

Charge Document for the Test Stand 2 Personnel Safety System Preliminary Design Review

Preliminary Design Review (PDR)
11 February 2019, Lund, Sweden

Charge for the PDR

Purpose of this PDR

The purpose of this PDR is to confirm that the initiating events, safety functions, requirements and interfaces are well understood, defined and documented; and that a preliminary design and concepts of operation sufficiently cover the high level system requirements.

The PDR also covers planning activities for the following processes:

- Configuration management,
- Software development,
- Verification and validation.

Supporting documentation

The expected outputs of safety analysis and preliminary design, which should be presented and reviewed in this PDR, will be documented in the following documents:

- Initiating Events Analysis for the Test Stand 2 Personnel Safety System
- Initiating Events Register for the Test Stand 2 Personnel Safety System
- SIL Determination for the Test Stand 2 Personnel Safety System
- Concepts of Operations for the Test Stand 2 Personnel Safety System
- Safety Requirements Specification for the Test Stand 2 Personnel Safety System
- System Architecture for the Test Stand 2 Personnel Safety System
- Hardware Requirements Specification for the Test Stand 2 Personnel Safety System
- Software Requirements Specification for the Test Stand 2 Personnel Safety System
- Interface Control Document for the Test Stand 2 Personnel Safety System

For reviewing the planning activities for the Test Stand 2 Personnel Safety System, the following general PSS documents will be used:

- Safety Plan for Personnel Safety Systems (ESS-0469185)
- Software Development Plan for Personnel Safety System (ESS-0330956)
- Verification and Validation Plan for Personnel Safety Systems (ESS-0328060)
- Configuration Management Plan for Safety Critical Systems (ESS-0058389).

PDR committee

The PDR committee consists of:

- John Weisend, AD - Group Leader for Specialised Technical Services Group (chair)
- Wolfgang Hees, AD - Section Leader for Utilities and Test Stands Section
- Helen Boyer, ES&H – Group Leader for Occupational Health & Safety Group
- Timo Korhonen, ICS - Chief Engineer
- Thilo Friedrich, ICS - Systems Engineering and Engineering Process Coordinator/Engineer

Presenters:

- Stuart Birch, ICS - Senior Engineer, Personnel Safety Systems
- Morteza Mansouri, ICS - Lead integrator Engineer for safety critical systems
- Paulina Skog, ICS – Technical Documentation Specialist
- Meike Rönn, ICS - Technical Documentation Specialist
- Fan Ye, ESC UK - PSS Safety Engineer, Isograph Expert
- Denis Paulic, ICS - Deputy Group Leader for Protection Systems Group

Committee Charge

The supporting documentation will be provided to the committee 5 days in advance, on the review Indico page, which also contains the agenda and presentations:

<https://indico.esss.lu.se/event/1193/>

- 13:00 Committee discussion (closed)
- 13:15 Introduction and PSS safety plan
- 13:45 Verification and validation plan
- 14:05 Safety analysis and safety functions
- 14:35 Coffee break
- 14:50 System architecture, Concepts of operations and Interfaces
- 15:20 Software development plan and software requirements
- 15:45 Configuration management plan
- 16:00 Committee deliberations (closed)
- 16:50 Closeout

The committee is asked to consider the following questions:

1. Have all action items from the Pre-Start Review been resolved properly to allow preparation of this PDR?
2. Are all or a sufficient coverage of requirements, safety objectives and specifications within the scope of this PDR documented and understood?
3. Is the safety plan for developing PSS systems such as TS2 PSS clear and properly documented?
4. Is the proposed implementation of the Oxygen Deficiency Hazard (ODH) detection system for TS2 acceptable?
5. Have all initiating events been identified and sufficiently evaluated in the initiating events analysis?

Document Type	Agenda	Date	Jan 31, 2019
Document Number	ESS-0680092	State	Released
Revision	1	Confidentiality Level	Internal

6. Have all safety requirements from the TS2 risk assessment been addressed in the TS2 PSS safety analysis and covered by the identified safety instrumented functions (SIF) and are they traceable through the process?
7. Is the validation and verification planning clear and appropriate for this stage of the project?
8. Have all operating procedures for TS2 PSS been addressed and are they properly documented?
9. Is the system architecture clear and mature enough for this stage of the project?
10. Have all interfaces with other systems been identified and agreed with system stakeholders, and properly documented for this stage of the project?
11. Does the planning for software development meet the requirements within the scope of this PDR?
12. Is the configuration management plan appropriate for this stage of the project and is it clear how modifications will be traced?
13. Are there any outstanding agreements to be made or other actions necessary to allow the PSS team to transition to detailed hardware and software design?
14. The results of the review should be summarized in a short report, outlining the answers to the above review questions and whether the review is considered passed, passed with action items, or failed.

The report may also provide findings, comments, and recommended actions. Actions should be clearly categorized as one of the following:

- Shall be addressed before PDR is considered closed
- Shall be addressed prior to the CDR