PERSONNEL SAFETY SYSTEMS FOR THE EUROPEAN SPALLATION SOURCE

S. L. Birch, A. Nordt, D. Paulic
European Spallation Source, ESS, Lund, Sweden

Abstract

Providing and assuring safe conditions for personnel is a key parameter required to operate the European Spallation Source (ESS).

The ESS will be responsible for developing all of the facility personnel safety related systems. All of these systems will be developed by the Integrated Control Systems Division (ICS) and all will be designed, manufactured, commissioned and operated in accordance with the IEC61508 standard, with regard to functional safety for Electrical/Electronic and Programmable Electronic (E/E/PE) safety related systems. This paper describes the ESS Personnel safety system's scope, strategy, initial design requirements, and methodology but also provides an update of the system design progress so far.

INTRODUCTION

In fall 2014 construction of the European Spallation Source (ESS) in Lund, Sweden started. The facility will comprise of a 2 GeV, 5 MW proton accelerator, a heavy metal tungsten target and 22 state of the art neutron instruments. The Integrated Control Systems (ICS) division will be responsible for the design, procurement, installation, commissioning and validation of all personnel safety systems at ESS.

PERSONNEL SAFETY SYSTEMS SCOPE

In late 2014 the overall scope of the ESS personnel safety systems was defined and 10 main systems were identified that are required to be commissioned, validated and operational for first beam of the European Spallation Source (ESS) facility in 2019. These systems are:

- The PSS for the on-site Cryogenic module test stand,
- The Accelerator Personnel Safety System,
- The Accelerator Radiation Monitoring System,
- The Accelerator Oxygen Depletion System,
- The Target Personnel Safety System,
- The Target Radiation Monitoring System,
- The Target Hot/Maintenance Cell Personnel Safety System,
- The Neutron Instrument LOKI Personnel Safety System,
- The Neutron Instrument NMX Personnel Safety System,
- The Neutron Instrument ODIN Personnel Safety System.

STANDARDS

IEC61508

As with many facilities within the accelerator research field, consensus has been that the international standard IEC61508-2010 [1] forms best practice for personnel safety systems. This has resulted in the wide adoption of this standard throughout many research facilities in the world. For it's personnel safety systems, ESS will implement the design, manufacture, commissioning, validation and operation in accordance with this standard. The IEC61508 lifecycle that ESS will follow is shown in Figure 1.

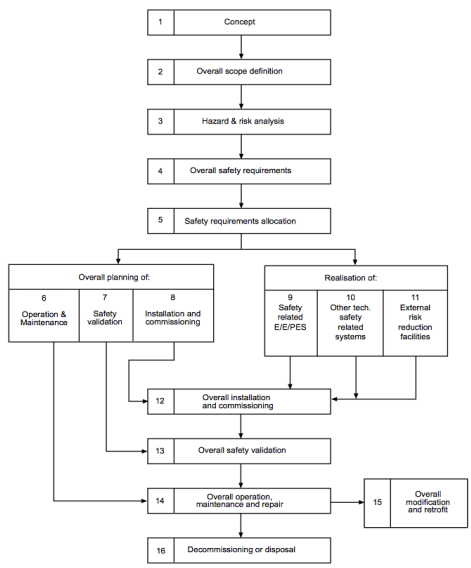

Figure 1: IEC61508 safety lifecycle.

Strålsäkerhetsmyndigheten (SSM) Swedish Radiation Authority

As part of the license application the SSM (the Swedish Radiation Authority) has requested that the ESS Personnel Safety Systems meet:

- SSM2014-127-1 [2]: "Review of application for licence for activity involving ionizing radiation" chapter 10 "review of control systems",
- SSMFS 2008-27 [3]: The Swedish Radiation Authority's "regulations concerning operations at accelerators and with sealed radiation sources".

It is important to point out that the ESS personnel safety systems primarily prevent both the public and workers

from the facility's ionizing radiation hazards but also identify as well as mitigate against all other potential hazards such as high voltage, radio frequency and oxygen depletion.

STRATEGY

To enable compliance of the standards mentioned above all personnel safety systems will comprise of a failsafe two-train system (two independent technical systems) that will be designed to cater for the following:

- Common Cause Failure: The result of one or more events, causing concurrent failures of two or more separate channels in a multiple channel system, leading to a system failure.
- Diversity: Different means and/or technologies used to perform a required function.
- Redundancy: The existence of more than one means for performing a required function or for representing information.
- Separation: Physical separation of independent systems to reduce the possibility of the personnel safety systems being affected by the same external event.
- Single failure: An occurrence, which results in the loss of capability of a component to perform its intended safety functions.
- External event: An external event such as earthquake, flooding, fire and power failure which can directly affect the facility and cause the degradation of the ESS personnel safety systems.

RISK

Three layers of risk reduction will take the residual risk beyond the maximum tolerable risk after protective measures have been taken. Figure 2 shows the risk reduction concept.

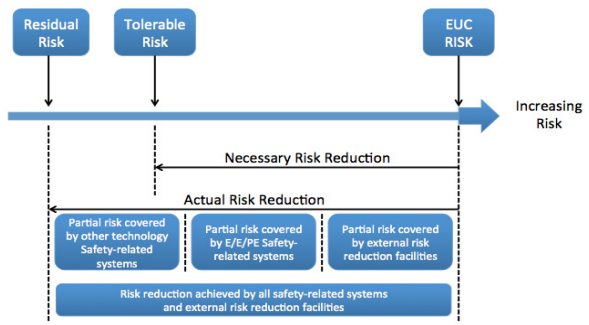

Figure 2: Risk reduction concept.

SAFETY PLC

The ESS personnel safety systems will use Siemens failsafe safety Programmable Logic Controller (PLC) systems as part of the actual risk reduction strategy.

Fail-safe PLC System

A fail-safe PLC serves to control processes and immediately switches to a safer state or remains in the current state if a fault occurs. It can be operated in STANDARD or FAIL-SAFE mode as shown in Figure 3.

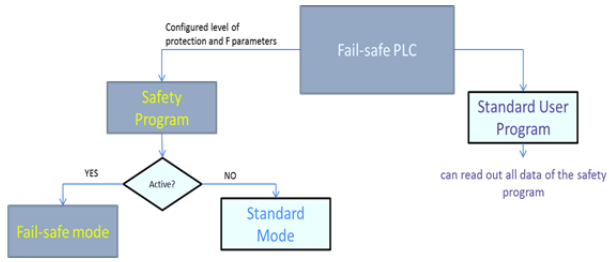

Figure 3: Fail-safe PLC operational modes.

Fail-safe signal modules react to faults similar to standard PLC modules when operated in standard mode and the standard user program can read out all data of the safety program, for example, through symbolic (fully qualified) accesses which can be very useful for system testing and debugging. Differences in accessing the process images from standard and fail-safe parts of the program are shown in Table 1.

Table 1: Read and Write Accesses from Standard and Safety Program Sections

		From standard user program		From safety program	
		Read	Write	Read	Write
Process image of standard I/O	Input	P	P	P	N
	Output	P	P	N	P
Process image of F-I/O	Input	P	N	P	N
	Output	P	N	N	P

P - permitted; N – not permitted

The latest generation of the fail-safe Siemens PLCs (SIMATIC safety) will be used for implementation of the safety concepts for personnel safety related systems (for example, for emergency stop devices for powering and processing equipment). SIMATIC safety F-systems can satisfy the following safety requirements:

- Safety Integrity Level SIL3 in accordance with IEC 61508:2010,
- Performance level (PL) and category 4 in accordance with ISO 13849-1:2006 or EN ISO 13849-1:2008 [4].

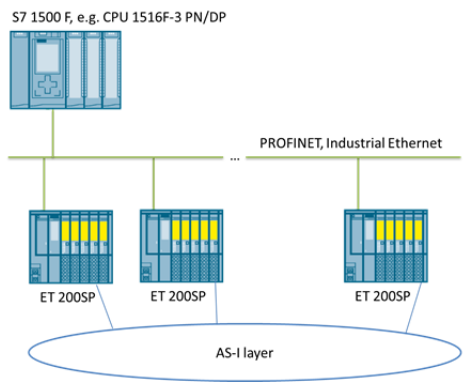

Figure 4: Fail-safe SIMATIC safety system configuration sample.

ISBN 978-3-95450-168-7

Two independent Siemens S7 1500 F-CPU-s (most probably the 1516F-3 PN/DP CPU's) will be used for functional safety implementation, principally through safety functions in the software. Safety functions are executed by the SIMATIC safety system in order to bring the system to a safe state or maintain it in a safe state in case of a dangerous event. They are contained in the following components:

- In the safety-related user program in the F-CPU,
- In the fail-safe inputs and outputs (F-I/O-s).

All sensors and actuators (AS-I, Actuator Sensor Interface) for personnel safety systems will be connected locally to the Siemens ET200SP distributed I/O stations with fail-safe I/O modules. These stations communicate with the F-CPU via PROFINET IO as shown in Figure 4. An example of reading the emergency stop pushbutton status for the two-train system is shown in Figure 5.

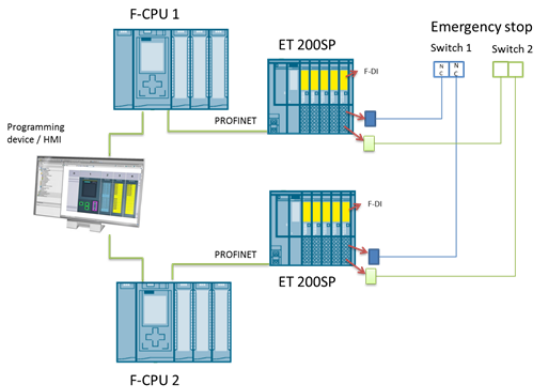

Figure 5: Example of a two-train system with E-stop.

Fail-safe I/O

The F-I/O modules ensure the safe processing of the information received from sensors and sent to actuators (e.g., emergency stop pushbutton, light barriers, contactors for interrupting the power supply, etc.). They have all hardware and software components for safe processing, in accordance with the required Safety Integrity Level:

- F-I/O is accessed via the process image. Direct I/O access is not permitted.
- Communication between the F-CPU and F-I/O for the purpose of updating the process image takes place in the background using a special safety protocol in accordance with PROFIsafe.
- If a safety-relevant parameter for an F-I/O has been changed, the whole safety program must be recompiled.
- The safety function for the process can be provided through a user safety function (from the active safety program downloaded to the CPU) or a fault reaction function (defined in parameterization of the F-I/O module, activated automatically when the safety program is compiled and downloaded to the CPU). In the event of an error, if the safety system can no longer execute its actual user safety function, it executes the fault reaction function; for example, the associated outputs are shut down, and the F-CPU switches to STOP mode, if necessary.

The following fail-safe I/O modules are available for the ET200SP distributed I/O system:

- Fail-safe power modules (F-PM): Used to supply the potential group load voltage and used for the safety-related tripping of the load voltage for standard output modules.
- Fail-safe digital input modules (F-DI): Detect the signal states of safety-related sensors and send the relevant safety frames to the F-CPU.
- Fail-safe digital output modules (F-DO): suitable for safety-related shutdown procedures with short circuit and cross-circuit protection up to the actuator.

Software

The automation software for personnel safety systems will be developed using the last version of Siemens SIMATIC STEP 7 Professional (V13, SP1) with the STEP 7 Safety Advanced V13 SP1 package for programming the safety program. The F-CPU and F-I/O will be configured in the hardware and network editor of the Siemens TIA Portal according to Siemens documentation. Safety checks are automatically performed and additional fail-safe blocks for error detection and error reaction are inserted when the safety program is compiled. This ensures that failures and errors are detected and appropriate actions are triggered to maintain the F-system in the safe state or bring it to a safe state as mentioned before (fault reaction functions).

CONCLUSION

Whilst ESS is in the early days of the personnel safety systems design, substantial progress on the scope, strategy and initial design has been achieved and as the systems designs mature within the next 12 months a true picture of each system requirement will become stronger.

REFERENCES

[1] IEC61508-2010 Functional safety of Electrical/electronic/programmable electronic safety related systems.
[2] SSM2014-127-1 Review of application for licence for activity involving ionizing radiation chapter 10.
[3] SSMFS 2008-27 The Swedish Radiation Authority's regulations concerning operations at accelerators and with sealed radiation sources.
[4] EN ISO 13849-1:2008