ISBN: 978-3-95450-238-7 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2023-TUPDP078

MANAGEMENT OF CONFIGURATION FOR PROTECTION SYSTEMS AT ESS

M. Carroll, G. Ljungquist, M. Mansouri, D. Paulic, A. Nordt
European Spallation Source, Lund, Sweden

Abstract

The European Spallation Source (ESS) in Sweden is one of the largest science and technology infrastructure projects being built today. The facility design and construction includes the most powerful linear proton accelerator ever built, a five-tonne, helium-cooled tungsten target wheel and 22 state-of-the-art neutron instruments. The Protection Systems Group (PSG), as part of the Integrated Control Systems (ICS) Division at ESS, are responsible for the delivery and management of all the Personnel Safety Systems (PSS) and Machine Protection Systems (MPS), consisting of up to 30 PSS control systems and 6 machine protection systems. Due to the bespoke and evolving nature of the facility, managing the configuration of all these systems poses a significant challenge for the team. This paper will describe the methodology followed to ensure that the correct configuration is correctly implemented and maintained throughout the full engineering lifecycle for these systems.

INTRODUCTION

In any facility, good configuration management is essential for maintaining the reliability and integrity of complex systems by preventing system inconsistencies, uncontrolled changes and conformity issues when related to regulatory bodies. Further when it comes to safety and protection systems, the failure to implement robust configuration management can be catastrophic as was demonstrated in high profile accidents such as the piper alpha disaster in 1988 [1] and the deep water horizon accident in 2010 [2]. In both these cases, poor configuration management was credited as one of the key contributing factors where uncontrolled or improperly made changes ultimately led to multiple fatalities, irreversible environmental damage and ultimately severe regulatory penalties for the companies involved. Accidents like these and personal experience from working at multiple facilities with various levels of configuration management, has demonstrated the cost of overlooking this process, especially when designing and implementing safety and protection systems. Further the requirement for configuration management is mandated from the functional safety standards IEC 61511-1:2016 [3] used for the development of personnel safety systems, and EN 61508 [4] used for the development of machine protection systems at ESS.

CONFIGURATION MANAGEMENT

The key elements of the configuration management strategy used by the PSG team are shown below and in Figure 1 with further details in the following chapters.

1. Configuration Identification
2. Version Control
3. Change Management
4. Configuration Auditing

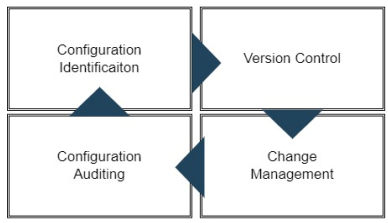

Figure 1: Configuration management elements.

CONFIGURATION IDENTIFICATION

The correct management of the configuration for PSG systems at ESS first requires that a system configuration is accurately identified in the initial design phase. This establishes an approved baseline for the system through a detailed documentation strategy. To achieve this each system has the following key documentation package developed through the design process.

- Concept of Operation (Conops)
- System Requirement Specification (SRS)
- Interface Control Documents (ICDs)
- Detailed Design Specification (DDS) / Electrical Schematics
- Test Specifications (see configuration auditing)

Concept of Operation

The 'Conops' document identifies at a high level the key conceptual requirements of the system, such as who the main interfacing systems and stakeholders are, how the stakeholders are expected to interact with the system and how the system is expected to interact with the rest of the facility.

System Requirement Specification

The *SRS* is a document used to collect all the requirements for a system, with a unique 'SRS-ID' for each requirement and a link back to the source of the requirement. Sources typically come from operational requirements originated in the Conops or as Safety Implemented Functions (SIFs) described in Safety Integrity Level (SIL) assessments or machine protection (MP) functions (PFs) from an MP analysis. An example can be seen in Table 1.

ISBN: 978-3-95450-238-7 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2023-TUPDP078

Table 1: SRS Example

ID	Source	Requirement
SRS-001	SIF-001	'System' shall notify system *x* when input *y* is over *threshold z*.

Interface Control Document

The ICDs are documents which are created to specify the interface between two or more systems and identifies technologies used, logic to be represented over the interface, and how the responsibilities are divided between the different stakeholders. An example schematic from an ICD can be seen in Figure 2.

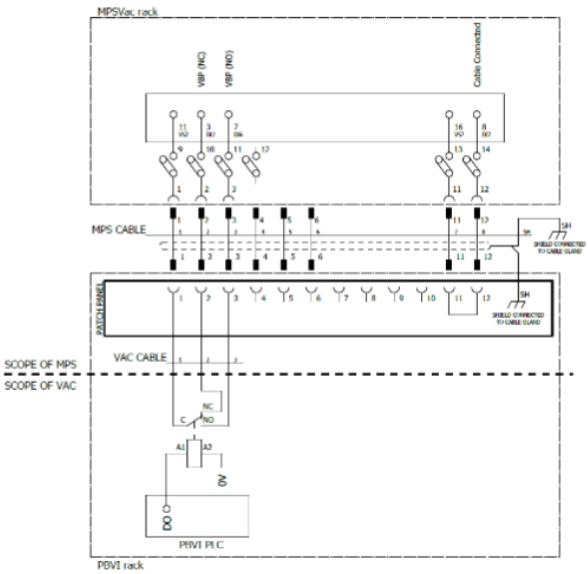

Figure 2: ICD example - machine protection interface with vacuum interlock system.

Detailed Design Specification / Electrical Schematics

Once all the requirements have been collected in the SRS and the key interfaces have been identified in ICDs, a DDS document is created for the system which collects all the different key design and functional elements required to implement each requirement listed in the SRS. The DDS has a number of 'DDS-ID' elements linked back to the rel-evant SRS-ID, which are intended to be written in verifia-ble steps to be incorporated in the system. The electrical schematics are also produced at this point to show in detail how the system and interfaces are to be installed. An ex-ample of a DDS table for SRS-001 can be seen in Table 2.

Table 2: DDS Example

ID	Source	Design Specification
DDS-001	SRS-001	read ai from y on I001.1 & I001.2
DDS-002	SRS-001	perform diagnostic on input signals….
DDS-003	SRS-001	scale input values, displays on OPI
DDS-004	SRS-001	Store constants for high limits
DDS-005	SRS-001	read reset signal from the OPI
DDS-006	SRS-001	check input values (DDS-001) are below constants (DDS-004)
DDS-007	SRS-001	energise output for Q001.1 when (DDS-006) is true, (DDS-002) no error, when (DDS-05) is pressed.

Once the designs have been completed and all the documentation is agreed with the relevant stakeholders, an 'as designed' baseline is registered with the ESS facility Configuration Item Documentation List (CIDL).

VERSION CONTROL

After the 'as designed' baseline is established, the system development takes place including installation and software/firmware development and deployment based on the DDS documentation and electrical schematics. All versions of software at this point are stored in their official repositories (see tools section below) with a versioning comment to indicate the stage of the development. After verification is completed the numbering indicates that the code is production code which matches the functionality as described in the baseline at the time of verification. For the PLC based systems, the checksums of the latest software are also stored in a configuration file which is continuously read and compared against the latest values calculated by the PLC. The system will remain in a safe state unless these values match preventing unintended operation with a different version of code than what was verified.

CHANGE MANAGEMENT

From this point, changes to the systems shall only be made based on a new requirement and require that an official ESS change control procedure is used. This procedure covers the basic procedural elements of standard change management as shown in Figure 3. Where a change request is created, identifying all affected systems and stakeholders, an impact assessment is performed to ensure no other unintended effects are anticipated, the change is approved or rejected by all stakeholders, and only then the change is implemented and verified. Changes to a system follow the same process as in the initial identification process where Conops, SRS, ICDs and DDS are updated as required. The verification process must ensure that the change is implemented correctly as per the documentation, and further appropriate regression performed to ensure that no other unintended changes have been incorporated.

ISBN: 978-3-95450-238-7 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2023-TUPDP078

Figure 3: Change management process.

After this point the system baseline is updated again with the new revisions of documentation and the official repositories identify the new code as the latest production version.

CONFIGURATION AUDITING

Configuration auditing is a continuous process through all phases of configuration management which consists mainly of configuration reviews and system verification.

Configuration Reviews

During the configuration identification process formal reviews are performed to ensure that, first through a Preliminary Design Review (PDR) that the requirements assigned to the system are sufficient to fulfil the facility needs, then through a Critical Design Review (CDR) that the system functionality as described in the baseline can fulfil the requirements assigned to the system. These formal reviews will be attended by the relevant stakeholders and other internal or external domain experts, who together will assess the documentation and approve the system to proceed to the next phase of design or implementation. Some other key formal reviews include Installation Readiness Review (IRR), Test Readiness Review (TRR) and System Acceptance Review (SAR).

System Verification

System verifications are performed using a V-Model to verify that the design specification as defined in the DDS has been fulfilled and that the system has been implemented correctly. To check this, various stages of testing are completed such as Factory Acceptance Testing (FAT) and Site Acceptance Testing (SAT) during the implementation process. The main functional verification performed for a system as a SAT is called the Site Integration Test (SIT). The SIT test specification is developed based on the information contained in the DDS document where each of the test scenarios in the specification is linked through the 'DDS-ID' and is written to challenge a verifiable functional element of the DDS, an example with linking can be seen in Table 3. Through this process, when all the 'DDS-IDs' are verified, it has demonstrated that all the design elements for each system requirement have been implemented, and that the system configuration is known to be as described in the baseline. Where some DDS items are not easily verifiable these must be identified and then verified or validated through a code review process or other suitable means.

Table 3: Test Specification Example

Test Steps	Source	Test Description
1.1,2,3…	DDS-001	verify ai inputs I001.1 & I001.2
2.1,3,3…	DDS-002	verify diagnostics (wire break etc.)
3.1,2,3…	DDS-003	verify scaling functions

After SIT specification is executed and the system is verified, the configuration is established and an 'as verified' baseline is registered with the CIDL. This means that the documentation at this point in time is confirmed to correspond to the functionality of our system as it is in the field with all requirements fulfilled. Once all the systems at ESS have been integrated and a Final Integration Test (FIT) has been performed, beam can be generated and commissioned. After this point an additional as operated baseline will be released.

TOOLS

The main tools and services used as part of the PSG configuration management process are shown below.

- ESS Configuration Identification Document List (CIDL) System – the CIDL is an internal framework for baselining documentation identified as part of a systems configuration. This has three different baseline phases called as designed, as verified and as operated. A facility baseline is created when all systems relevant have released a baseline for each phase.
- ESS Change Management System – framework for managing changes between different stakeholders at ESS. This is used for monitoring changes and ensuring correct stakeholders are identified.
- CHESS – Document management system for storing, versioning and managing approvals for all ESS documentation.
- JIRA – tool used for issue tracking and project management at ESS. When changes are to be made, Jira can be first used to notify and collect all relevant tasks related to the change, then used to follow them to completion.
- EAM – Maintenance management systems and tool intended to be used for scheduling changes to ensure operations can control and are informed of when changes are made.

ISBN: 978-3-95450-238-7 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2023-TUPDP078

- GitLab – repository for storing and controlling versioning for EPICS related IOC Code and OPIs.
- Artifactory – firmware repository and used for versioning.
- Versiondog [5] - repository for storing and controlling versioning for PLC and HMI Code for PLC based systems.

CHALLENGES

As with any facility, one of the key challenges for configuration management is schedule and cost constraints. These constraints can often lead to important steps in the process being overlooked or deferred in an attempt to make quick schedule or cost gains. Through personal experience, these short term gains will often lead to much higher schedule or cost implications due to requirements not being fully understood, insufficient test coverage in the verification process, or from errors being introduced through uncontrolled changes to the configuration. Another challenge is to ensure that there is a consistent approach followed by all stakeholders. This is especially important for systems like the ones developed by PSG as they have many interfaces to different stakeholder equipment, and have a high risk of their configuration being affected by an uncontrolled change to an interfacing system. This risk can only be solved if all stakeholders are encouraged to follow the same internal processes consistently.

CONCLUSION

Implementing and maintaining robust configuration management is key for ensuring the continued reliable and safe operation for any critical system; failure to do this can lead to increased downtime, higher maintenance costs and even to disaster as shown in the piper alpha and deep water horizon accidents.

The key elements of the configuration management strategy used by the PSG team at ESS was described in this paper. So far we have found this process to be effective for managing the configuration and to ensure that our systems' design fulfil the requirements assigned, and that they then continue to operate as designed.

REFERENCES

[1] The Public Inquiry into the Piper Alpha Disaster, https://www.hse.gov.uk/offshore/piper-alpha-disaster-public-inquiry.htm

[2] The National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, https://www.govinfo.gov/content/pkg/GPO-OIL-COMMISSION/pdf/GPO-OILCOMMISSION.pdf

[3] IEC 61508, https://webstore.iec.ch/publication/5515

[4] IEC 61511, https://webstore.iec.ch/publication/24241

[5] Versiondog automation change management system, https://auvesy-mdt.com/en/versiondog