Charge Document for the Test Stand 2 Personnel Safety System (TS2 PSS) Critical Design Review

Critical Design Review (CDR)
9 April 2019, Lund, Sweden

Charge for the CDR

Purpose of this CDR

The purpose of this CDR is to confirm that hardware and software design, and planning activities for the Test Stand 2 Personnel Safety System (TS2 PSS) are likely to meet all requirements and safety objectives and are specified in sufficient detail for design and integration testing, installation and commissioning.

Supplementary documentation

The expected outputs of detailed design, which should be presented and reviewed in this CDR, are covered in following documents:

- Concepts of Operation for TS2 PSS (ESS-0304995) – 3rd revision
- Updated analysis documents:
  - TS2 PSS Initiating Events Analysis Document (ESS-0468688)
  - TS2 PSS Initiating Events Register (ESS-0507830)
  - SIL Determination Report for TS2 PSS (ESS-0288441)
- Safety Requirements Specification for TS2 PSS (ESS-0288460)
- SIL Verification for TS2 PSS (ESS-0478596)
- Hardware Requirements Specifications document for TS2 PSS (ESS-0707794)
- Software Requirements Specification document for TS2 PSS (ESS-0681179)
- V&V plan specific for TS2 PSS (ESS-1075793)
- Updated Configuration Management Plan for Safety Critical Systems (ESS-1074904)
- TS2 PSS and TS2 RF Systems Interface Control Document (ESS-0517355)
- TS2 PSS and TS2 Radiation Monitors Interface Control Document (ESS-0517371)
- TS2 PSS Electrical and Mechanical Drawings Document (ESS-0508473) – 2nd revision
- TS2 PSS Hardware Design Specifications Document (ESS-0515707)
- TS2 PSS Software Design Document (ESS-0515371)
- Installation and Commissioning Plan for TS2 PSS (ESS-1076214)

The supporting documentation will be provided via email to the committee members about one week in advance.

CDR Committee

The CDR 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
- Annika Nordt, ICS - Group Leader for Protection Systems Group
- Joakim Söder, ICS – Electrical 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
- Peter Holgersson, ICS - Senior Technician
- Alberto Toral Diez, ICS – Technician
- Mattias Eriksson, ICS – Technician
- Denis Paulic, ICS - Deputy Group Leader for Protection Systems Group

Agenda

The agenda for the review is available on the Indico page:
https://indico.esss.lu.se/event/1222/
Preliminary agenda:

- 13:00 Committee discussion (closed)
- 13:15 PDR follow-up, SIL verification and updates on safety analysis
- 13:40 Verification and validation plan for TS2 PSS
- 14:00 Updates on concepts of operation and system's architecture
- 14:20 Hardware integration and interfaces
- 14:40 Hardware requirements, electrical and mechanical design
- 15:00 Coffee Break
- 15:15 Software requirements and software design
- 15:40 Progress on configuration management - example for TS2 PSS
- 16:00 Installation and commissioning plan
- 16:20 Committee deliberations (closed)
- 17:10 Closeout

Committee Charge

The committee is asked to consider the following questions:

1. Are all or a sufficient coverage of requirements, safety objectives and specifications within the scope of this CDR documented and understood?
2. Have all of the recommendations from the PDR been satisfactorily addressed?

a. Are the changes in operation procedures added so that the waveguide removal interlock is Safety Integrity Level (SIL) 2 (or lower) rated?
b. Are the cross references and traceability between risks and requirements in the documentation properly addressed?
c. Is the recommended solution for the ODH detection system tied into TS2 PSS design?
d. Have possible common mode failures been addressed and presented at this CDR?

Note: V&V recommendation is addressed in the next question.

3. Is the TS2 PSS specific verification and validation planning clear and appropriate for this stage of the project?
4. Does the committee believe that the TS2 PSS safety analysis satisfactorily verifies that the system design meets the required safety integrity levels?
5. Are the updates on operating procedures clear and properly documented?
6. Are the interfaces with RF systems and Radiation monitors clear and well understood?
7. Does the hardware design meet the requirements within the scope of this CDR?
8. Have the software requirements been properly documented, with traceability to higher level requirements?
9. Does the software design meet the requirements within the scope of this CDR?
10. Is it clear from the presentation how modifications and changes are planned to be managed, traced and documented for TS2 PSS?
11. Are the installation and commissioning strategies appropriate for this stage of the project?
12. Are there any outstanding agreements to be made or other actions necessary to allow the PSS team to transition to hardware and software design and integration testing, installation and commissioning phases?

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:

- Must be addressed before CDR is considered closed
- Must be addressed prior to the system verification
- Must be addressed at some time during the project