Personnel interlock systems for protection against ionizing radiation produced by FEL beams and high power lasers

Michael Dressel, Brunhilde Racky

Deutsches Elektronen-Synchrotron Notkestr. 85, 22607 Hamburg
May 16, 2017

Abstract

Requirements on the personnel interlock arising from the combination of different sources of ionizing radiation in a single experiment area are considered. As an example the HED experiment at XFEL is presented. HED uses a FEL beam and two high power lasers, each capable of producing ionizing radiation by secondary interactions.

1 Risk assessment in brief

Some of the basic steps of a risk assessment according to ISO 12100 [1] in brief are:

- Define the limits of the machine e.g.: geometrical limits, frequency and duration of operation, reaction times, ...
- Identify all hazards and hazardous situations and scenarios.
- Estimate the risk $R = S * P$ of each hazard by estimating the severity (S) of the harm and the probability (P) of the occurrence of the harm related to the hazard.
- Reduce the risk to an acceptable level by means of
  1. inherently safe construction,
  2. technical safety measures,
  3. user information.
- Verify that the risk reduction has been achieved.

If there is an unacceptable risk that has to be reduced, the risk reduction to be done may be expressed as a requirement on a safety function.

Here we only consider hazards due to ionizing radiation.

2 SIL of a safety function

We now assume the risk assessment demands to implement a safety function as a technical safety measure to reduce the risk. In order to achieve the required risk reduction the safety function has to be of a certain minimum quality standard.

This can either be expressed as SIL (Safety Integrity Level) according to IEC 62061 [2] (the standard we use here) or as *performance level* PL according to the EN ISO 13849 [3].

The level required by the risk assessment is named SIL_r. In the end the achieved SIL of the chosen safety function has to be estimated and it has to be at least as good as SIL_r.

The measures to achieve a certain SIL level according to IEC 62061 [2] are basically governed by two domains: systematic safety integrity and hardware safety integrity.

Systematic safety integrity is concerned with quality management and control. Some basic and exemplary topics are:

- A safety plan for the project, defining responsibilities in the fields of specification, design, validation and verification has to be established. The relevant qualification of personnel has to be documented and matched to the tasks the personnel is responsible for.
- Control the quality of components used in the project.
- The system has to be designed failsafe, i.e. in case of loss of energy it it has to obtains a safe state.
- Verify that all parts are used within their specified limits.
- Do verification and validation in a stepwise and iterative way.

Hardware safety integrity is about quantifying the requirements on the probability of dangerous failures. The components used have to ship with information from the manufacturer about the failure rate of the components. The components have to fulfill structural requirements e.g. the hardware failure tolerance (e.g. via redundancy) required by the SIL_r to be achieved. Based on the failure rate and information obtained from the designed use of the component, e.g. frequency of actuation and duration of operation, the so called $PFD_{D,i}$ (Probability of Dangerous Failure on Demand) of every partial system i used in the safety function has to be calculated. Some exemplary quantities to be considered during the calculation of the $PFD_{D,i}$ are:

- SFF: the safe failure fraction. This is the fraction of failures of a component that result in a safe state of the machine.
- CCF: the common cause failure is a quantity that has to be estimated in case the safety function consists of two or more redundant channels. It takes into account that redundant channels may fail simultaneously due to a single cause.

All parts from the sensors via logic and actors of a safety function have to be assigned a $PFD_{D,i}$ value. These values have to be summed up to give the PFD_D of the safety function.

The PFD_D of the safety function together with the requirements of the systematic safety integrity may allow to assign a SIL value to the safety function.

3 HED experiment

In the following we regard the HED experiment of the European XFEL as an example for an area with three sources of ionizing radiation. The three sources of ionizing radiation at the HED experiment [4] can be characterized as:

FEL beam:

- hard x-ray up to 25 keV, energy per pulse: $\approx$ mJ.

Optical lasers: ionizing radiation via secondary interactions

- HE-OL: High-energy optical-laser: 100 J / pulse
- UHI-OL: Ultra-high-intensity optical-laser: 100 TW

Figure 1 displays the outline of the experiments HED and MID following the SASE2 undulator.

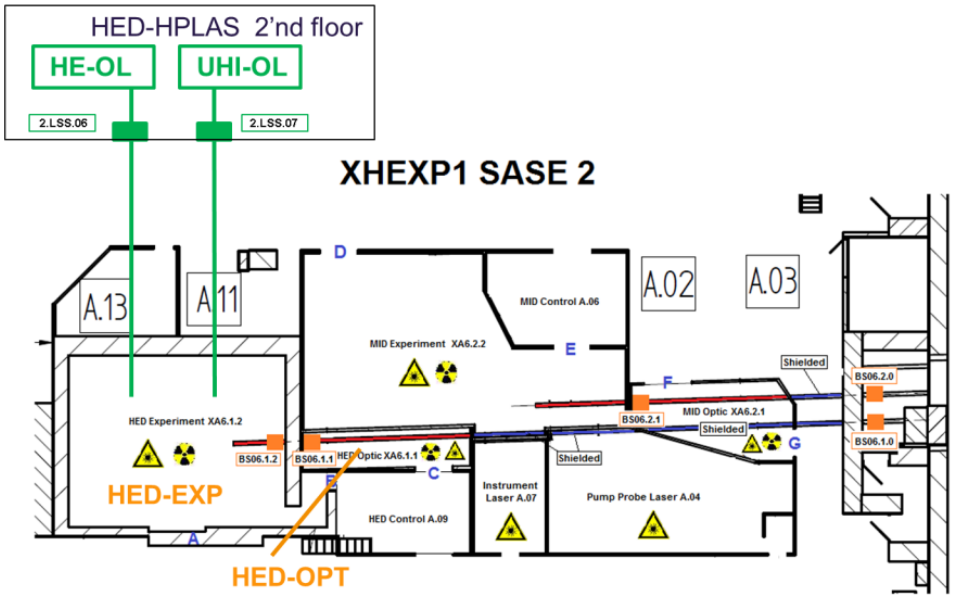

Figure 1: Outline of the SASE2 experiments HED and MID.

The FEL beam is produced by the SASE2 undulator and is distributed to either HED or MID experiments according to the position of a mirror inside the tunnel.

The HED-HPLAS area houses the two lasers HE-OL (high energy optical laser) and UHI-OL (ultra high intensity laser). The HED-HPLAS is build right on top of the HED experiment area. In the drawing it is placed beside the HED experiment for display purposes only. The laser beams from HE-OL and UHI-OL enter the HED experiment through the roof.

HEDs beamline 6.1 is equipped with the front-end absorber and beam shutter 6.1.0 capable to prevent the FEL beam from entering into the HED-OPT optics area. The beam pipe between the front-end beam shutter and the optics area is shielded to prevent ionizing radiation to occur in the areas the beam is only passing through.

The beam shutter 6.1.1 separates the FEL beam from the HED-EXP experiment area. Beam shutter 6.1.2 prevents ionizing radiation produced by the high power lasers to propagate from the experiment area into the optics area.

The laser shutter 2.LSS.06 and 2.LSS.07 are used to prevent the laser beam from HE-OL and UHI-OL to enter into the experiment area.

4 Requirements on FEL beam permission

The safety of the experiment and optics areas is a precondition of the XFEL beam permission. This means that the beam permission for the XFEL may not be given or is removed in case the experiment or optics areas are not safe.

In addition the front-end beam shutter is not allowed to be hit by the FEL beam. Therefore another precondition of the XFEL beam permission is the safety of the front-end beam shutter.

The requirements are:

Safety of experiment and optics areas:

- the beam shutter in front of the area is closed or
  - the beam permission for the area is granted and
  - the following area is safe ...

Safety of front-end beam shutter:

- the absorber is closed
- or the beam shutter is open

Figure 2 shows a logic diagram of the requirements.

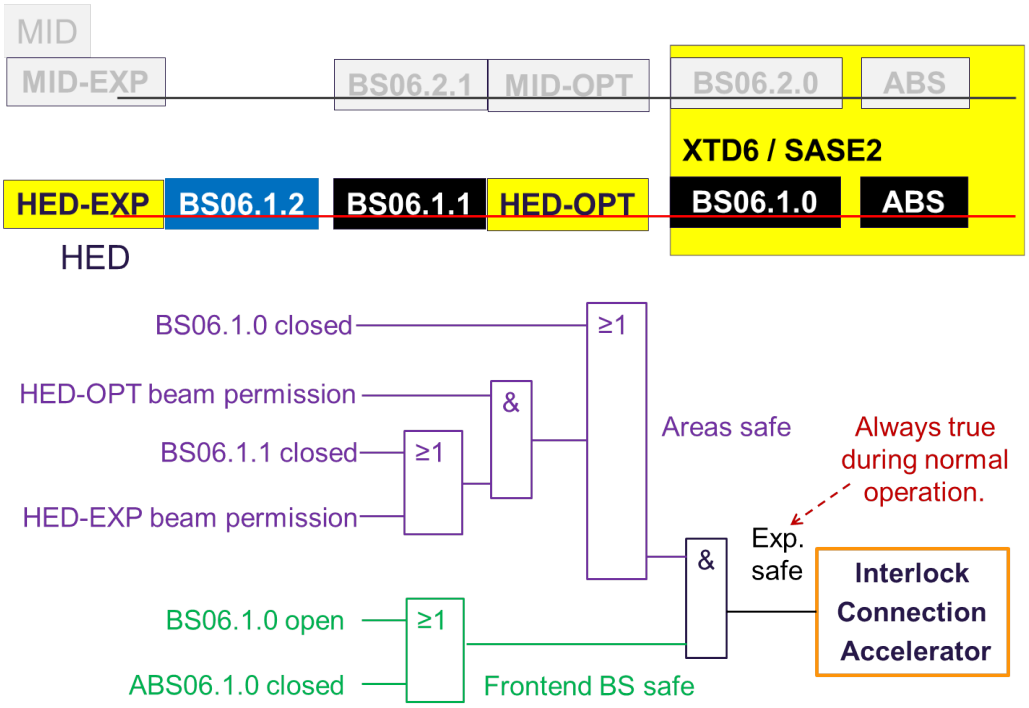

Figure 2: Schematic view of beamline 6.1 and logic diagram of the experiment and optics areas safety.

The output ”Exp. safe” of this logic is feed into the accelerator interlock. It is supposed to be true in all allowed operational modes. The logic displayed is used to specify safety functions that have to be implemented with a certain SIL.

The logic diagram (figure 2) includes only aspects relevant to the safety functions. Other, non safety relevant, aspects of controlling e.g. the steering of the beam shutters are not regarded. These other functionalities are designed to be not of high safety relevance and may be implemented in a reliable but not safety oriented way.

5 Requirements on laser operation in the HED-EXP area

The safety of the experiment and optics areas are preconditions to the permission for the operation of the HE-OL and UHI-OL lasers. Permission to operate the lasers will not be given or will be removed in case an areas are is not safe.

Safety of HED experiment area HED-EXP:

The lasers HE-OL and UHI-OL may only be operated in high power mode if the experiment hutch is safe.

- The appropriate laser shutters to HE-OL / UHI-OL are closed
- Or the HED-EXP is safe:
  - The beam permission for HED-EXP is granted
  - And the optics hutch HED-OPT is safe

Safety of HED optics hutch HED-OPT:

The lasers HE-OL and UHI-OL may only be operated in high power mode If the optics hutch is safe.

- The beam shutter BS06.1.2 is closed
- Or beam permission for HED-OPT is granted

Figure 3 shows a logic diagram of safe laser operation concerning ionizing radiation.

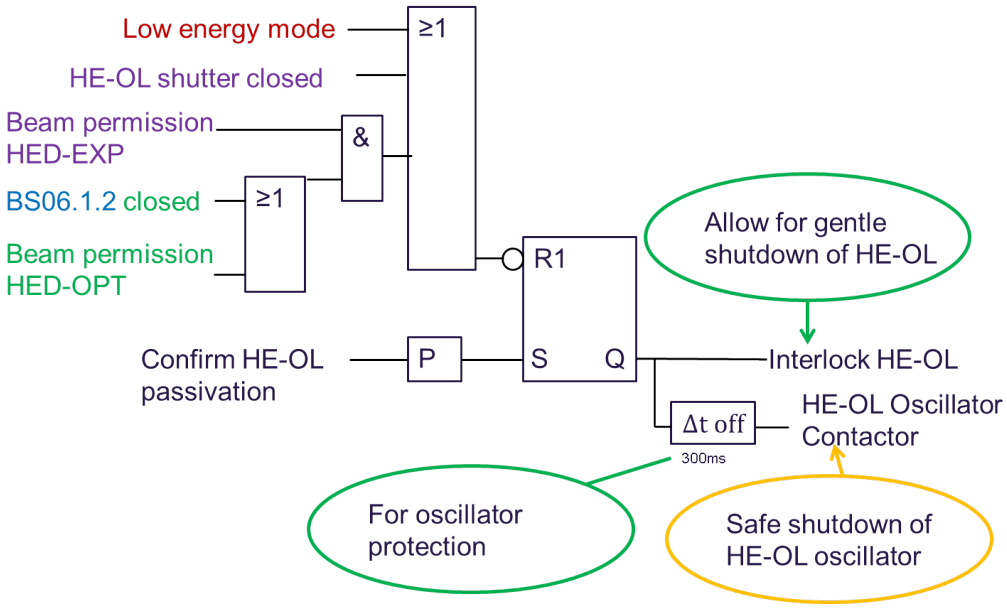

Figure 3: Logic diagram for safe laser operation of HE-OL concerning ionizing radiation.

Safety concerning the operation of the laser as an optical class IV laser is covered by a separate laser interlock system manufactured by a third party company.

The logics safety rated output ”HE-OL Oscillator Contactor” controls a contactor that removes power from the main oscillator in case of an unsafe condition and thereby prevents the laser from operation. The logic

is used to specify safety functions and therefore it includes only aspects relevant for safety functions except for the output ”Interlock HE-OL”. The output ”Interlock HE-OL” is not part of a safety function but merely provided for shutting down the oscillator in a more gentle way before the power is cut by the contactor.

Figure 4 displays the logic used for the UHI-OL laser. It is similar to the logic for the HE-OL laser.

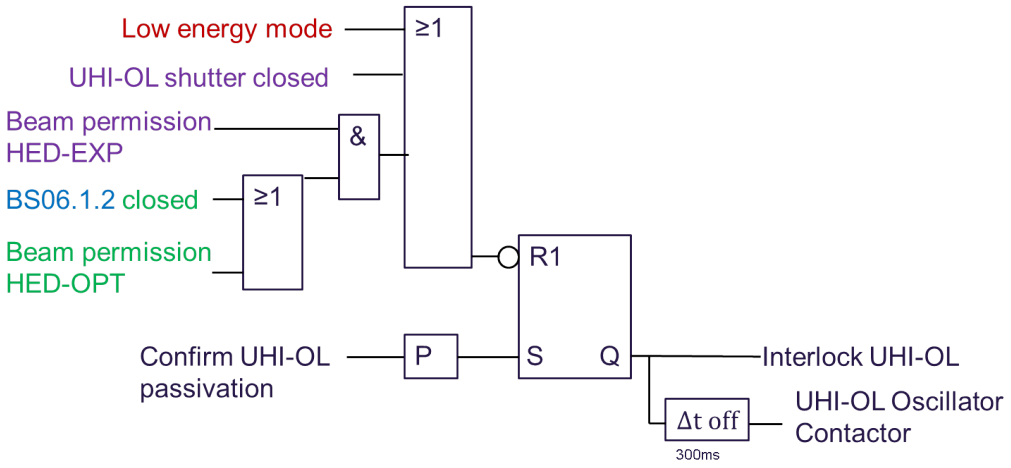

Figure 4: Logic diagram for safe laser operation of UHI-OL concerning ionizing radiation.

6 Dedicated Contactor

For both lasers a dedicated contactor is used connecting the oscillator of each laser to the 230V power line. These contactors are used for the safety oriented switching off of the related lasers. It has been identified as necessary to use a dedicated contactor with certified safety ratings since the lasers do not provide safety rated methods to shut them down.

Figure 5 shows the connection between the safe PLC and the contactor for the oscillator power.

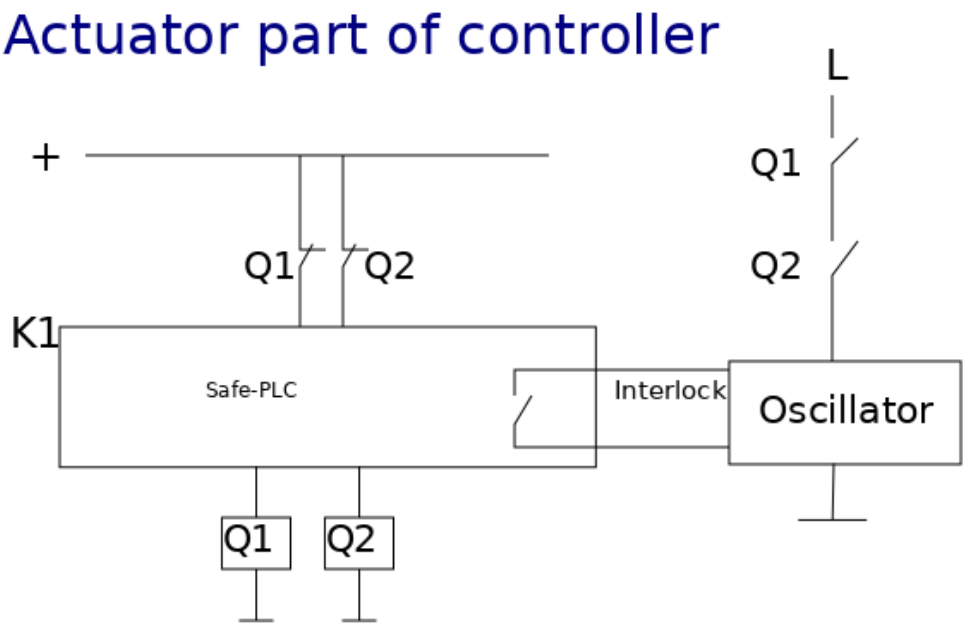

Figure 5: Schematic of a dedicated contactor for safely switching off an optical laser controlled by a safety PLC.

7 Reliability block diagram

The method of reliability block diagrams allows to display in a straight way all the components of a safety function that are able to fail in a way that prevents the safety function from operation. The reliability block diagram must therefore include all components that are potentially able to degrade the safety function. The components are drawn as blocks. Each block can be assigned the dangerous failure rate of the component it represents. No other components should be put in the reliability block diagram.

A safety function typically has some sensors a logic unit and some actors. All blocks belonging to one safety function are connected with a line. In case there is redundancy there will occur parallel lines in the diagram called channels.

A dangerous failure of a component is considered as disconnecting a line at the block representing the failing component.

As long as there is at least one closed connection between a sensor and an actor the safety function is able to perform. But the reliability of the safety function is degraded in case lines are disconnected by a failing component.

Figure 6 shows the mapping of the HE-OL logic diagram into a reliability block diagram.

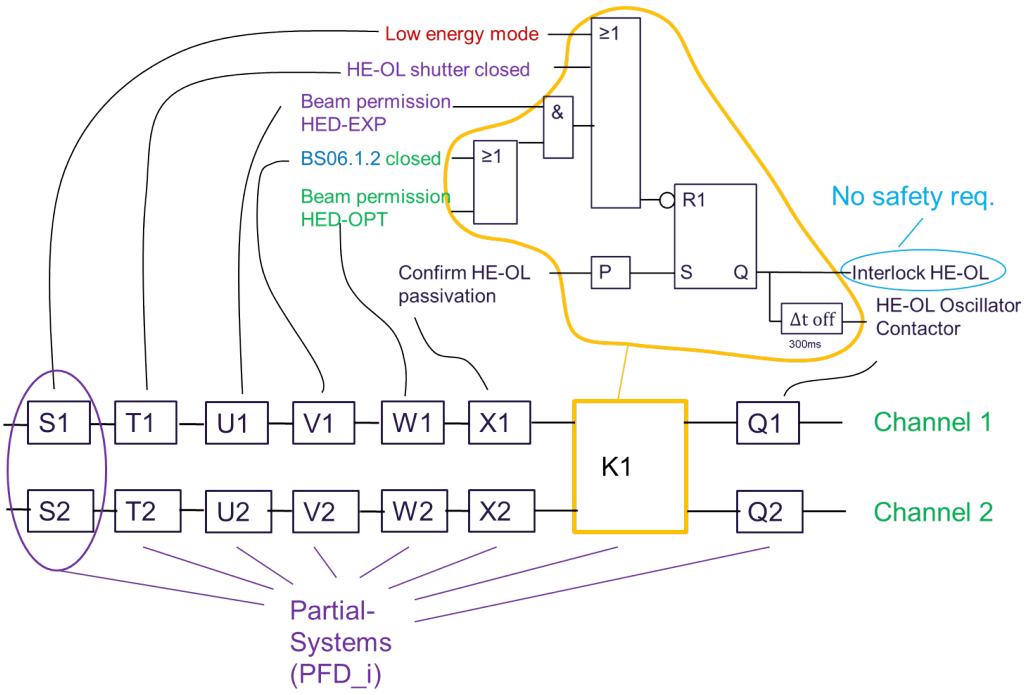

Figure 6: Mapping of safety function components from a functional representation onto a reliability block diagram.

In this case we choose a two channel architecture. The logic unit used is a safety PLC certified to be used for safety functions up to SIL=3 and in two channel architectures.

8 Calculating the achieved SIL

In our case we estimate the $PFD_{D,i}$ values for every partial system e.g. door contacts, beam shutter contacts etc. These partial $PFD_{D,i}$ values are not only determined by the failure rates of the single components but also by the kind of diagnosis done by the logic units they are connected to. The safety PLC used in our case performs several checks e.g. plausibility of the two channels, shorts between channels, isolation etc. and performs failure reactions in case errors are detected.

In our case we have to sum up all partial $PFD_{D,i}$ for every partial system to produce the result PFD_D of the safety function.

$$PFD_D = \sum_{i=S,...,X,K,Q} PFD_{D,i} \leq PFD_r \tag{1}$$

In addition to the partial $PFD_{D,i}$ every partial system used has to fulfill all the additional (e.g. systematic safety integrity, structural limitations, etc.) requirements of the SIL_r to be achieved by the safety function.

$$SIL_i \geq SIL_r \mid i \in S, ..., X, K, Q \tag{2}$$

This means obviously, the SIL of the safety function is limited to the SIL_i of the partial system with the lowest SIL_i.

9 Summary

We briefly reviewed some aspects of risk assessment and the design of safety functions. As an example for requirements on safety functions the three sources of ionizing radiation present at the European XFELs HED experiment were shown. The need to use dedicated contactors to switch off the power of components of the optical lasers in order to comply with the safety requirements was presented.

References

[1] *EN ISO 12100, Safety of machinery - General principles for design - Risk assessment and risk reduction*

[2] *IEC/EN 62061, Safety of machinery: Functional safety of electrical, electronic and programmable electronic control systems*

[3] *ISO 13849, Safety of machinery - Safety-related parts of control systems*

[4] *Technical Design Report*
Interlock Concept for Experimental Area SASE 2 in XHEXP1
E. Boyd and S. Kozielski
August 2015
for Safety and Radiation Protection (SRP)
at the European XFEL