development environment, with no modifications, and still use any editor or tool.

6.3. EPICS development

At ESS, EPICS base, EPICS modules and parts of IOC start-up are managed with a custom framework called the ESS EPICS Environment (EEE) [16]. Here, “EPICS base” refers to the EPICS core software developed by the community and available for download at the EPICS collaboration website [8]. Modules in the ESS convention are packages of software or configuration that may contain EPICS driver and device support code, EPICS record

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

templates, configuration files and similar, to be used on top of the EPICS base to implement specific functionality. A functional EPICS IOC is built by configuring a set of modules and loading them on top of the IOC software that is included in the EPICS base. See [16] for more detailed explanation.

The main use cases of EEE are the following:

- Building and installing EPICS modules for multiple EPICS versions, architectures and operating systems.
- Managing all installed versions of EPICS and EPICS modules within a single environment.
- Choosing the versions of EPICS base and EPICS modules to build other modules against.
- Choosing the versions of EPICS base and EPICS modules that a particular IOC uses as part of IOC configuration.
- Resolving dependencies between EPICS modules at build time and IOC start-up time.

The EEE framework has been designed to minimize the overhead of managing the above and provide a fast development cycle. EEE consists of the following components:

- A single directory tree where all versions of EPICS base for all architectures are installed in a standardized structure.
- A single directory tree where all versions of all available EPICS modules for all versions of EPICS base and architectures are installed in a standardized structure.
- An extension of the EPICS build system that builds EPICS modules for a configurable list of EPICS base versions and architectures, handles all types of resources a module can provide, handles build dependencies between modules and installs modules into appropriate locations.
- An IOC shell command that dynamically loads a particular version of an EPICS module and recursively loads the appropriate versions of all additional modules it depends on.
- A script that adds boilerplate code to an IOC startup script at runtime so that it isn't necessary to repeat it in each startup script.

The EEE framework implies the following:

- Development of EPICS modules can be distributed, but to be deployed at ESS, an EPICS module has to be included in the ESS Software Repository (BitBucket)
- Modules in the ESS repository are available for all EPICS applications and shall be used for systems that will be deployed in ESS.

A list of modules is available on the ICS Wiki [28], and will be kept up to date by the developers.

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

6.4. ICS Configuration Management Tools and Services

The integrated control system will be a very complex and large system that is impossible to manage without tools to support the construction, configuration, operation and maintenance of the ICS.

6.4.1. Naming Service

Web-application to create and retrieve information about devices names is available at: <https://naming.esss.lu.se>

6.4.2. Controls Configuration Database (CCDB)

The Controls Configuration Database (CCDB) enables the collection, storage, and distribution of (static) controls configuration data needed to build, commission and operate the ESS control system.

More specifically, the CCDB manages the information of (physical and logical) devices such as cameras, PLCs, IOCs, racks, crates, etc., connected to the ESS control system by defining their properties and relationships from the control system perspective.

This information enables both end-users and related ICS-applications (e.g. Cable Database, IOC Factory) to perform the functions that require use of configuration data.

The main purpose of the CCDB is to build a “plant model” by defining the hierarchical organisation of the components stored in it. For instance, the location of a certain device can be defined and tracked from the device to the rack containing it, to the room where the rack is and to the building where the room is located. Similar hierarchies are foreseen for tracking the supply of electrical power to the components and the integration hierarchy to the control system.

The integration hierarchy, which describes the relation “controls/controlled by”, enables control system users to track down the components in a processing chain, from an EPICS PV on a GUI in the control room to the specific IOC in the facility.

The powering hierarchy enables users to track the source of electric power for a specific device. This is useful to analyse problems with the electrical distribution.

Control system integrators, who are responsible for data entry, verification and updates, will maintain the data in CCDB.

Documents from the website: <https://ess-ics.atlassian.net/wiki/display/CDM/Controls+Configuration+Database> have to be put into CHESS so that they can be referenced from here.

6.4.3. Cable Database, CDB

The Cable Database (CDB) manages information about cables that are required to connect the devices together.

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

More specifically, the CDB supports the tracking, configuration and labelling of cables in all phases of the ESS project (design, installation, maintenance and troubleshooting). Information about approved cable types and their properties is stored in the database. Also the information (type, length, endpoints, id-number) of each individual cable instance shall be stored in the CDB.

This information enables end-users and other ICS applications (e.g. CCDB) to successfully perform their tasks, for instance tracking down a signal through the plant.

Documents from the website: <https://ess-ics.atlassian.net/wiki/display/CDM/Cable+Database> have to be put into CHESS so that they can be referenced from here.

6.4.4. IOC Factory

The IOC Factory is an application for managing IOCs at ESS. It is designed to maximize the Integrated Control System (ICS) division's productivity by providing a consistent, formal and centralized approach on how IOCs are configured, generated, browsed and audited (which would otherwise have to be performed manually). By managing, the following use cases are meant:

- Configure IOC
- Generate IOC
- Browse IOC
- Audit IOC

The "Configure IOC" allows the user to select and configure a set of EPICS modules for a certain IOC to use to access the devices it controls. In principle, every time that the topology of the IOC evolves (i.e. the layout of devices that the IOC uses changes) the user creates a new configuration to reflect these changes.

The "Generate IOC" allows the generation of an IOC instance according to a certain configuration selected by the user. The generated IOC is stored in the EEE server for development or production, depending on what the user has selected.

The "Browse IOC" allows the user to retrieve, organize and display information about historical (i.e. past) generation of IOCs. It gives a broad view/understanding of when, how and why a certain IOC was generated in the EEE server and by whom.

Finally, the "Audit IOC" enables the user to track the changes that may have been done locally to an IOC stored in the EEE server. To enable quick troubleshooting and fixing of issues, it is not practical to restrict direct access to the local configuration of an IOC. The Audit mechanism makes it easy to see what are the differences (if any) between a configuration generated by IOC Factory and the contents of the corresponding directory in the EEE server.

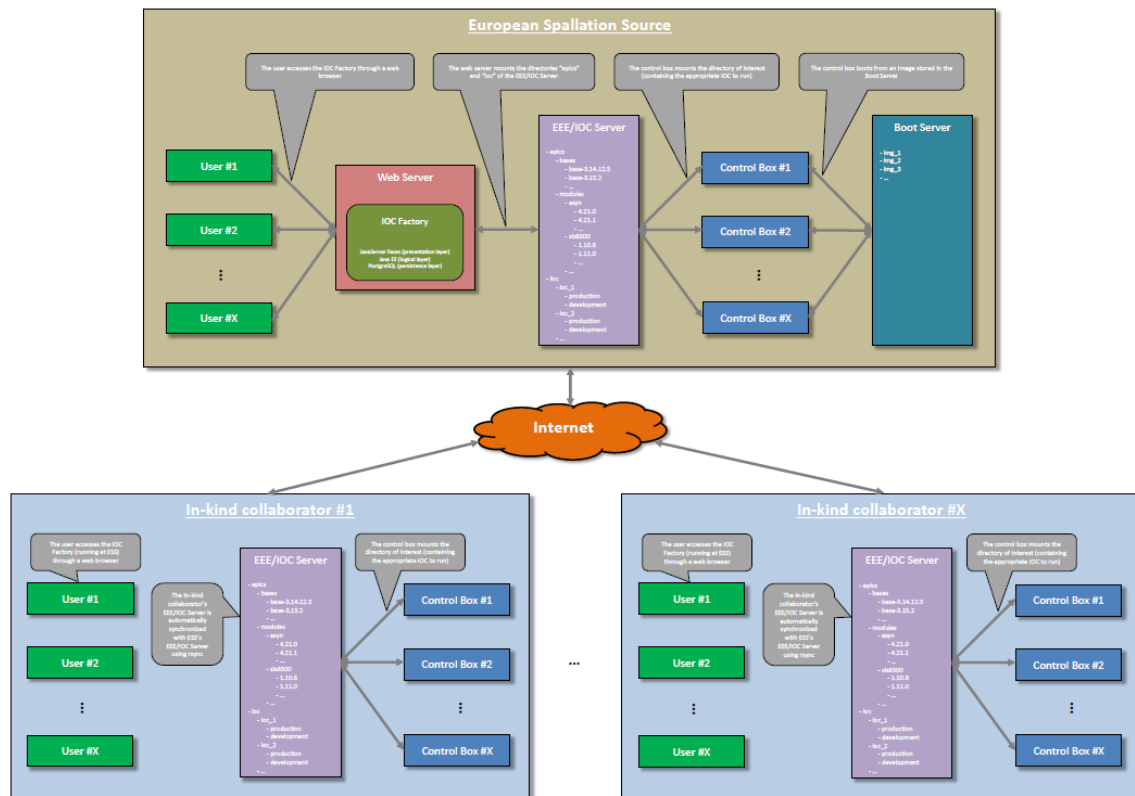


Figure 15. IOC Factory deployment

Website: <https://ess-ics.atlassian.net/wiki/display/CDM/IOC+Factory>

6.4.5. Lattice Database

The ESS accelerator lattice information will be collected by the Accelerator division using the LinacLego tool.

The purpose of LinacLego is to coalesce all relevant information needed for accelerator physics and related applications into a single source. It is an XML-based system for describing a linear accelerator lattice in an organised hierarchical manner.

For ICS purposes, device data is extracted for use in e.g., the accelerator physics application environment. At a later stage the data in LinacLego is foreseen to be managed in a database by ICS.

6.4.6. Channel Finder

Channel Finder is a directory service to enable management of a big EPICS-based control system with a large number of EPICS records.

The name space of the EPICS Channel Access protocol is flat. A sound and thoroughly enforced naming convention solves the problem of creating unique predictable names in

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

the system, but it does not remove the need for having each application configured explicitly with all channel names it may be interested in. Channel Finder tries to overcome this limitation by implementing a generic directory service, which can be queried by the applications for lists of channels matching certain conditions.

Overview documentation (community): <http://channelfinder.sourceforge.net/ChannelFinder/>

The Channel Finder can provide us with dynamic information from all IOCs that have been started in the system.

6.4.7. Other supporting applications

6.5. EPICS Services

The control system provides also a set of services that enable operating and maintenance of the facility. The most important services are listed in this chapter.

6.5.1. Archiver

An archiving service is a channel access client that automatically records PVs as a function of time and then stores them to disk. Examples of data to be archived are the delivered proton beam current and beam power or beam orbit data. Also key values from each subsystem like RF power, vacuum readings, magnet currents and operating status will be archived. Data from the archive can be retrieved for analysing the performance of the accelerator or its subsystems. Archived data is retained for long periods, depending on how the data is required to be used.

The archiver can be configured to sample at a periodic rate or it can post a channel access monitor on PV. The data can be viewed at a later date using several tools. At ESS, the chosen solution to implement an archiving service is the Archiver Appliance (AA). The AA aims to archive millions of PVs and has the following main features:

- Ability to cluster appliances and to scale by adding appliances to the cluster.
- Multiple stages and an inbuilt process to move data between the stages. This supports the ability to use faster storage (which is perhaps limited in size) to improve performance.
- Ability to reduce (decimate) the data as it moves into a store.
- Various metrics to help with capacity planning.
- Ability to define system-wide defaults for archiving parameters using policies.
- Ability to configure various archiving parameters on a per PV basis.
- Support for retrieval of data using CS-Studio, the ArchiveViewer and Matlab.
- Focus on data retrieval performance.

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

More detailed information about the Archiver Appliance can be found in [29] and [30].

6.5.2. Alarm Service

- EPICS Alarms handler
- Control System Studio BEAST (Best Ever Alarm System Toolkit)
- Other Alarms management tools: To be defined

For further information on alarm strategy and management see section 5.3. Information about the service implementation can be found at [31].

6.5.3. Logbook

The Logbook is to be defined and developed. The current logbook (alpha version) is available as a web application at [32].

Save, Compare and Restore

The “Save, Compare and Restore” service is used to save the state of the facility or part of it (accelerator, target, instrument), to be able to restore the facility to a known state at a later point in time. This is achieved by saving the values of a set of PV values into a “snapshot”, by providing means to compare live values from the facility with saved ones and to restore the live PVs to the values in the snapshot.

For now, the save and restore utilities available in CS-Studio will be used. If the operational requirements cannot be fulfilled with these utilities, another solution may be provided upon evaluation of the requirements. The final solution will be announced at a later stage.

6.5.4. Other EPICS services

ICS also supports the SaveRestore service, also known as Bumpless Reboot. This is a service that enables an IOC to save its state over restarts. That is, if an IOC needs to be restarted, it automatically re-establishes the conditions it had before the reboot. This is done by saving EPICS PV values to a (remote) disk during normal operation of the IOC and restoring them back in the IOC startup process, before the IOC resumes its normal operation.

IOC developers shall prepare a configuration file for the service as a part of the development.

6.6. User Interface and other end user tools

6.6.1. Control System Studio

Control System Studio (CS-Studio) is an Eclipse-based collection of tools to monitor and operate large-scale control systems, such as the ones in the accelerator community. It's a product of the collaboration between different laboratories and universities. CS-Studio will be the tool used to build most of the engineering screens.

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

- CS-Studio BOY: Display manager
- CS-Studio Probe: Connect to PV:s
- CS-Studio Data browser: Archive Viewer
- CS-Studio BEAST: Alarm Server for alarm logic, Alarm Clients for GUI:s
- CS-Studio Channel Viewer: Channel Finder

Website: <https://ess-ics.atlassian.net/wiki/display/SCA/Description+of+the+project>

6.6.2. Role-Based Access Control (RBAC)

At ESS, the actions that a user can perform on the control system are controlled by a system called the Role-Based Access Control (RBAC) [33].

The RBAC authenticates and authorizes the user to act on an RBAC protected resource. The main goal of the service is to prevent a user from making a change by mistake, which could lead to a machine shutdown, damage the machine or cause injuries. RBAC is not intended to prevent deliberate attacks on the control system.

The RBAC consists of two separate but complimentary interactions with the user. First, the user must be authenticated when accessing an RBAC protected resource. Authentication is the verification of user identity; i.e. is this person he says he is. At the same time, authentication prevents unidentified users from accessing the RBAC protected resource. After the user is authenticated and attempts to perform an action on the resource, authorization is granted or denied on grounds of roles and permissions. Authorization to write to an EPICS IOC's is determined by the role and/or IP address of the user and the state of the machine. Other RBAC protected resources use the authorization service to grant permission. In both cases, if the user is authorized the action is executed, if not the action is denied.

Developers and users of the ESS ICS that need access to the protected services (configuration services, production IOCs) shall contact ICS to be registered with the proper roles.

6.6.3. Kameleon

Kameleon [34] is a simulator to simulate the behavior of devices or servers that communicate over a TCP/IP connection using a command/response protocol.

Kameleon uses a user-defined configuration file that describes the commands received from a client and, optionally, the reaction to these through statuses sent back to the client.

Possible scenarios where Kameleon may be used:

- EPICS devices integration in general.
- Continuous Integration of IOCs.

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

- OpenXAL (to model devices with a rather complex behavior).

6.6.4. Other tools

Others TBD

7. SYSTEM HARDWARE STANDARDS AND SPECIFICATIONS

7.1. Hardware platforms

The ESS Control System Hardware platforms and the strategy are described in [7]. This chapter summarizes the central points of that strategy.

7.1.1. MicroTCA

The ESS standard platform for the most demanding tasks in terms of data acquisition and online handling is the MTCA.4 standard [35]. These tasks are characterized by:

- need for synchronized actions and processing in real-time (i.e., processing of one beam pulse must be finished before start of the next, in 71 milliseconds corresponding to the 14 Hz operation)
- high-speed processing that requires use of FPGAs or similar technology
- capability to handle large data rates and volumes.

MTCA.4 shall be used when the controlled system requires:

- acquisition of analogue signals faster than 100 kSPS
- precise time synchronization that requires access to the ESS timing system
- clock signals that are synchronised to the main RF source
- generation of waveform data in the range of megabytes or more per second
- actions on the data need to happen within milliseconds or faster

This technology tends to be expensive and requires special expertise so its use shall be limited to cases where the above requirements apply. Typical examples are beam instrumentation and low-level RF (LLRF) controls.

7.1.2. EtherCAT

EtherCAT [36] is a real-time Ethernet-based fieldbus that relies on conventional Ethernet frames but employs a conceptually different mechanism to communicate with multiple devices.

In ICS, EtherCAT is deployed when:

- Beam-synchronous operation is required and
- The data sampling and transfer rates are modest, i.e., 100 kHz or less.
- The I/O is distributed and cabling to a central unit is difficult

More detailed information about EtherCAT is available in the ESS Wiki (<https://ess-ics.atlassian.net/wiki/display/HAR/EtherCAT>), where also an up-to-date list of supported I/O modules can be found.

The main strategy to deploy EtherCAT systems is to use EtherCAT as a fieldbus and a regular IOC platform (MTCA.4 CPU or an industrial PC) as the EtherCAT master. In some

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

applications this may not be appropriate, for instance in motion control applications where an elaborate synchronization of multiple motors is required. In these cases, Beckhoff TwinCAT [37] may be used as the bus master.

7.1.3. PLCs

A programmable logic controller (PLC) is the best choice for most systems that do not require tight synchronisation with the ESS accelerator cycles (14 Hz). ESS has selected Siemens automation equipment as the standard to optimize costs for programming and maintenance.

Consider PLCs when your system:

- needs to have built-in logic that ensures safe autonomous operation of the device under control even if the connection to the upper layer (EPICS) is broken
- has a rate of I/O that is relatively slow (in 10 Hz range) and not bound to the 14 Hz beam rate.
- Cooling systems, vacuum control, (slow) interlocks, etc., are typical examples of areas where PLC is an appropriate choice.

The PLCs are foreseen to be connected to EPICS IOCs that run on virtual machines on robust server infrastructure maintained by the ICS infrastructure team. During development, in cases when the infrastructure is not yet available, it is possible to have the EPICS controllers running on industrial or even regular off-the-shelf PCs. However, this hardware will be removed when the systems will be taken in production.

7.1.4. Other hardware and fieldbuses

There are many components and devices that do not fit into the categories mentioned above and are required to be integrated into the control system. Examples of this kind of components are standalone controllers like power supplies, vacuum controllers, measuring instruments, etc., that have their own internal logic.

The standard EPICS integration solution for this category of systems is the StreamDevice driver. StreamDevice can be used to connect to devices that communicate with a data stream protocol (usually character-based). Typical examples are devices with serial ports, Ethernet connections or some other serial interface.

7.2. Global Timing System Specification

The Timing System provides a complete timing distribution system including timing signal generation with only a few components.

The timing system is capable of generating and distributing different subharmonic frequencies, trigger signals and sequences of events, etc. synchronous to an externally provided master clock reference. ESS timing system is synchronized to the RF Master clock of ESS that runs at the frequency of 352.21 MHz.

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

Support for timestamps makes the system a global time base and allows attaching timestamps to collected data and performed actions.

At the root of the timing system is the Event Generator (EVG) that converts timing events and signals to an optical signal. This signal is multiplied to several branches in fan-out units. From the fan-out units the optical signal is routed to an array of Event Receivers (EVRs). The signal is in effect a bit stream that carries event codes and additional information in data frames at a high frequency, 88.0525 MHz in the case of ESS.

The data frames are 16 bits wide. Each frame carries one event code of 8 bits. The other 8 bits are used for transporting synchronous data and/or distributing eight simultaneous signals, which do not interfere with events. These signals can be for example clock signals, derived from the upstream RF frequency.

The Event Receivers decode the optical signal and produce hardware and software output signals based on the timing events. Event Receivers use a phase locking circuit to synchronize precisely to the event clock of the Event Generator, so the hardware outputs are phase locked to the event clock and thus also to the master RF signal.

The configuration of the timing system components, especially the Event Receivers is done completely using EPICS variables. With EPICS, an EVR can be programmed to respond to event codes in several ways (trigger outputs, software actions) and to handle the data that is distributed through the timing system.

The ICS supports event receivers in both the MTCA.4 platform and on industrial PC platforms.

The ESS timing system will support the following functions:

- Distributing trigger events that define an accelerating sequence timeline. This timeline repeats at 14 Hz even though proton beam is not accelerated in every cycle.
- Distributing beam-related information, synchronized to the machine frequency of 14 Hz. The information consist of machine mode, (intended) beam mode, operating frequency, pulse length and several other items that will be defined in more detail in the Timing System Specification document [1]. The information is broadcast during the accelerator cycle so that it is available at the event receivers in time before the start of the next cycle (exact time TBD, assumption 20 ms). All actions in the receiving IOCs shall be arranged so that the controlled subsystem is ready for the next cycle in time.
- Distributing timestamps that can be attached to each EPICS process variable. The timestamps are synchronous over the entire facility.
- Distributing RF-synchronous clock signals with a programmable frequency. There are two options for this: a few (4-5) clock signals will be distributed globally so

that all receivers receive the same signal, or creating a local clock for an individual event receiver.

7.3. ICS Network and Server Infrastructure specifications

The ICS Network will provide OSI L2 switches with 10/100/1000 Mbps copper compatible ports. The switch's ports will use the Medium-Dependant Interface Crossover feature (Auto-MDIX), which permits either straight through, or crossover cables to connect from the device to the switch. Patch cords should be category 5e (Enhanced Category 5) or 6A shielded foiled twisted pair (S/FTP) and conform to fire certification of low smoke with zero halogen (LSZH) as in Table 2.

Category	Standard	Connector	Min – max length metres	Shielding Against RF	Fire certification
5e	TIA/EIA 568C ISO/IEC 11801	8P8C/RJ45	0.5 - 5	S/FTP	LSZH
6A	TIA/EIA 568C ISO/IEC 11801	8P8C/RJ45	0.5 - 5	S/FTP	LSZH

Table 2 Copper communication cable requirements

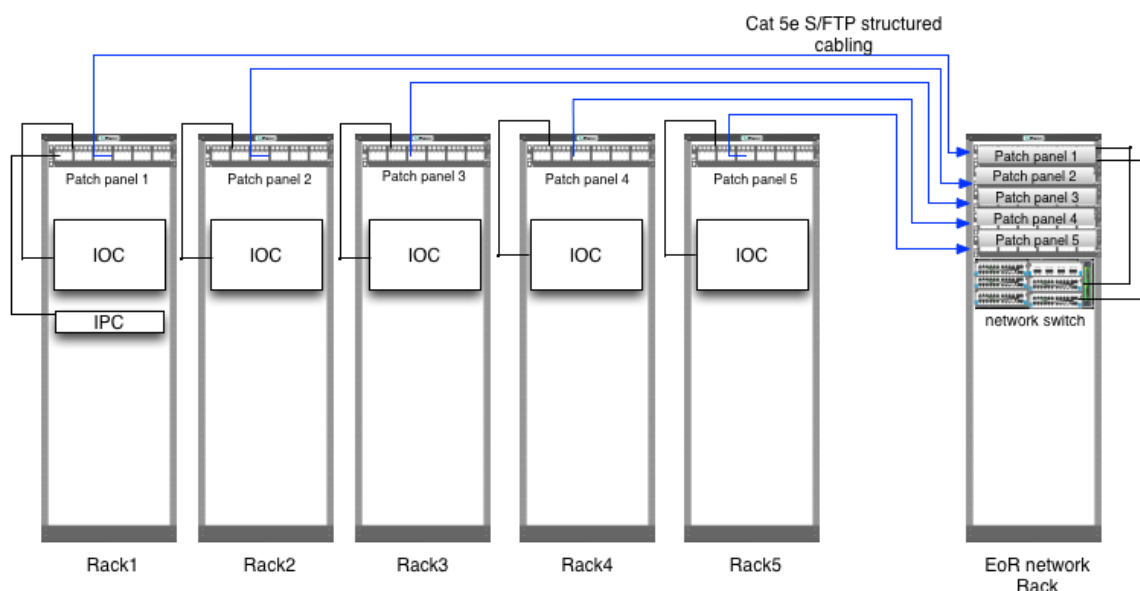


Figure 16. End device patch panel physical network topology

ICS will manage the following networks:

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

1. PV access network

The expected network protocols include:

- PV access -
- TFTP
- DHCP
- DNS
- NFS
- NTP
- Kerberos and LDAPS (639)

2. PV Gateway network

The expected network protocols include:

- PV access
- SSH

3. Control Room network

- PV access
- Printer

4. Diagnostics network

- a. Per machine facility dedicated VLAN for S7 Siemens PLCs
- b. Access to management interface for serial devices (e.g. MOXA).

Patch cable colours for the technical network and other networks are listed in [38].

The PV access network, the equivalent of the legacy channel access (ca) network in EPICS version 3, will be a flat network and all inter-VLAN communication will occur across the PV gateway (pv2pv). The ICS network subnet addresses are available in [39].

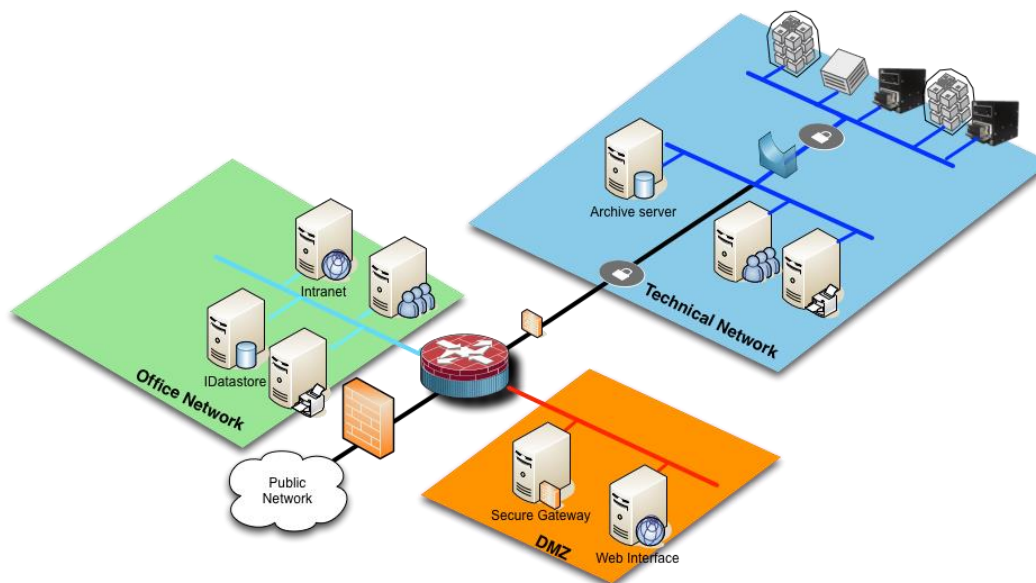


Figure 17 Conceptual drawing ESS Network

8. INTERFACE SPECIFICATIONS

8.1. Introduction

All the field devices that provide physical (analogue or status) signals shall be connected to ICS devices so that the signals can be accessed by/through the control system. A short description of the interfaces is provided in this chapter.

8.2. Functional Interfaces

All I/O that is relevant to operation of the ESS has to have an EPICS record associated to it. The EPICS channels can include raw I/O channels or derived channels that provide a higher level of abstraction.

The control system shall implement the following functions for the EPICS channels in the system:

- Process monitoring and data processing
- Process control, operating logic and sequencing when appropriate
- Alarms
- Error and trace logging
- Archiving

When the I/O comes from an underlying system with its own processing functions, the division of functionality needs to be decided case by case. In general, however, any critical protection functions shall reside in the low level controller and not in EPICS.

8.3. Physical Interfaces

8.3.1. Connecting I/O signals to ICS equipment

The three-layered hardware standard for ESS provides different ways of connecting signals to the ICS equipment. The different standards are shortly described here. For details please consult the referred documents or Wiki pages.

8.3.2. Standards for signal interfaces

PLCs (Siemens)

Signals to be connected to the PLC equipment shall follow those standards that the ESS standard equipment list provides. If the standard equipment list needs adjustment it shall be discussed with the people in ICS who maintain the standard.

The standard list can be found here:

<https://ess-ics.atlassian.net/wiki/display/HAR/PLC> .

EtherCAT modules

Signals to be connected to EtherCAT equipment shall follow those standards that the ESS standard equipment list provides. If the standard equipment list needs adjustment, it shall be discussed with the people in ICS who maintain the standard.

The currently supported modules are listed here:

<https://ess-ics.atlassian.net/wiki/display/HAR/EtherCAT+-+ESS+support>

MTCA.4 supported I/O

ICS supports a standard Digital Controller Board on MTCA.4, in two variants as described below. This board provides the following:

- A powerful FPGA for I/O interfacing and online processing
- An on-board CPU for general processing and running EPICS
- I/O extensions in two variants
 1. Two FMC (VITA-57) HPC slots and digital connections to a rear transition module (RTM). This card model number is IFC_1410.
 2. On-board AD converters, 10 channels through analogue signal connections to a rear transition module and one HPC FMC slot. This card model is IFC_1420.
- A comprehensive firmware library for developing FPGA applications
- Software support including EPICS and associated drivers.

Contact ICS for more detail about the standard platforms. At the time of writing the card is in development. Full documentation will be distributed to users on request as soon as it is available.

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

In most cases, the requirements for I/O processing in the MTCA.4 platform shall be specified by the end user and the final decision made in agreement with ICS. However, ICS will support at least acquisition of the following signal categories:

- Analog input in the range of 10 to 250 MSPS with a 16-bit AD converter
- Analog input up to 5 MSPS, 16-bit ADC, wide voltage range up to +- 10 V.
- Analog input up to 900 (or 1000) MSPS with a 12-bit AD converter
- Analog output up to 500 MSPS with a 16-bit DA converter
- Fiberoptic communication through a SPF+ interface.

In all of these cases, ICS shall be contacted before starting implementation of a specific system.

8.3.3. I/O through fieldbuses

The recommended interfaces are Ethernet or RS-242/485 serial ports. Other fieldbuses are in general not allowed. If there are pressing reasons to use devices with another fieldbus standard, it is required to contact ICS before deciding to buy or use such devices.

Ethernet

Devices with an Ethernet (but not EtherCAT) connection shall primarily be supported through the EPICS StreamDevice driver as far as the data volumes allow. For large-volume devices (cameras or similar detectors) Area Detector software is the primary option. Any other requirements shall be discussed with ICS before starting any development.

Serial connections

Devices with a serial port interface will be connected to a serial-to-Ethernet converter. The standard device supported by ICS, unless otherwise announced, is a MOXA serial server. Please contact ICS for details.

Other types of I/O

For any other type of I/O, ICS shall be contacted before use. Otherwise integration to the control system cannot be guaranteed.

8.3.4. Timing trigger standards

Trigger signals from the timing system can be provided in a few standards:

- LVTTTL is the most common output type. 0 to 3.3V, terminated to 50 Ohm.
- CML, short for Current Mode Logic is available for high frequency clock signals.
- Other output types can be supported through Universal I/O modules that are available for a number of output types (Optical, PECL, LVPECL, etc). Contact ICS for details.

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

8.3.5. Beam interlock system I/O

Each system that is relevant to Machine Protection needs to have a connection to the Beam Interlock system. The standards for this are specified in chapter 9.5.

8.4. Division of responsibilities related to interfaces

As already defined in 2.2, the responsibilities between divisions related to definition, implementation and installation are defined in separate documents, one between each division and ICS ([3],[4],[5] and [6]).

8.5. Standards related to electrical equipment

ICS standards that are related to electrical equipment, in particular supply of electrical power to ICS equipment, are described in the document “ICS Standard for Electrical Equipment”, ESS-0056053.

9. MACHINE PROTECTION SPECIFICATION

9.1. Introduction

9.1.1. The Role of Machine Protection at the ESS

The concept for Machine Protection is described in CHES Document ESS-0035197.

ESS, being a user facility for neutron science is facing high neutron beam availability requirements [ESS-0008886] and is largely relying on custom made, specialized, and expensive equipment for its operation. Damage to this equipment could cause long shutdown periods, induce high financial losses and, as a main point, interfere with international scientific research programs relying on ESS operation and related beam production. Implementing a fit-for-purpose machine protection concept is one of the key challenges in order to mitigate these risks.

9.1.2. Achieving High Operational Availability of the ESS

Availability of the ESS facility can be used to characterize the average neutron production during a certain time period. It represents the average proportion of the planned production time when the ESS research infrastructure is found operational. The availability characteristics of a system can be determined by its reliability, availability, maintainability and inspect-ability. The ESS equipment relevant for neutron beam production is defined as the *equipment under control* (EUC), commonly called “the machine”. The expected operational time between two consecutive corrective or preventive maintenance actions for EUC systems is defined here as *mean time between maintenance* (MTBM). The time for fault diagnostics, corrective and preventive maintenance, logistics, cool down and restart times is defined here as *mean down time* (MDT).

9.1.3. The Machine Protection Equipment under control (EUC)

In the context of ESS Machine Protection, the term “machine” encompasses all elements in the Accelerator, Target Station and Neutron Science system segments; all being necessary for neutron beam production and its further use by the neutron science experiments. **Figure 18** shows a simplified architectural view of the equipment under control (EUC) and the beam states.

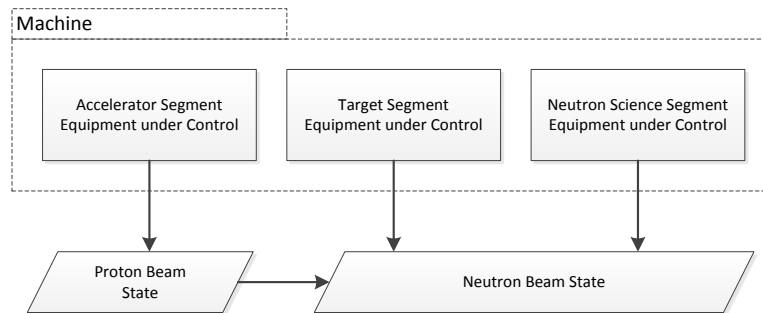


Figure 18: Simplified representation of the “machine”. Equipment under control from the accelerator segment controls the proton beam state. The neutron beam state is controlled by the Target and Neutron Science Segment EUC and is influenced by the proton beam state.

The EUC is exposed to potential damage sources relating to proton and neutron beam properties, radiation, electrical power, vacuum, cooling, RF, etc. The severity of damage needs to be considered in regard to neutron beam quality losses, quality loss duration and resource costs for the recovery of operational capabilities.

9.1.4. Machine Protection Goals

More specifically, the goals for machine protection (MP-G) are:

- MP-G-1 Machine protection shall, in that order, prevent and mitigate damage to the machine, be it beam-induced or from any other source, in any operating condition and lifecycle phase, in accordance with beam and facility related availability requirements.
- MP-G-2 Machine protection shall protect the machine from unnecessary beam-induced activation having a potential to cause long-term damage to the machine or increase maintenance times, in accordance with beam and facility related availability requirements.

9.1.5. Relation of ESS Machine Protection to ESS Safety

Machine protection is concerned with operational goals of the ESS, that means, enabling neutron science and investment protection. It is not concerned with safety aspects of the ESS that are regulated by legal authorities, such as personnel safety or public safety.

9.1.6. Means to achieve Machine Protection

The high operational availability goals shall be achieved by means including:

- Designing the equipment under control (EUC) with high inherent reliability and overall low damage potential,
- Minimization of the mean down time (MDT) of EUC by introducing dedicated technical systems preventing and mitigating damage,
- Minimization of the MDT of EUC systems by introducing dedicated operational and preventive maintenance procedures reducing the probability for (unscheduled) corrective maintenance.

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

- Supporting systems dedicated to reducing MDT. These include analysis, management and recovery tools addressing operational activities related to machine protection (e.g. for post-mortem analysis).

The right strategy to achieve the availability goals will involve a mix of those measures. In the remainder of this document, the ESS concept for achieving the operational availability goals using the aforementioned measures will be presented.

9.1.7. Machine Protection and EUC design

One vital part of Machine Protection can be achieved by designing EUC systems with inherently high availability, thereby reducing the probability of events increasing the MDT (MP-G-1). Also, potential risks of damage can be avoided by means of EUC design, for example, by EUC system shielding and positioning. Machine Protection by means of EUC design is addressed by the design groups in the ESS divisions (e.g. Accelerator groups).

9.1.8. Machine Protection and dedicated technical protection systems

A number of technical systems have to be dedicated to machine protection in order to prevent and mitigate production losses and equipment damage.

Beam related protection concerns are addressed by input systems (BLMs etc.), which are connected to the beam interlock system (BIS). The BIS can stop the beam by triggering actuators (proton source, LEBT chopper, etc.).

“Local Protection Systems” address concerns related to protection of the systems themselves. For example a local protection system shall protect RF systems from internal (non beam-related) damage.

Dedicated EUC protection systems can be implemented by different technologies, including

- hardwired interlocks
- risk mitigation by software actions.

Scopes and boundaries of the different EUC systems and their protection systems are defined in Machine Protection scope documents.

9.1.9. Machine Protection and operational and preventive maintenance procedures

For effective and efficient execution of Machine Protection related tasks, procedures that guide human interactions with the EUC need to be defined. Machine Protection related procedures include

- operational procedures regarding operation of the EUC,
- preventive maintenance procedures for the EUC.

9.1.10. Machine Protection support systems

Machine Protection support systems enhance the effectiveness and efficiency by which ESS staff can execute Machine Protection related tasks. Machine Protection support

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

systems can relate to post-mortem analysis, early fault detection, alarm analysis, root cause analysis, documentation of Machine Protection related events and their statistical evaluation.

9.1.11. The Machine Protection mandate at the ESS

ESS Machine Protection addresses stakeholder concerns and functions that cut across different ESS divisions and systems. Hence, a cross-divisional organizational unit is established for the overall coordination and decision-making on machine protection concerns, the ESS Machine Protection Committee.

9.1.12. Tasks of the ESS Machine Protection Committee (MPC)

The MPC shall coordinate Machine Protection related activities with the relevant ESS divisions, working groups, in-kind contributors and experts of the ESS equipment and operation teams. This includes to

- coordinate the identification, assessment and documentation of relevant risks, hazards, failure scenarios of the EUC,
- coordinate the coherent development (including design, integration, commissioning) of the EUC and its future changes or upgrades in regard to Machine Protection,
- coordinate the operation of the ESS concerning machine protection in line with the ESS goals,
- identify possible bottlenecks that would prevent neutron beam production according to ESS goals.

The MPC shall approve overall Machine Protection decisions. This includes to

- approve overall machine protection requirements and machine protection functions,
- approve the overall technical decisions,
- approve the delegation of tasks (system development, commissioning, operation, etc.) to the divisions,
- define boundary conditions for operation (proton beam power, repetition rate, etc.) and authorities/ procedures for short-term interventions (e.g. overnight relaxation of operational boundaries),
- approve the overall development approaches for EUC protection systems.

The MPC meetings are primarily intended to formally approve issues that have been prepared and discussed according to a pre-defined workflow.

9.1.13. Composition of the MPC

The MPC is composed of representatives of all ESS divisions who are stakeholders in Machine Protection. The representative shall have decision-making authority for their division. It includes representatives of Accelerator division, Target division, ICS division,

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

NSS division and Operations division. The MPC is chaired by the ESS Machine Protection champion (currently Annika Nordt).

9.1.14. Relation of the MPC to other ESS decision making bodies

The MPC receives its mandate from, and reports back to EPG.

9.1.15. Related Machine Protection venues

The meeting venue “Machine Protection Panel” is a discussion forum for gathering Machine Protection relevant information and one way of communicating Machine Protection issues.

9.2. ESS Machine Protection Systems Engineering Management Plan

The SEMP (Systems Engineering Management Plan) for Machine is being described in ESS-0057245. The approach that is being followed is the System of Systems approach (MP-SoS).

9.3. Machine Protection Systems Requirements Architectural Framework

The MP systems requirements and the architectural framework are described in ESS-0057251. For any questions please contact Annika Nordt (annika.nordt@esss.se).

9.3.1. Machine Protection Capability Objectives

The capability objectives for machine protection have been stated in the Machine Protection Concept (ESS-0035197). Because of the high risk potential, Machine Protection shall be implemented in accordance with functional safety standards to achieve an appropriate Protection Integrity Level.

9.3.2. Machine Protection General Requirements

The following set of general requirements is deduced from the capability objectives. Explanations and rationales for and consequences from the requirements are inserted where deemed necessary. The term “Machine protection” includes all machine-protection related systems, including all related procedures that are necessary to keep the machine in a protected state.

MP-GR-1 Machine protection shall detect all off-nominal states that can lead to relevant damage to the machine.

Damage can be caused by many different sources of hazard, the proton beam not being the only one. This requirement implies that (a) machine protection detects off-nominal beam states that might lead to damage but also, that (b) machine protection detects all other off-nominal states that can occur locally within a specific EUC and that could potentially lead to damage, i.e. overheating, overcurrent, etc. However, it shall be noted that the responsibility of implementation does not necessarily lie in ICS but has to be defined case by case. In general, implementation of local protection is under

responsibility of the relevant design group but the implementation has to conform with the overall machine protection requirements.

- MP-GR-2 Machine protection shall take all the necessary actions needed to, in that order, prevent and mitigate damage in case of detection of a relevant off-nominal state, including switching-off of the proton beam.

This requirement implies that the actions of machine protection shall not be limited to the switch-off of the proton beam. Machine protection shall take appropriate action if local off-nominal states, i.e. overheating or loss of cooling are detected. Machine protection must also consider whether the local actions have an impact on the proton beam parameters in a way to lead to a hazardous beam. If that is the case, the beam shall be switched off in addition to the local action. Damage that could be caused by switching on the beam while some EUC is in an off-nominal state shall be anticipated and switching the beam on must be prevented in such a case. Switching the beam on knowing that damage could occur and relying on beam monitoring to detect this and then react is a mitigating and not a preventive action: beam would be in the machine (accelerator and target), and beam would need to be stopped to mitigate the potential damage. Prevention shall happen before mitigation.

- MP-GR-3 Machine protection shall detect all off-nominal states that can lead to relevant unwanted beam-induced activation.

- MP-GR-4 Machine protection shall take all the necessary actions needed to, in that order, prevent and mitigate unwanted beam-induced activation in case of detection of a relevant off-nominal state, including switching-off of the proton beam.

While it might at first seem clear that unwanted activation can be prevented and mitigated by switching off the proton beam, this might not be the only action that can be taken. The formulation of this general requirement aims at not excluding additional actions a-priori.

- MP-GR-5 Machine protection functions shall be implemented with timing constraints and protection integrity levels in accordance with damage risk reduction requirements.

This requirement implies that the beam and facility related availability requirements get translated into damage risk reduction requirements. This will need to be done during the allocation of the protection integrity requirements.

- MP-GR-6 Machine protection functions shall be implemented such that the probability of spurious trips is reduced in accordance with availability and damage risk reduction requirements.

Spurious trips, i.e. an erroneous action of machine protection, will negatively impact the facility availability (i.e. there was no damage risk, but still the machine operation was stopped). This requirement implies that the probability of spurious trips gets properly taken into account in the design of the MP-SoS constituent systems.

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

MP-GR-7 Machine protection shall transmit all necessary information to the responsible staff allowing them to take adequate actions to resume facility operation within a minimum amount of time.

The availability of the facility and the beam will largely depend on the Mean-Time-To-Restoration (MTTR) after any protective, mitigative or corrective actions have been taken. An efficient restoration can only take place if the necessary information to diagnose the problem is available to the responsible people.

MP-GR-8 Machine protection shall record all information about detected off-nominal states and performed prevention and mitigation actions to allow for a-posteriori event reconstruction and analysis.

A continuous optimization of the performance of machine protection with respect to facility and beam availability will be required. Such an optimization can only be based on a detailed analysis of the systems behaviour. The analysis can only be done if all relevant data gets recorded and if rich diagnostics are implemented allowing the fast detection of what went wrong. This requirement implies that all machine protection related systems collect machine protection related data and make this data available for recording and further analysis.

MP-GR-9 Machine protection shall support operation during all foreseen lifecycle phases of the machine, including, but not limited to assembly and installation, commissioning, tuning, operation, faultfinding, maintenance, and dismantling.

The stakeholders will probably expect a specific behaviour from machine protection for each of the lifecycle phases of the facility. “Supporting” operation has the meaning of “not hampering” the operation while still reaching the required protection integrity levels. Safety or protection systems that are perceived as an obstacle will be bypassed, which will result in an uncontrolled risk situation. A thorough analysis of the concepts of operation for the facility in all lifecycle phases is mandatory for the proper refinement of this requirement.

MP-GR-10 Machine protection shall support all foreseen operating modes of the machine, including but not limited to proton-beam up to intermediary targets, proton-beam with reduced beam power or alternative beam envelopes, and proton-beam with alternative duty cycles.

This requirement is closely related to MP-GR-9. Stakeholders should not be lead to improvise to reach their goals but machine protection should readily support them in any operation mode.

MP-GR-11 Machine protection shall support operation in case of degraded mode of operation of equipment under control, if required for reaching the availability goals and if compatible with damage risk reduction requirements.

Equipment under control will fail, and, depending on the equipment and the failure, the facility might be operated while repair is still on-going to achieve availability goals. Machine protection will have to support such scenarios to avoid the stakeholders from

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

improvising solutions and potentially leading into uncontrolled high-risk situations. Machine protection should, in such a case, still provide the required protection integrity levels¹.

MP-GR-12 Machine protection shall support operation in case of degraded protection functions, if required for reaching the availability goals if and compatible with damage risk reduction requirements.

This requirement is related to MP-GR-11 but has a different goal. Failure of a protection function will in general have no impact at all on the EUC functionality and beam can be produced as during normal operation. However, due to completely or partially missing protection functions, the required protection integrity level is not achieved anymore and the facility is operated with a higher risk for damage. Machine protection should support facility operation at a lower protection integrity level than specified under normal conditions if required by ESS management. Stakeholders should not be forced to improvise for solutions and potentially lead into completely uncontrolled risk situations.

9.3.3. Machine Protection System-of-Systems Architectural Framework

Machine Protection has been recognized to be an acknowledged System-of-Systems. The architectural structure of the MP-SoS has already been anticipated in ESS-0057245. It is composed of five classes of constituent systems (Figure 19). These five classes are:

- Local MP-related systems located in the accelerator, the target station and the neutron science segment of the ESS facility;
- MP-related proton beam monitoring systems;
- Beam Interlock System (BIS);
- MP-related beam switch-off actuation systems;
- MP management systems.

The following basic description of the constituent systems classes and their interaction define the architectural framework of the MP-SoS constituent systems. This description is meant to serve as a framework for the engineering of the MP-SoS constituent systems and the refinement of the requirements applicable to those systems. This framework does not try to anticipate detailed design features of the constituent systems.

9.3.4. Local MP-related Systems

The local MP-related systems located in the accelerator, target station and neutron science segments of ESS implement the needed local protection functions to

- keep the local EUC they are responsible for, protected from non-beam-induced damage;

¹ The required protection integrity levels might be lowered in such cases by management decision. This has to be anticipated.

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

- prevent beam from being switched on/injected to the linac or sent to the target if the local EUC is not ready to support beam operation².

If a local damage risk gets detected, these local protection functions will result in a locally protected state for the affected EUC³. If such an action has a potential to negatively influence the state of the proton beam, the local protection functions additionally trigger a switch-off of the proton beam⁴. If the local EUC is not ready to support beam production, the local protection functions will not permit beam. If other EUC depends on the operation of the affected EUC, then necessary actions will need to be taken to prevent damage to that other EUC⁵.

For this purpose, MP-related systems will implement a LOCAL-PERMIT and a BEAM-PERMIT state. The LOCAL-PERMIT is a state variable that is internal to the MP-related system and represents whether it is correctly functioning or an off-nominal state has been detected. The BEAM-PERMIT state is communicated to the Beam Interlock System and tells whether the MP-related system is in a state where beam production is safe.

² This includes the detection of local off-nominal states that might negatively impact, with respect to its hazard potential, the proton beam state.

³ An example might be the detection of an abnormally high temperature in a magnet power-supply, resulting in the switch-off of that power-supply.

⁴ Switching-off a magnet power-supply might result in a potentially hazardous beam; hence the same local protection function that switches off the power-supply would also cause a switch-off of the beam.

⁵ An example for such a case could be the following: If the performance of a cooling-water pump degrades and switches off in order not to get damaged, then the power supplies that generate current through magnets depending on that cooling water should be switched-off immediately. Such cases need to be uncovered during the required RAMS analysis ([40],[41]).

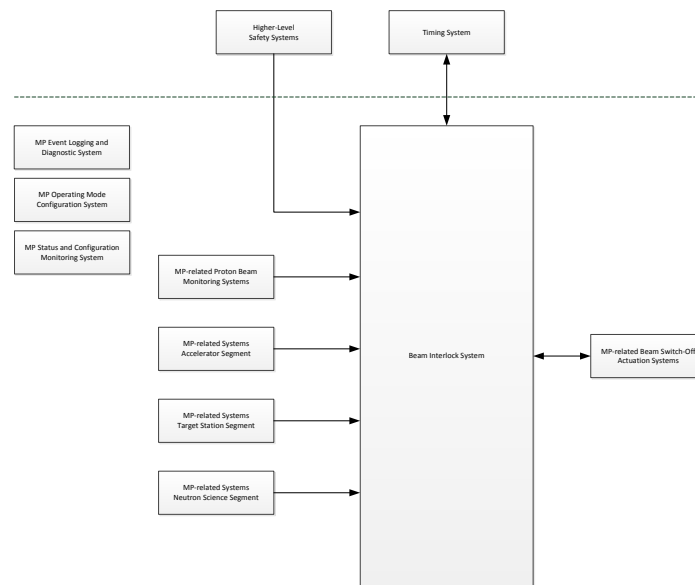


Figure 19: Architectural Framework for the Machine Protection SoS. Machine Protection is composed of: MP-related systems located in the accelerator, target station and neutron science segments from ESS; MP-related proton beam monitoring systems; the beam interlock system; MP-related beam switch-off actuation systems and MP management systems.

Figure 20 shows the same architectural framework as Figure 19 with a detailed representation of the currently identified constituent systems in the ESS accelerator segment, the identified higher-level safety systems and the potential MP-related Switch-Off Actuation Systems.

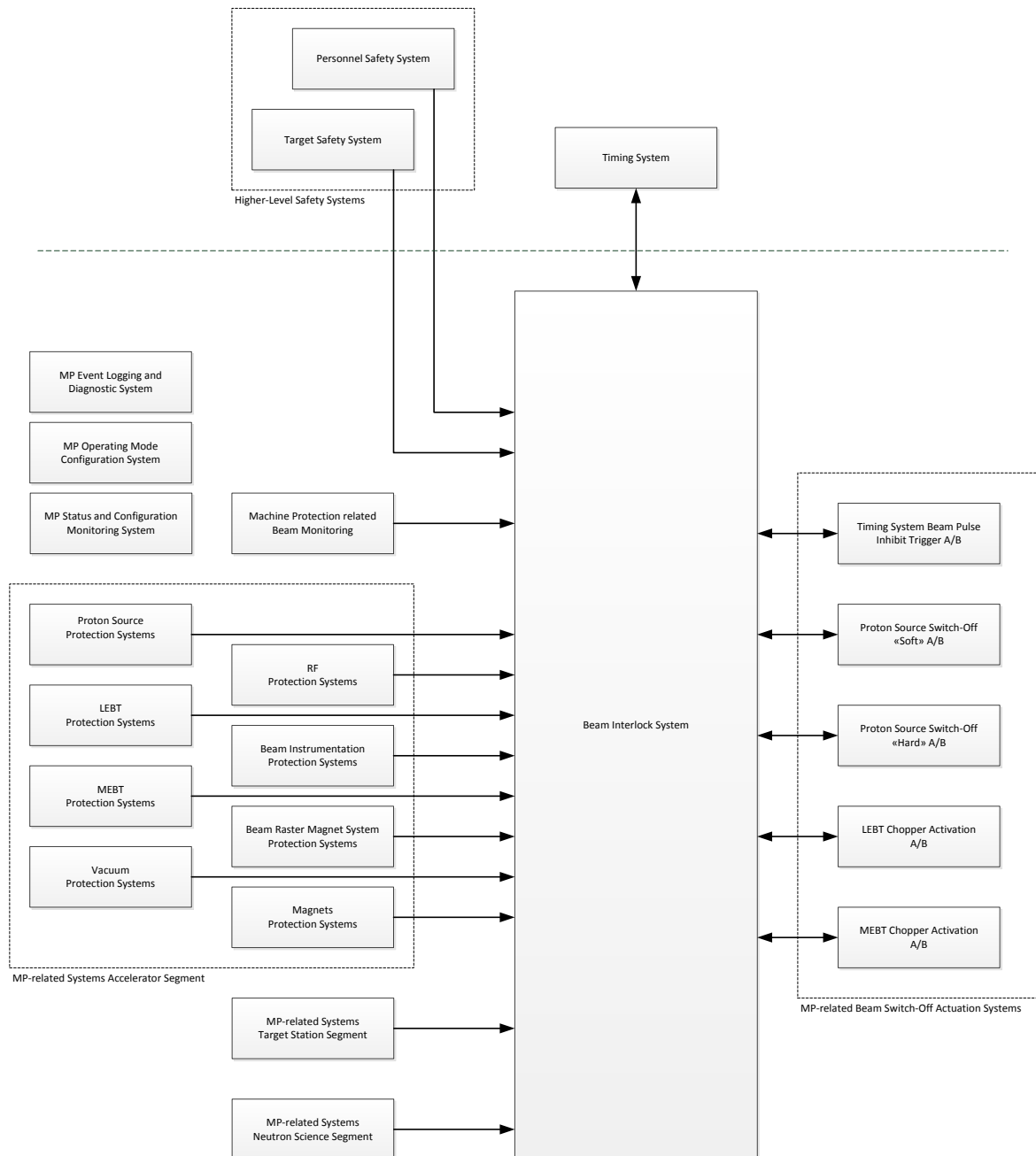


Figure 20: Architectural Framework of the Machine Protection SoS. This representation is similar to **Figure 19**; it details the currently identified MP-related Systems from the Accelerator segment, the MP-related Beam Switch-Off Actuation Systems and the Higher-Level Safety Systems.

9.3.5. MP-related Proton-Beam Monitoring Systems

The MP-related proton-beam monitoring systems detect any off-nominal states of the proton beam itself that might cause damage to or unnecessary activation of any equipment. The corresponding protection functions will trigger a switch-off of the proton beam by means of a BEAM-PERMIT signal transmitted to the Beam Interlock System.

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

9.3.6. MP-related Proton Beam Monitoring versus Beam Instrumentation Protection Systems

The requirement to detect off-nominal states of the beam parameters has been allocated to the MP-related Proton-Beam Monitoring Systems.

The requirement to detect off-nominal states of the beam monitoring systems themselves, i.e. states that might lead to damage to the beam instrumentation itself, and to detect states where the monitoring systems are not ready for beam, is allocated to the Beam Instrumentation Protection Systems.

The physical implementation of the beam instrumentation might well implement MP-related Proton-Beam Monitoring functions and Beam Instrumentation Protection functions in the same physical system. Care must be taken to do a proper requirements allocation during the architectural design phase of those systems and to define adequate verification and validation procedures to cover both goals.

9.3.7. Beam Interlock System

The Beam Interlock System evaluates the BEAM-PERMIT signals from all local MP-related systems and MP-related proton-beam monitoring systems. If required, the Beam Interlock System initiates the switch-off of the beam by triggering a set of MP-related beam switch-off actuation systems in a specific sequence⁶. This set and sequence need to be chosen to reach compliance with the protection integrity level requirements and to allow for a painless⁷ recovery to normal operation.

The BIS will verify the correct reaction of the actuation systems and, in case beam is not switched-off, an emergency sequence disregarding any recovery requirements will be triggered.

After an interlock, beam production will only be allowed to resume once all BEAM-PERMIT input signals are in the expected state and all affected MP-related systems as well as the Beam Interlock System have been actively reset.

Since the Beam Interlock System is purely dedicated to machine protection, requirements applicable to the BIS will be defined in a dedicated BIS Requirements Specification document.

9.3.8. MP-related Beam Switch-Off Actuation Systems

The MP-related beam switch-off actuation systems implement functions to “switch the proton beam off”, i.e. stop the further generation of proton beam and deflect the

⁶ That’s the event we use to call “interlock”.

⁷ We anticipate for example that switching off the HV supply to the proton source in a brute-force manner might cause damage to the source or that it might be hard to recover after such a switch-off.

protons that are already in the accelerator to an absorber in a controlled way to minimize damage and activation potential.

The different ways considered to achieve a proton beam “switch-off” are listed in Table 3. Which combination of those methods will be used in the final design will be decided during the detailed design phases of the constituent systems. Whatever combination is chosen, it will have to comply with the protection integrity level requirements.

The classical way applied in safety systems engineering, that is allocating the protection integrity level requirements onto the subsystems and defining the requirements of the subsystems such that compliance is achieved, is in our opinion not fully applicable within the system-of-systems approach. The timing system, the proton source control electronics as well as LEBT and MEBT chopper power supplies or associated beam dumps do partially already exist or have been designed with a focus not on machine protection, but on their functional scope.

We do not believe that a proper selection of switch-off actuation system selection can be defined or enforced through brute-force requirements specification. We rather believe that the actual designs of those systems need to be analysed with respect to their protection level capabilities and that the right combination of “switch-off” methods, with potentially necessary corrective actions, will lead to compliance with protection integrity goals and functional goals⁸.

Timing System Beam Pulse inhibit Trigger	Proton pulse generation is controlled by the Timing System. Preventing the timing system from generating the events leading to a proton beam pulse would prevent proton beam from being injected and accelerated.
Proton Source Switch-Off “Soft”	Prevent the proton source from injecting protons into the Linac by using an inhibit feature of the proton source control electronics.
Proton Source Switch-Off “Hard”	Switch off the HV power to the proton supply using redundant contactors to prevent protons from being injected into the Linac.
LEBT Chopper Activation	Activate the LEBT Chopper to deflect the beam onto the LEBT dump.
MEBT Chopper Activation	Activate the MEBT Chopper to deflect the beam onto the LEBT dump.

Table 3: Ways to achieve a proton beam “switch-off”. The final decision which combination is going to be used will be taken during the detailed design phases of the constituent systems.

9.3.9. MP Management Systems

Since the MP Management Systems are purely dedicated to machine protection, requirements applicable to those systems will be defined in dedicated Requirements Specification documents.

⁸ Protection integrity goals and functional goals do indeed converge: both strive at optimizing the facility availability.

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

9.3.10. MP Event Logging and Diagnostics System

This system collects logged data from all MP-SoS constituent systems and provides means to perform automated or manual event analysis for diagnostic purposes. As the ESS operating procedures might require an operator to acknowledge the event analysis result before beam injection is allowed to proceed, the performance of this system might have a large impact on beam availability.

9.3.11. MP Operating Mode Configuration System

This system sets and reads configuration data to and from all MP-SoS constituent systems.

9.3.12. MP Status and Configuration Monitoring System

This system performs online monitoring of the status and configuration of all MP-related systems. Configuration data include: the current operating mode, hard-, firm- and software identifiers. This system can request to switch the beam off in case it detects a problem.

9.3.13. Higher Level Safety Systems

Identified higher-level safety systems are the Target Safety System (TSS) ⁹ and the Personnel Safety System (PSS) [10]. Both of those systems are required to implement safety functions with the needed safety integrity level independently of the MP-SoS. Triggering a beam interlock for machine protection purposes when the TSS or the PSS see a problem is consistent with the goals and concepts of Machine Protection: TSS and PSS need to be in a state allowing beam. If they are not, damage could be caused to the machine and beam operation needs to be stopped. Of course, if TSS and PSS are not in a state to allow beam, those systems should handle this on their own. But they will do it for safety purposes and will most possibly neglect machine protection. A combination of reactions, both from TSS or PSS and the MP-SoS, will make sure that both goals, safety and machine protection, are covered. Functionality of the MP-SoS will not be credited in any way for a contribution to safety.

9.3.14. Timing System

The pulsed operation of the accelerator relies heavily on the Timing System [5.2.3,7.2]. The timing system will not only broadcast timing events to its client systems, but it will also be used to broadcast operation mode information. In the present architectural framework, we have introduced a dedicated MP Operating Mode Configuration System (see section 9.3.11) for the purpose of configuring the MP-related system. The relation between those two systems will need to be clarified during the detailed design phases of the constituent systems. Any solution must be compliant with the protection integrity level requirements.

⁹ A description of the TSS is not within the scope of this document.

9.3.15. Interfaces between the Constituent Systems

Table 4 describes the interfaces between the MP-SoS constituent systems. Detailed specifications of these interfaces will need to be developed as the engineering of the MP-SoS constituent systems progresses. They will be described in dedicated Interface Control Documents.

Source	Target	Identifier	Description/Purpose
MP-related Beam Monitoring	Beam Interlock System	BEAM-PERMIT	The BEAM-PERMIT signal is used by the source systems to trigger a proton beam “switch-off” in case off-nominal states are detected. They emit this signal to the Beam Interlock System.
MP-related Systems Accelerator Segment			
MP-related Systems Target Station Segment			
MP-related Systems Neutron Science Segment			
Higher-Level Safety Systems			
Beam Interlock System	MP-related Beam Switch-Off Actuation Systems	BEAM-PERMIT	The Beam Interlock System produces this BEAM-PERMIT output signal based on all BEAM-PERMIT input signals it receives from its sources. The logic implemented in the Beam Interlock System and producing this BEAM-PERMIT output should ensure that MP-related Beam Switch-Off Actuation Systems are actuated when needed.
MP-related Beam Switch-Off Actuation Systems	Beam Interlock System	Status	The MP-related Beam Switch-Off Actuation Systems communicate their status to the Beam Interlock System. The status information indicates whether they are ready to operate and indicate their actual setting (beam “on” or “off”).
Timing System	Beam Interlock System	Time Reference Trigger Events Operating Modes	Timing information, beam pulse trigger events and operating modes are transmitted from the Timing System to the Beam Interlock System.

Table 4: Interfaces between MP-SoS constituent systems.

9.4. Software Specifications

The design of the software implemented on the slow local protection systems for magnets, interceptive devices, vacuum gate valves and target has to be done following a formal approach involving the design of finite states machines and the extraction of logic state and output equations.

Software engineering practices for real-time safety critical applications have to be followed. In this way, the probability of software errors is reduced and the dependability increased. Besides, in order to achieve the intended availability figures, use cases have to be defined in order to obtain the behavioural rules of each local machine protection system.

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

For the above purposes we plan to use extensively proven safety and standard software development packages provided by the PLC manufacturer and to perform our tests evaluating the most critical paths inside the programmed state machines.

9.5. Hardware Specifications

All our slow machine protection systems will be based on PLC (Programmable Logic Controllers) technology. This technology has been proven in similar facilities and in the industrial world to be very robust and reliable. It allows building highly distributed control architectures by using fieldbus technologies like PROFINET or PROFIBUS.

We plan to locate the CPUs of our local machine protection systems in the front-end building, and all the remote periphery units in the Klystron gallery. All the remote periphery units will be connected with the CPUs using a fieldbus technology optical (to avoid EMI) and copper based. We use one CPU per slow local machine protection system and several remote periphery stations distributed in the enclosures of the klystron gallery. This means four CPUs and several remote periphery units.

Approximately 350 resistive magnets and 350 power converters (PC) will be installed in the 600 m long linear accelerator (LINAC) at the European Spallation Source, ESS, transporting the proton beam from the source to the target station. In order to protect this equipment from damage (e.g. due to overheating) and to take the appropriate actions required to minimise recovery time, a dedicated magnet powering interlock system will be installed. The magnet powering interlock system will safely switch off a PC upon the detection of an internal magnet or PC failure and inform the beam interlock system to inhibit further beam operation. Failures of the magnet cooling system can be detected by interlocking the opening of a thermo-switch or a flow-switch. To achieve the required level of dependability, an interlock system based on safety Programmable Logic Controller (PLC) technology, distributed safety PLC software programming tools, PROFINET fieldbus networking, and current loops for hardwired interlock signal exchanges, will be used.

Approximately 30 interceptive devices will be installed in the 600m LINAC for beam instrumentation, including 7 faraday cups, 2 Allison scanners, 14 Wire scanners, 2 Slit & Grid and 4 LBM devices. In order to protect this equipment and the beam, a set of position switches will be installed at each interceptive device. These position switches will indicate if the device is inside or outside of the beam pipe. Permission for insertion and extraction of the interceptive device is required to move it. This permission will be granted or deny by our protection system depending on the beam destination and beam properties (beam mode). Under some situations a removal of the beam may be needed and therefore a connection to the beam interlock system required to inhibit further beam operation. Additional information like status of each interceptive device is expected by our local protection system. To achieve the required level of dependability, an interlock system based on safety Programmable Logic Controller (PLC) technology, distributed safety PLC software programming tools, PROFINET fieldbus networking, and current loops for hardwired interlock signal exchanges, will be used.

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

Approximately 110 vacuum gate valves will be installed in the 600m LINAC. In order to protect this equipment and the beam, a set of position switches will be installed at each vacuum gate valve. These position switches will indicate if the valve is open or close. In case that there are bad vacuum conditions or beam on whilst vacuum gate valve closed, the beam has to be stopped according to beam destination, and therefore a connection to the beam interlock system required to inhibit further beam operation. To achieve the required level of dependability, an interlock system based on safety Programmable Logic Controller (PLC) technology, distributed safety PLC software programming tools, PROFINET fieldbus networking, and current loops for hardwired interlock signal exchanges, will be used.

The target local machine protection system design is in progress at the time of writing. The initial risk analysis is coming and the proper use cases and identification of hardware interfaces and requirements will follow. As a general rule we plan to use hardwired current loops as basic mechanism for signals exchange, electrical isolation for the exchanged signals between the controller and the system to protect (using relays and opto-couplers), failsafe CPUs and digital I/O modules as well as safety communications protocols in the fieldbus network. The involved sensors and actuators shall be also qualified to the proper protection level or made redundant if needed.

10. PERSONNEL SAFETY SYSTEMS SPECIFICATION

10.1. PSS Introduction

The primary role of the ESS personnel safety systems is to protect workers from ionising radiation from proton and neutron beams and ionising radiation from Radio Frequency (RF) systems (X-Rays). The systems do not protect from residual radiation from activated components. The systems will also protect workers from conventional safety hazards when appropriate. The following hazards will be considered (but not limited to) and assessed and analysed for each system:

- Proton beam induced Ionising radiation in the accelerator
- RF induced ionising radiation from accelerator Radio frequency systems
- Proton beam induced Ionising radiation in the Target utility rooms and the target buildings
- Neutron instrument radiation
- Neutron radiation in the instrument halls
- Oxygen depletion
- High voltage from assorted equipment
- Magnetic Field Hazards.
- Laser Hazards
- Motion/Mechanical Hazards

The ICS division Protection Systems Group is responsible for the design, installation, commissioning and validation of the Personnel Safety Systems (PSS) at ESS. The scope of the PSS covers the following systems:

- The Accelerator PSS 1.
- The overall accelerator PSS.
- The Cryo module test stand PSS.
- The Target PSS.
- The Accelerator ODH safety systems
- The Target ODH system.
- Up to 26 Neutron instrument systems PSS

10.2. PSS Standards and lifecycle

All personnel safety systems will meet the applicable sections of the Swedish Radiation Authority, Strålsäkerhetsmyndigheten (SSM). The requirements are available as CHES document ESS-0018828.

The IEC standard that ESS will use is the functional safety standard IEC 61508:2010. This standard was chosen by ESS early in the project and is used in the design and development of personnel safety systems in many facilities throughout Europe and around the world.

IEC 61508 is an international standard concerned with functional safety achieved by safety related systems that are primarily implemented in

Electrical/Electronic/Programmable Electronic technologies (E/E/PE). The ESS personnel safety systems are examples of this and fall within the scope of IEC 61508:2010. This IEC standard provides an overall safety lifecycle structure for functional safety systems as detailed in Figure 18.

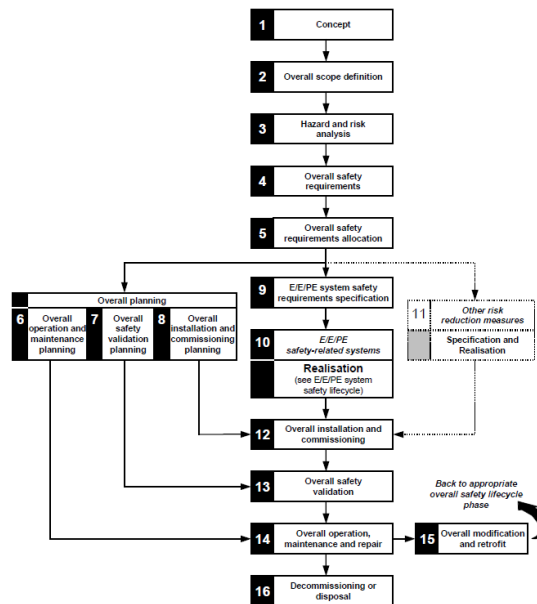


Figure 18: IEC 61508 overall safety life cycle.

This safety lifecycle is divided into three sections:

- Phases 1 – 5 addresses Analysis
- Phases 6 – 13 addresses Realisation
- Phases 14 – 16 addresses Operation

ESS will obtain independent reviews of all documentation of each system at three stages:

- Analysis
- Design
- Validation

These reviews will be carried out regularly and all reports will eventually be passed on to the SSM.

The PSS equipment will be designed using standard equipment that has been proven in use with safety systems throughout the world. Chapter 10.3 details the high level architecture and the standard hardware.

10.3. Personnel Safety System Software Specifications

10.3.1. PSS Software Strategy

To fulfil the requirements for redundancy, separation and diversity, the PSS control system will be realised through the two-train, fail-safe PLC system. Siemens is chosen as a

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

supplier for the implementation of PSS control system. The PSS control system will consist of four main subsystems (Accelerator, ODH, Target and Neutron instruments); and each subsystem will have its own PLC interconnected with other subsystem PLCs within a single train. The main Siemens automation components are shown below:

- The latest generation of the fail-safe Siemens PLCs (S7-1500):
 - Two independent S7-1518 F-PLCs for Accelerator PSS;
 - A single S7-15xx (TBD) F-PLC for ODH monitoring system;
 - Two independent S7-1518 F-PLCs for Target PSS;
 - A single S7-15xx (TBD) F-PLC for each Neutron instrument.
- A standard S7-15xx PLC (TBD) that will be used as a gateway between the subsystem's F-PLC and supervision computer, HMI-s, etc.
- Distributed I/O stations with fail-safe I/O modules – either ET200SP or ET200MP.
 - All the sensors and actuators will be connected locally to the distributed I/O stations that will communicate with PLCs, preferably using the PROFINET protocol.
- ET200SP Open Controller with embedded Windows 7 for connecting to enterprise databases and PSS Access Control System devices.

Siemens fail-safe CPUs (and Siemens SIMATIC Safety F-systems in general) are certified to satisfy the Safety Integrity Level SIL3 in accordance with IEC 61508:2010, which means it is suitable for the SIL required by each SIF it services in PSS system. They allow the processing of standard and safety programs on a single CPU.

The automation software for PSS will be developed using the latest version of Siemens SIMATIC STEP 7 Professional (TIA Portal), together with the Safety Advanced programming package, where the safety checks are automatically performed and additional fail-safe blocks for error detection and error reaction are inserted automatically when the safety program is compiled. This ensures that failures and errors are detected and appropriate actions are triggered to either maintain the safe state or bring the system to a safe state. All HMI-s and supervision screens will be developed using the Siemens WinCC Comfort software.

10.3.2. PSS Cyber Security Plan – Defence-in-Depth

The ESS cyber security countermeasures will be applied in layered manner, and since PSS is treated as a stand-alone system using its own local network, here will be presented just a system layer concerning only the PSS system. This system layer consists of three levels (sub-layers):

- Application level
 - Passwords management
 - Physical protection of critical devices
 - PLC Access Control Lists and Checksum tests
 - System hardening
 - Authentication and use administration

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

- Detection of attacks (antivirus, intrusion detection)
- Integrated access protection in automation
- Recovery procedures
- Database level
 - Database authentication and permissions
 - Data management (logging, storing, retrieving...)
 - Data encryption and encryption keys management
- Update management level
 - Patch management – software and firmware updating
 - Hardware replacement

It is essential to provide access protection in operation mode for the access to the safety part of the software. The access to PSS safety software will be protected by two password prompts: one for the safety program and another for the safety CPU. To prevent the misuse, the system automatically checks the collective signature of the safety program (Checksum test) and in case of the software misuse; the system goes to Alarm mode and PSS system administrator must be informed immediately. The PSS software engineering workstation will be system hardened PC, without Acrobat Reader, Java and Flash and running two up to date anti-virus programs. The possibility of procedural internet/intranet connection, patching procedures, data exchange with databases and software and firmware update strategies still need to be defined. More information about password protection of safety related software, software backup and versioning can be found in Personnel Safety System Configuration Management Plan (ESS-0058389).

10.3.3. PSS Software Architecture

All safety functions are realised through the safety part of PLC program and there are few dedicated global fail-safe data blocks dealing just with data important for safety. The software for ODH monitoring will be developed on separated PLC, as well as the software for Target PSS and each of neutron instruments. All these PLCs will communicate with the main Accelerator PSS PLC providing the needed inputs for interlocking the proton beam, as shown in figure below (Figure 21).

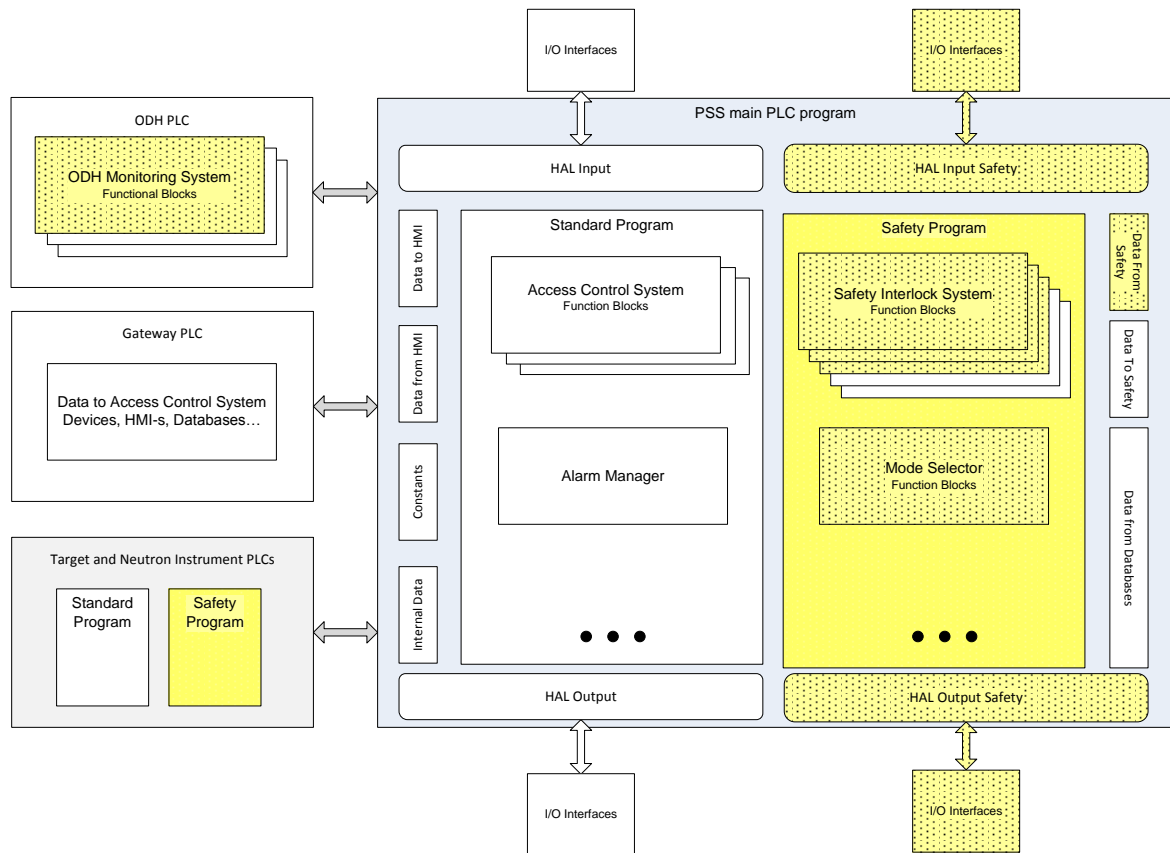


Figure 21: General PSS PLC Software Architecture

Data received on input cards will always be stored first in global Hardware Abstraction Layer (HAL) Input data blocks at the beginning of each program cycle, and prepared to be used in the software. Similarly, at the end of each program cycle, data will be written to physical outputs from the HAL Output data blocks. The purpose of using the HAL data blocks is to avoid using physical input and output addresses directly in the software, which makes programming more practical.

Siemens Safety Advanced programming package comes with the library, which contains several useful instructions for the safety program, and some of them are planned to be used in PSS software, like for example:

- ESTOP1 : Emergency STOP up to stop category 1 - discrepancy monitoring of the two NC contacts;
- EV1oo2DI: 1oo2 evaluation with discrepancy analysis – detecting the discrepancy error;
- SFDOOR: Safety door monitoring – monitoring the status of door position switches;
- FDBACK: Feedback monitoring – comparing the actuator feedback signal with the command sent to actuator.

More information on safety and software requirements can be found in Safety requirement specification document (ESS-0062932).

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

10.3.4. PSS Software Virtual Commissioning

To facilitate software development and system testing, PSS team will use Siemens Simulation Unit (Siemens reference: 9AE4120-2AA00) for virtual commissioning and Factory Acceptance Test on the PSS test stand. Main software functionalities will be tested:

- Control/automation loops
- Switching functions
- Pre-allocation, reading-out and changing digital and analogue I/O-s
- Functionality test for alarms and messages

10.4. Personnel Safety Hardware Specification

10.4.1. PLC modules

As part of IEC 61508 and in order to achieve diversity, redundancy and separation, ESS personnel safety systems will be built using two independent technical systems (called two train system at ESS). PSS will use the latest generation of Siemens failsafe PLCs (S7-1500 series). PSS sensors and actuators will be connected to standard and failsafe Input/output modules, and each group of I/O modules are connected to PSS PLC CPU through interface module ET 200SP using PROFIsafe (PROFINET safety) protocol.

10.4.2. PSS enclosures

- PSS standard enclosure size for housing PLC I/O modules is W: 600 mm, D: 800 mm, H: 2000 mm.
- The heat dissipation is 0.25 KW per enclosure.
- The PSS enclosures will have a high level of EMC protection. It is sheet steel, powder-coated on the outside and painted in RAL 2000.
- The cables enter the PSS enclosures from the top side.
To protect against electromagnetic interference, multipole earth rails with earth clamps will be installed at the top of PSS enclosures to:
 1. Terminate the screens of the cables/wires entering PSS cables.
 2. Provide grounding for equipment inside enclosures such as: PLC modules, power supplies, etc.
 3. Provide grounding for enclosure components.
- For system-compatible grounding of all enclosure parts on the enclosure frame, pre-assembled earth straps will be used.
- Wiring inside enclosures:
According to EN 60204-1 which is part of ESS electrical design rules, the insulated conductors will be colour coded as follows:
 - BLACK: ac and dc power circuits;
 - RED: ac control circuits;
 - BLUE: d.c. control circuits
 - ORANGE: interlock control circuits supplied from an external power source.

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

- **PSS Enclosures powering method**

The AC power (230 VAC) required for PSS enclosures is 1.5 kW per enclosure.

Requested DC power values for each PSS enclosure are as below:

- i. Buffer time : 60 min
- ii. Nominal current : 6 A
- iii. Minimal buffer voltage : 21.53 V

Using the **Siemens SITOP Selection Tool** to select the power supply and also find the matching uninterruptible power supply (DC UPS) based on battery technology, the following equipment will be installed in each PSS enclosure to provide the required DC power:

- i. Power Supply : SITOP PSU100S 24 V/10 A
- ii. DC UPS with batteries:
 - I. UPS : SITOP UPS1600 24V/10A
 - II. Battery : SITOP UPS1100 BATTERY MODULE WITH SERVICE- FREE SEALED LEAD BATTERIES FOR SITOP DC-UPS-MODULES 24 V 12 AH DC

10.4.3. Beam-off stations

Beam-off station is an enclosure with dimensions of H: 300 mm, W: 300 mm, D: 210 mm. It is sheet steel, powder-coated on the outside and painted in RAL 2000. Beam-off stations will be installed at various points in PSS controlled areas. Each beam-off station contains the following components and functions:

- Beam-off button to turn the proton beam off in case of emergency by the person(s) missed during patrol search and left behind in the tunnel.
- Oxygen deficiency hazard (ODH) indicator for different zones; showing the ODH status in each of the zones in PSS controlled areas.
- Search button to be used during search patrol.
- Buzzer to be used during search patrol.
- Signalling column showing alarms such as:
 - Red: ODH alarm in current zone
 - Blue: Proton beam ON
 - Green: TBD
 - Orange: TBD

10.4.4. Monitoring doors in PSS controlled areas

All doors in PSS controlled areas will be monitored according to the following design solutions:

Access doors:

Two switches of different technologies (to achieve diversity):

- Mechanical safety switch
- Non-contact magnetic safety switch

Fire doors:

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

In case of accelerator tunnel, the fire doors separate the exit routes from tunnel. To facilitate PSS search patrol these doors will be monitored by PSS using two switches of different technologies (to achieve diversity):

- Mechanical safety switch
- Non-contact magnetic safety switch

Emergency exit doors:

Two switches of different technologies (to achieve diversity):

- Mechanical safety switch
- Non-contact magnetic safety switch

E-exit special lock with following specifications:

- Spring locked (power to unlock)
- Escape release from inside (mechanical push button to release door)
- A special key driven override facility to unlock the unit from outside (to be used by fire protection in case of emergency or in the event of a power failure)

10.4.5. Access control system

In order to control and monitor the personnel access to PSS controlled areas at any time, there will be access points as below:

Accelerator tunnel:

- Front end building (G01 level 90)
- HEBT loading bay (G01 Level 100)

Target building:

- To be defined

The requirements by PSS on access system are:

- Double-door access system to ensure single person entry/exit.
- Entry of personnel upon identification thorough swipe system (password protected) and ESS databases.
- Monitoring of access system doors by safety switches as part of PSS safety instrumented functions.
- Interface between access system control box and PSS PLC to allow personnel in/out of PSS controlled areas.
- Accommodate PSS key exchange system inside the access system booth to be used for personnel access.
- Accommodate HMI inside the access system booth to be used for personnel access.
- Communication between the access system booth and Main Control System (MCR) by intercom.
- Video surveillance (CCTV) inside the access system booth to be used in MCR.

The access system dimensions and sub-systems are as below:

- Access booth dimensions: H: 2130 mm, W: 1070 mm, D: 1120 mm
- Two automatic glazed single swing doors.
- Mechanical override key available to unlock and open any of the two doors at any condition.
- CCTV

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

- Loudspeaker to broadcast control box messages.
- Intercom to communicate with MCR.

The access system has following features:

- Single person detection contact mat (2 zones).
- The contact mat has an identified central zone, with limited dimensions, on which user has to stay to validate there is just one person inside the booth.
- Objects of approx. below 15 kg are not detected in both zones.
- Configurable electronic Control Unit with power back-up (with 2 batteries 6,5 Ah)

The unit will be configured to provide the following signals:

- Send signals to PSS PLC to inform:
 - Long presence inside booth
 - Presence detection from the contact mat
 - Breaking Door 1
 - Breaking Door 2
 - Door 1 locked
 - Door 2 locked
 - Control box error
 - Door 1 opened too long
 - Door 2 opened too long
- Receive signals from PSS PLC to:
 - Open door 1 in entry/exit cycles.
 - Open door 2 in entry/exit cycles.

All interface signals are sent/received on dry contacts.

In case of power failure (loss of main power and back-up battery), door 1 unlocks (failsafe) and door 2 stays locked (fail secure).

Door 1 is interlocked with door 2 (D1 cannot be unlocked at the same time as D2).

10.4.6. Key exchange system

The PSS key exchange system (Trapped Key Interlock Switches) will be used to ensure that a predetermined sequence of events takes place or that hazards have been removed before personnel become exposed to them. This system ensures that the access process to PSS controlled areas is followed and cannot be circumvented or shortcut.

PSS will use modular key exchange units, which are used to exchange one or more keys for a number of other keys. The unit will contain stainless steel mechanical lock modules with uniquely coded keys.

The procedures to remove/enable proton beam, the sequence of using keys for access to PSS controlled areas, etc. are to be defined.

10.4.7. PSS blue/red lights

To be used as a layer of protection, PSS will install blue and red lights in PSS controlled areas. Each light fitting will have two luminaries (2x58W), which are separately switched.

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

The blue lights will turn on when the proton beam is on and the red lights will turn on when there is Oxygen Deficiency Hazard (ODH).

10.4.8. Message display system

Message displays will be installed at the access and emergency exit points to PSS controlled areas as a pre-warning for radiation hazards, ODH, access status, etc. The displays will be controlled by PSS PLCs.

10.4.9. Public address system

PSS public address system will be installed in all PSS controlled areas to broadcast messages during search patrol, or any other message that has to be broadcasted by PSS. Public address system will be triggered by PSS PLC(s).

10.4.10. PSS cable routes

As part of PSS safety requirements specifications in accordance with IEC 61508:2010, the two independent PSS trains should be physically separated to reduce the possibility of the PSS being affected by the same external events. Therefore, in any two train personnel safety system, the cables of each train (from sensor to logic solver to actuator) will run through two separated enclosed, sealed and marked containments/conduits.

10.4.11. PSS cables

Considering the requirements such as temperature, ionizing radiation, EMI and RFI at various levels in Accelerator, Target and Neutron instruments buildings, for signal and fiber optic cables, PSS will use radiation resistant (up to 1000 kGy), high temperature (up to 125 °C), individually screened, low frequency industrial cables in all PSS installations.

10.4.12. PSS interfaces

For PSS interfaces with various equipment in Accelerator, Target and each Neutron instrument, PSS will use the following type of equipment (more equipment will be added to this list as the PSS design gets more mature):

- Siemens SIRIUS contactor (3-pol, screw terminal, DC, 2NC+2NO) for PSS interfaces with AC power lines.
- Siemens SIRIUS contactor relay (4-pole, 2NO+2NC, screw terminal, DC circuit integrated) for PSS interfaces with low power DC equipment.
- Instantaneous under voltage release coil in Molded case circuit breakers (MCCB). As an example, to be used in case of PSS interface with RF modulators in accelerator.

The under voltage release coil instantaneously opens the circuit breaker when its supply voltage drops to a value between 35 % and 70 % of its rated voltage. If there is no supply on the release, it is impossible to close the circuit breaker, either manually or electrically. Any attempt to close the circuit breaker has no effect on the main contacts. Circuit breaker closing is enabled again when the supply voltage of the release returns to 85 % of its rated value.

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

The control signal for the under voltage coil passes through the two PSS contactor relays.

- PSS will install switches to monitor the status of RF waveguides and RF coaxial lines (the PSS switches specifications to be defined).
- PSS will use failsafe, 24 VDC RF switches with indicator mirror contacts to interface with Low level Radio Frequency systems (LLRF) in RF cells such as MEBT bunchers, RFQ, DTL(s), spoke cavities, etc.

The PSS devices for interfacing with other equipment will be installed in a sealed box painted and marked as PSS device. The access, maintenance and any modification to the PSS devices used for interfacing with other equipment during any mode of PSS operation shall only be done by an authorized PSS person.

10.4.13. Radiation monitors

Radiation monitors installed at strategic locations of Accelerator, Target and Neutron instruments buildings measure continuously dose levels and trigger a beam stop within a few milliseconds if pre-defined thresholds are being exceeded. If a critical radiation level (according to the thresholds set in the radiation monitor control units) is detected, two relays (for High Level Alarm) inside the radiation monitor's safety box will be triggered. Similarly, two relays are being triggered in case of errors in the radiation monitors detectors. The safety interlock system is interfacing these relays (High level alarm and Error) activating the SIF for radiation monitoring and removing beam permit if needed. The High level alarm and Error relays in each radiation monitor shall provide the trigger(s) to PSS PLC(s) through dry contact(s).

10.4.14. ODH monitors

The ODH Monitoring System will detect and alarm through the OXIGRAF oxygen deficiency monitors in the event of oxygen levels detected to be below 19.5%. In case of an oxygen level detected to be < 19.5%, the Cryogenics Control Room and the Main Control Room will be informed and Red lighting, Sirens & Strobe lighting, Beam off Station ODH indication will be turned on.

The Oxigraf sensor uses a laser diode absorption technology to measure oxygen concentration in the gas sample. It can be configured as Single or Multipoint Scan mode. An internal battery backup system will keep the O2iM operational and will report for one hour in case the external power is interrupted. From off state till full accuracy, the Oxigraf monitor needs approximately 10 minutes.

10.5. Personnel Safety Configuration Management and Quality Assurance Plan

10.5.1. PSS Configuration Management Plan

The PSS Configuration Management Plan gives requirements to the following:

- Planning of the process, including defining activities, responsibilities and the tools to be procured;

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

- Identifying uniquely the name and versions of each configuration item and when they are to be brought under configuration control (configuration identification);
- Identifying the versions of each software item which together constitute a specific version of a complete product (baseline), including re-used software, libraries, and purchased and customer supplied software;
- Identifying the versions of relevant hardware modules, including the hardware release and firmware version;
- Identifying, tracking and reporting of the status of items, including all actions and changes resulting from a change request or problem, from initiation through to release (configuration status accounting);
- Providing release management and delivery.

Change Management

No modification tracking

The first change management stage is “no modification tracking”.

This stage is applied as long as:

- A document or code is in work and has not been passed for approval the first time
- Changes to the document are reduced to correction of spelling mistakes
- Process- and Specification documents if they haven’t been officially passed to the customer the first time
- Software and Design- documents, if verification has not been started (before FAT).

In this stage changes to the items above are not tracked.

Request for Modification

Whenever a modification is requested, it is set to status “OPEN” in the CTL:

OPEN	Request for modification has been placed, but was not processed until now. This status is set by the initiator of the Modification Request
------	--

Impact Analysis

The responsible Designer does an impact analysis for the Modification Request.

In this impact analysis, the Designer points out:

- Which systems and modules are affected by the modification?
- Which documents are affected?
- How big is the effort (for each system or module and document)?
- How major is the modification?

The Designer classifies the parameters above with light / medium / heavy.

The Designer keeps record of the assumptions for the classification in the CTL.

Modification is safety-relevant

Any request for modification is assessed to be safety relevant. In this step, the Designer has to identify whether the modification is affecting any system-part with safety-relevant functionality. If e.g. code in the failsafe operating system is affected which is only relevant for e.g. diagnosis it is not needed to classify the modification as safety-relevant. Otherwise if signals from non-safety code are transferred into the safety-program it can

be seen as not safety relevant. This step is mainly necessary for modification of software but not limited to only these aspects.

Risk Assessment

In the Risk Assessment, the Designer analyses the risk of the modification with the parameters of the Impact analysis. The Designer is responsible to point out how dangerous the change can be. Points to assess are:

- Severity of the consequences in case of a module function change or subsystem by mistake
- Probability of occurrence of the function change
- Testability of the modifications

The Designer classifies the parameters above as low / medium / high. The Designer keeps record of the assumptions for the classification in the CTL.

Classification

In the Classification, the Designer defines whether the modification is “Major” or “Minor”. Manager shall approve the modification. The classification for Minor and Major can be seen in the table below. The classification depends on the parameters, classified during Risk Assessment and Impact Analysis. As the classification of the different parameters is done by the Designer and proven by the Verifier, it is subject to their individual understanding.

Impact Analysis			Risk Assessment			Classification
Light	Medium	heavy	Low	Medium	High	
		x	x			Major
		x		x		Major
		x			x	Major
	x		x			Minor
	x			x		Minor
	x				x	Major
x			x			Minor
x				x		Minor
x					x	Major

Table 1: Classification of Modifications

If the Modification Request has been classified, the status is set to “ANALYSED”:

ANALYSED	The request for modification is analysed. The Designer gives a recommendation for implementation of the modification request (YES or NO and why)
----------	--

Approval

The Safety relevant Modification Request has to be approved before the implementation starts during Change Management. Approval must be given by the Change Control Board, which consists of:

- Manager
- Designer
- Verifier
- Functional Safety Manager (if necessary)

The decision must be documented; comments by single roles can be added. The manager or a person who is authorized by the manager (e.g. DES or VER), can approve a Minor modification. If the modification is approved, the status is set to “APPROVED”, otherwise in case of refusal the request is set to “FINISHED”.

APPROVED	The modification is approved and can be implemented
FINISHED	<ul style="list-style-type: none"> - The safety relevant modification is not approved, no change is done - The non-safety relevant modification is approved

Manager could approve non-safety relevant changes solely after Designer analysed the impact to the system. Non-approve cases can be categorized as non-relevant modification request to the system.

Modification

The Designer implements the changes and modifies the documentation. If the Modification has been carried out, the status is set to “MODIFIED”.

MODIFIED	Changes are implemented but not yet tested.
----------	---

During Change Management finished- status is directly set after the implementation of the modification has been carried out, as the verification is performed independently with the relevant test concepts.

FINISHED	The modification has been implemented successfully, and the test has been carried out and is finished.
----------	--

Regression Test Concept

Parallel to the modification process, the Verifier develops the Regression Test concept. The mechanisms for the Regression Tests are depending on the influence on the system, identified during impact analysis.

Regression Test Review

During Regression Test Review, the Designer checks the Regression Test scenario for covering all critical items from the Impact Analysis and the Risk Assessment. In addition, the Designer decides whether the modifications are testable with the Regression Test Concept:

REVIEWED	The Regression Test concept has been reviewed and no changes are necessary
WRONG	The Regression Test has been reviewed and changes are necessary. The Designer must note a detailed failure description in order to provide enough information to enable the Verifier to correct the failure.

Regression Testing

After the modification has been implemented, the Verifier checks the correctness of the modification according to the test mechanisms developed parallel to the modification phase. After the regression testing has been carried out successfully, finished- status is set. If the regressions test has not been passed, the status is set to "FAILURE":

FAILURE	The modification has not been implemented correctly, changes are necessary. The Verifier must note a detailed failure description in order to provide enough information to enable the Designer to correct the failure. After the failure has been corrected, modified- status is set.
WRONG	If the Test Case is not usable, the Regression Test Concept must be adapted. The status is set to wrong and the Verifier changes the Regression Test Case. Before the test is carried out with the corrected Regression Test Concept, the Designer has to review the test case
FINISHED	The modification has been implemented successfully, and the test has been carried out and is finished.

Overview Change Management and failure documentation

The following figure gives an overview about the interactions between change management and documenting faults during test. For fault documentation the relevant checklist and failure description template is used. The Designer classifies the fault in "safety relevant" or "not safety relevant". In case the fault is not safety-relevant, the fault is only documented using the failure description template. The document number of this

failure description is the line number of the test list with always five digits. If the fault is classified as safety- relevant, a modification request is generated using the Design Change Request Template additionally. In this Design Change Request Template, the IDs of the failure descriptions are documented. The Design Change Requests are tracked via the CTL. After the Modification has been implemented, the test in the relevant check list is carried out again to verify the modification for being implemented correctly. Design Change Request not coming from a test are directly implemented into the CTL using the Design Change Request Template independent whether the request is safety-relevant or not.

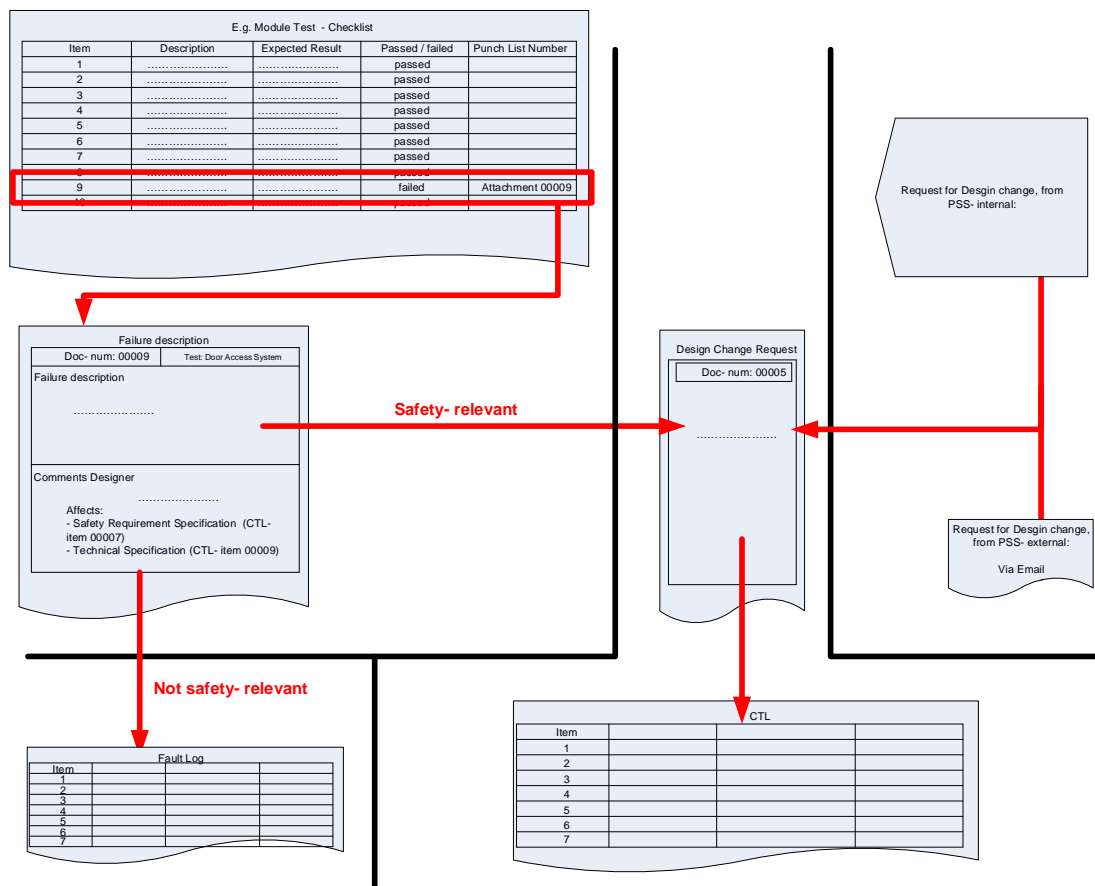


Figure 22: Document interactions during change management

10.5.2. PSS Development and Quality Assurance Plan

The objective of this Development Plan is to outline the methodology and approach that will be used to create the mainly the safety relevant functionality of PSS. The development is aimed to define the steps, necessary to design, create, verify and validate the whole system architecture. Main targets of this document are:

- Definition of management activities, which are necessary in the different phases of the system lifecycle of PSS

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

- Definition of the technical activities in the different phases of the safety lifecycle which are necessary to achieve the required functionality
- Definition of the responsibilities and activities of people, departments and organisations in each phase of the system lifecycle

Definition of Roles and Qualification

- Process controlling
One person shall be responsible for implementation of this process and shall also control compliance to the process.
- Design phase
All tasks, regarding system design can be conducted by the same person, but not by a person responsible for either verification or validation
- Verification and Validation
Tasks, regarding system verification or validation can be conducted by the same person, but not by a person responsible for system design, programming or installation.

Furthermore for the development of the safety-relevant PSS, roles and responsibilities are defined. One Person with full responsibility for the whole development has to be assigned to a role. It is possible to change the roles during development process. In this case a detailed handing over of all information has to be done between actual responsible and successor. The successor assigned to the role must be enabled to process previous PSS working packages if a modification request does affect them.

Safety Management and Lifecycle

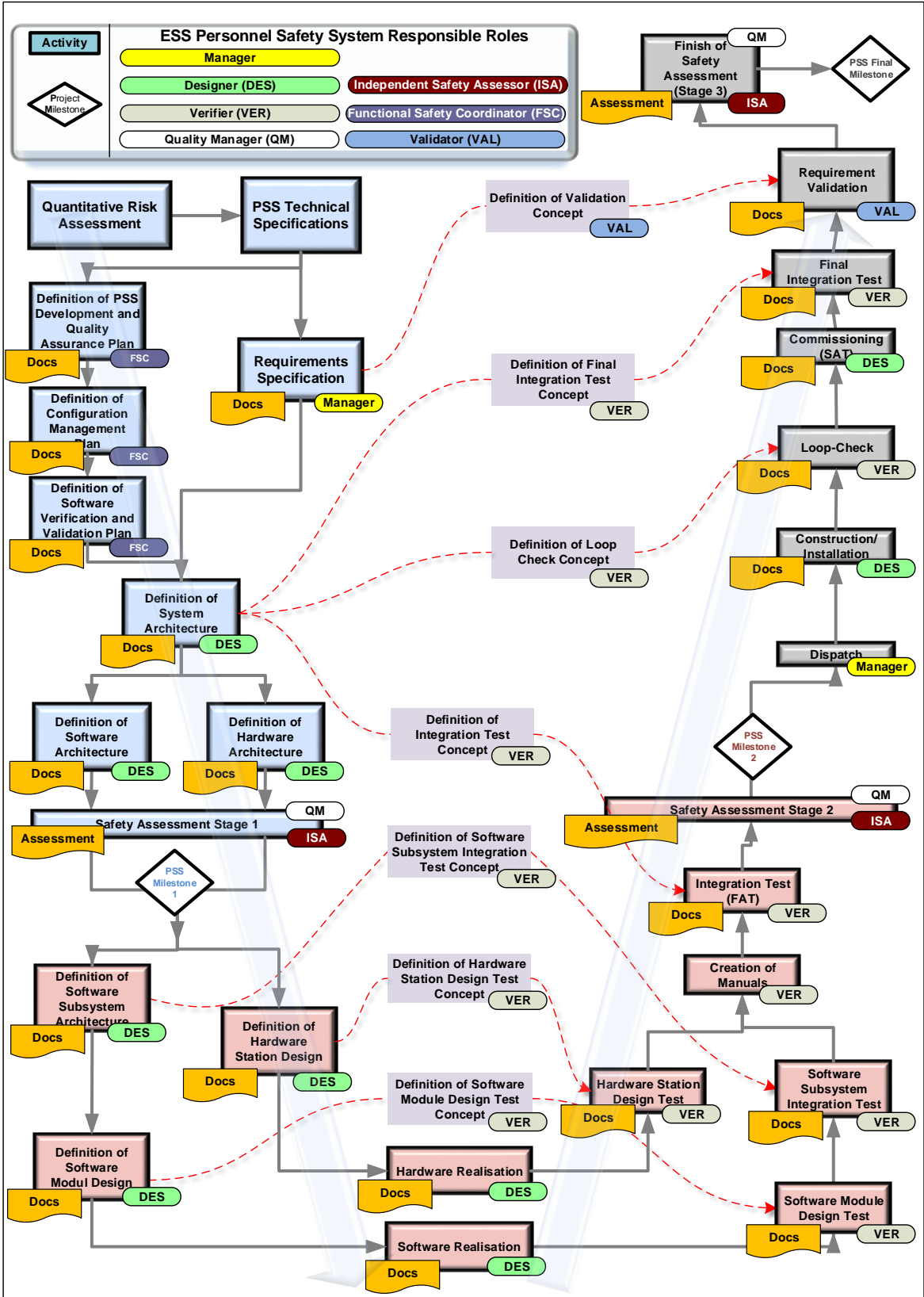


Figure 23: PSS Development Process (V – Cycle)

11. DEVIATIONS POLICY

11.1. Introduction

The aim of this chapter is to contribute to a quality risk management approach in the handling of deviations from a practical perspective as per ICS expectations on the matter. Deviation handling plays a key role in assuring quality in control systems and contributes to continuous improvement.

In this context, a deviation means that a delivered artefact, for instance a hardware component or a software package, does not meet its specifications. A situation when a potential deviation is found is called event.

The intent is to support effective and timely implementation of tools related to deviation management encountered during control systems implementation by concentrating resources and efforts to investigation of the root causes of relevant deviations.

11.2. Handling of Deviations and Non-Conformances

Potential deviations are identified and avoided by implementing risk control measures and preventive actions. The application of risk management in dealing with deviations is not only practical but provides a framework for a decision-making process based on a scientifically sound and objective approach. It also enables decisions to be confidently upheld before ESS System Responsible Officers (described in 4.2).

Under this approach, a sequence of steps may be identified when handling events and possible deviations:

1. Event detection
2. Deviation categorization
3. Deviation treatment
4. Root cause investigation
5. Corrective and preventive actions

11.2.1. Event detection

As a basic requirement, personnel involved in the implementation of control systems are expected to be alert and aware of possible undesirable events and clearly know what to do in terms of documenting and communicating them.

11.2.2. Deviation categorization

The decision tree depicted in Figure 24 is a simplified risk assessment that answers the following questions when an event is encountered:

- Can the event affect a control system attribute, operational parameter or the control system's quality?
- Does the event contradict or omit a requirement or instruction contemplated in any kind of approved written specification?

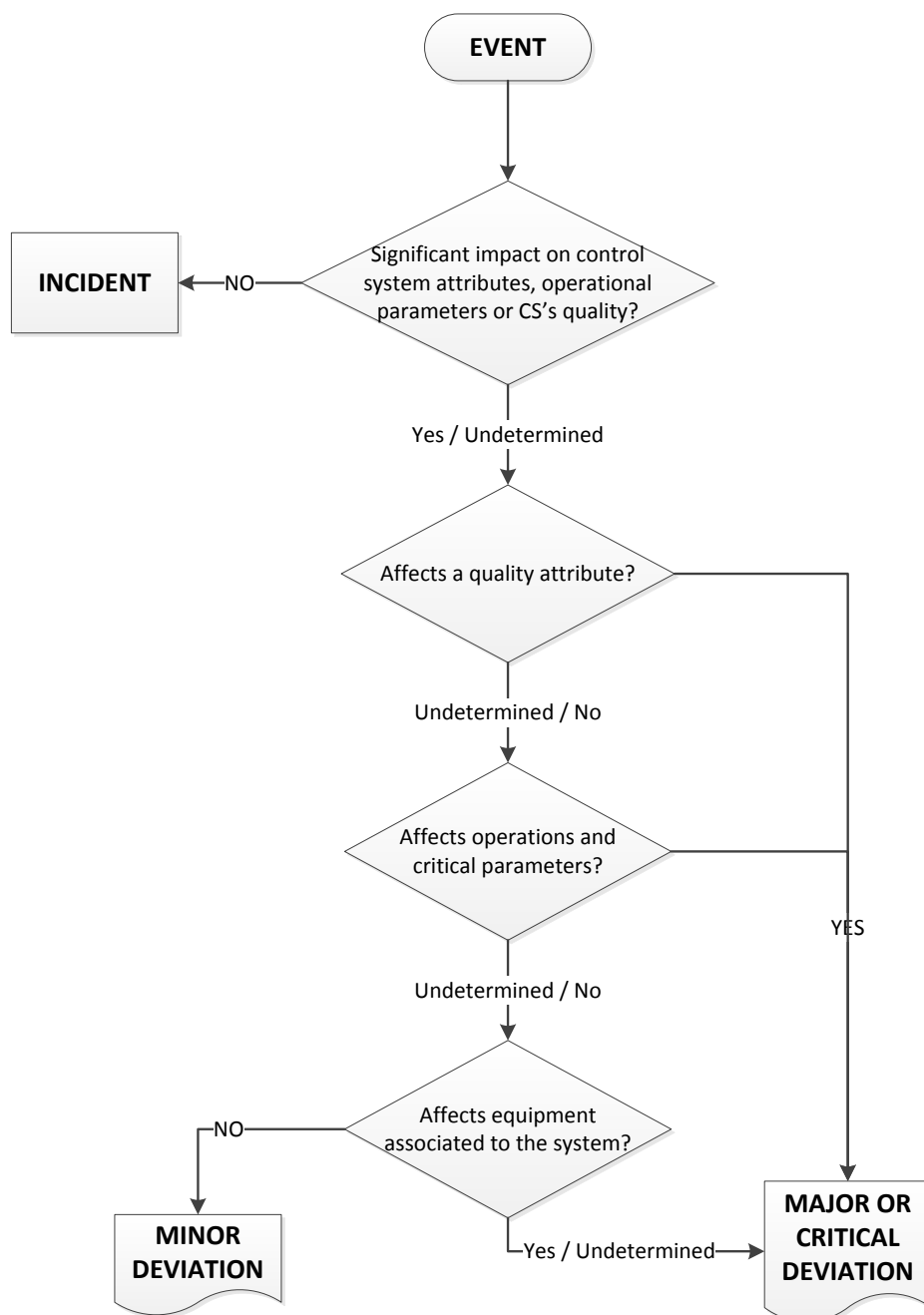


Figure 24 Decision making process for deviation classification

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

11.2.3. Deviation treatment

Incidents

Incidents need to be documented.

Minor deviations

An adequate description of the deviation requires documented objective evidence written in a concise and clear way stating time, location, and person that found the deviation when possible. Minor deviations are normally addressed by **Corrections** which are taken to correct and contain the problem (including immediate actions), based on sufficient documented evidence.

Corrections are immediate actions taken based on a simplified analysis of the deviation. Minor deviations do not necessarily require an investigation aimed at identifying the root causes of the problem as major and critical deviations do. Some corrections could require a change control.

The information, including the efficacy of the corrections, may be recorded in any form of data base (at ESS the Atlassian tools could be used as they are readily available) where it can be retrieved later during quality reviews or investigations.

Major or Critical deviations

Major or Critical deviation may be treated as follows:

1. Description (an adequate description associated to the deviation is essential in order to perform a meaningful investigation)
2. Correction (typically first addressed by corrections)
3. Efficacy of Correction
4. Batch Disposition, if applicable (e.g. a reprocess)
5. Root Cause Investigation
6. Corrective and preventive actions
7. Efficacy of Corrective Action
8. Conclusion
9. Data base record

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

11.2.4. Root cause investigation

Root cause investigation is used for quality improvement. Among the different tools available for root cause investigation, the “5 Whys” and “Ishikawa Fish Bone Diagram” are the simplest and most used ones.

The impact on the affected process, equipment or system should be addressed regarding other similar situations that could take place or will occur. A “vertical” analysis to identify the root cause should always be accompanied by a “horizontal” analysis on the possible events that could be avoided in the future by extending the scope of the investigation to evaluate the possible impact of the deviation on other similar systems.

It is reasonable to assume that often there will be deviations for which the root cause cannot be readily and clearly determined, and that a probable cause will not be determined. Also, in certain cases, the deviation will be attributed to unpredictable circumstances beyond control. In any case, conclusions and rationale should always be well supported and well documented.

11.2.5. Corrective and preventive actions

Corrective actions are taken to eliminate the root causes of deviations, and should be based on good quality investigations. Corrective actions are “reactive” in nature and are triggered in response to detected deviations and could generate preventive actions as well. These preventive actions (originally linked to nonconformities) will act on similar systems where there has not been yet a deviation.

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

12. APPENDICES

13. GLOSSARY

Term	Definition
IOC	Input-Output Controller, an EPICS software component
CHES	Document management system used at ESS
EPICS	Experimental Physics and Industrial Control System, the standard control system software for ESS
MCR	Main Control Room
PV	Process Variable
E2H2C	ESS Electronics Hardware Harmonisation Committee
HMI	Human-Machine Interface, also known as GUI (Graphical User Interface)
TA	Technical Annex, a document describing technical details of an in-kind contract
I&C	Instrumentation and Control
FAT	Factory Acceptance Test
SAT	Site Acceptance Test
MPS	Machine Protection System
PSS	Personnel Safety System
NSS	Neutron Scattering Systems, a division of ESS

14. REFERENCES

- [1] ICS Documentation Structure: ESS-0066423
- [2] Integrated Control System-Requirements Document: ESS-0057371
- [3] ICS-Accelerator Interface Control Document (ICD): ESS-005732
- [4] ICS-Target ICD: ESS-0005738
- [5] ICS-NSS ICD: ESS-0005735
- [6] ICS-CF ICD: ESS-0005737
- [7] ICS Hardware Platforms: ESS-0037909
- [8] Experimental Physics and Industrial Control System (EPICS):
<http://www.aps.anl.gov/epics/index.php>
- [9] pvAccess Protocol Specification: http://epics-pvdata.sourceforge.net/pvAccess_Protocol_Specification.html
- [10] ESS Alarm Strategy: ESS-0076326
- [11] ESS Naming Convention: ESS-0000757
- [12] <https://ess-ics.atlassian.net/wiki/display/HAR/How+to+install+an+EEE+module>
- [13] Ansible: <https://www.ansible.com/>
- [14] Vagrant: <https://www.vagrantup.com/>

Document Type	System Architecture Description
Document Number	ESS-0067637
Date	Mar 5, 2017
Revision	1
State	Released
Confidentiality Level	Public

- [15] Oracle VirtualBox: <https://www.virtualbox.org/>
- [16] ICS EPICS Environment: ESS-0067642
- [17] <https://ess-ics.atlassian.net/wiki/display/HAR/EPICS+Development+Workflow>
- [18] Python to pvAccess binding: <https://github.com/epics-base/pvaPy>
- [19] PostgreSQL Database: <https://www.postgresql.org/>
- [20] ESS JIRA: <https://ess-ics.atlassian.net/secure/Dashboard.jspa>
- [21] ESS BitBucket: <https://bitbucket.org/europeanspallationsource/>
- [22] Representational State Transfer (REST):
https://en.wikipedia.org/wiki/Representational_state_transfer
- [23] Control System Studio: <http://controlsystemstudio.org/>
- [24] OpenXAL: <https://openxal.github.io/>
- [25] Jupyter: <http://jupyter.org/>
- [26] MANTID: <http://www.mantidproject.org/>
- [27] Rsync description: <https://en.wikipedia.org/wiki/Rsync>
- [28] Available ESS EPICS Modules : <https://ess-ics.atlassian.net/wiki/display/HAR/EPICS+Modules>
- [29] Archiver Appliance documentation:
https://slacmshankar.github.io/epicsarchiver_docs/
- [30] Archiver Appliance at ESS: <https://ess-ics.atlassian.net/wiki/display/CSS/Archive+Service>
- [31] Alarm Service at ESS: <https://ess-ics.atlassian.net/wiki/display/CSS/Alarm+Service>
- [32] ESS Logbook: <https://logbook.esss.lu.se>
- [33] Role-Based Access Control: <https://ess-ics.atlassian.net/wiki/display/CSS/RBAC>
- [34] Kameleon device simulator: <https://ess-ics.atlassian.net/wiki/display/CDM/Kameleon>
- [35] MicroTCA: <https://www.picmg.org/openstandards/microtca/>
- [36] EtherCAT Technology Group: <https://www.ethercat.org/default.htm>
- [37] Beckhoff TwinCAT: <https://www.beckhoff.be/english.asp?twincat/default.htm>
- [38] Ethernet patch cable colours: <https://ess-ics.atlassian.net/wiki/display/HAR/Colour+Standards+for+Ethernet+Cabling>
- [39] ICS network subnet addresses (Please first login to view the file): https://ess-ics.atlassian.net/wiki/pages/worddav/preview.action?fileName=IP_address_plan.xlsx&pageId=39780882
- [40] Machine Protection - Systems Engineering Management Plan, ESS-0057245
- [41] ESS Systems Engineering Management Plan, ESS-0002908

DOCUMENT REVISION HISTORY

Revision	Reason for and description of change	Author	Date
1	First skeleton draft	Timo Korhonen	2016-02-01
2	First draft for release	Timo Korhonen	2016-09-08
3	Incorporated review comments	Timo Korhonen	2016-12-06