

Hints and Tips on Determination of the Safety Integrity Levels

Arto Meskanen
KEMIRA
Helsinki Finland

IEC 61508 Phases 3, 4, 5 & 9

Key Words Hazop, Hazan, SIL, P&ID, Risk

A) Procedure in case of risks to persons

1. Build a team for carrying out the risk evaluations
 - Process specialist
 - Operations specialist (e.g. shift supervisor)
 - Instrument specialist
 - Risk analysing specialist (person qualified for carrying out Hazop / Hazan analyses)
2. Define the scope using flow and P&I diagrams
3. Select the sub processes by marking them on the P&I diagrams
4. List all risks found in the sub process under examination. This information is normally available from a previous Hazop study.
5. For each risk determine the following parameters:
 - Consequences of the final event, this is parameter C in the risk graph.
 - Probability of the final event to take place without a Safety Integrated System (SIS) in terms of frequency, e.g. once in 3 years.
 - Occupancy of the hazardous area, i.e. average number of persons in the area.
 - Possibility of avoiding the hazardous event in case the SIS fails.
6. For each risk define the possible sequences of events leading to the hazardous event.
7. For each risk:
 - evaluate, whether the risk can be avoided or reduced by using mechanical protection systems or mechanical mitigation systems e.g. relief valves, rupture disks etc. If so, modify the P&I diagram accordingly and re-evaluate the risk graph parameters.

- determine the safety function necessary for eliminating the remaining risk or mitigating the consequences to an acceptable level.
- determine the required Safety Integrity Level (SIL) for the safety function using either the qualitative or semiquantitative risk graph.
- Design the safety loop taking into account the requirements of the standard IEC-61511 concerning the redundancy and device selection.
- Estimate the PFDavg (Probability of Failure on Demand) of the safety loop using Tables B.2 to B.5 of the standard IEC 61508-6 or by calculations based on the reliability data of the devices in the loop.
- Compare the resulting PFDavg with the required upper limit value for the SIL. If the PFDavg is higher than the upper limit, redesign the loop.

The last three steps are normally done under the realisation stage of the project.

B) Procedure, when the risk is economic loss

Steps 1 to 4 as in case A.

5. For each risk determine the following parameters

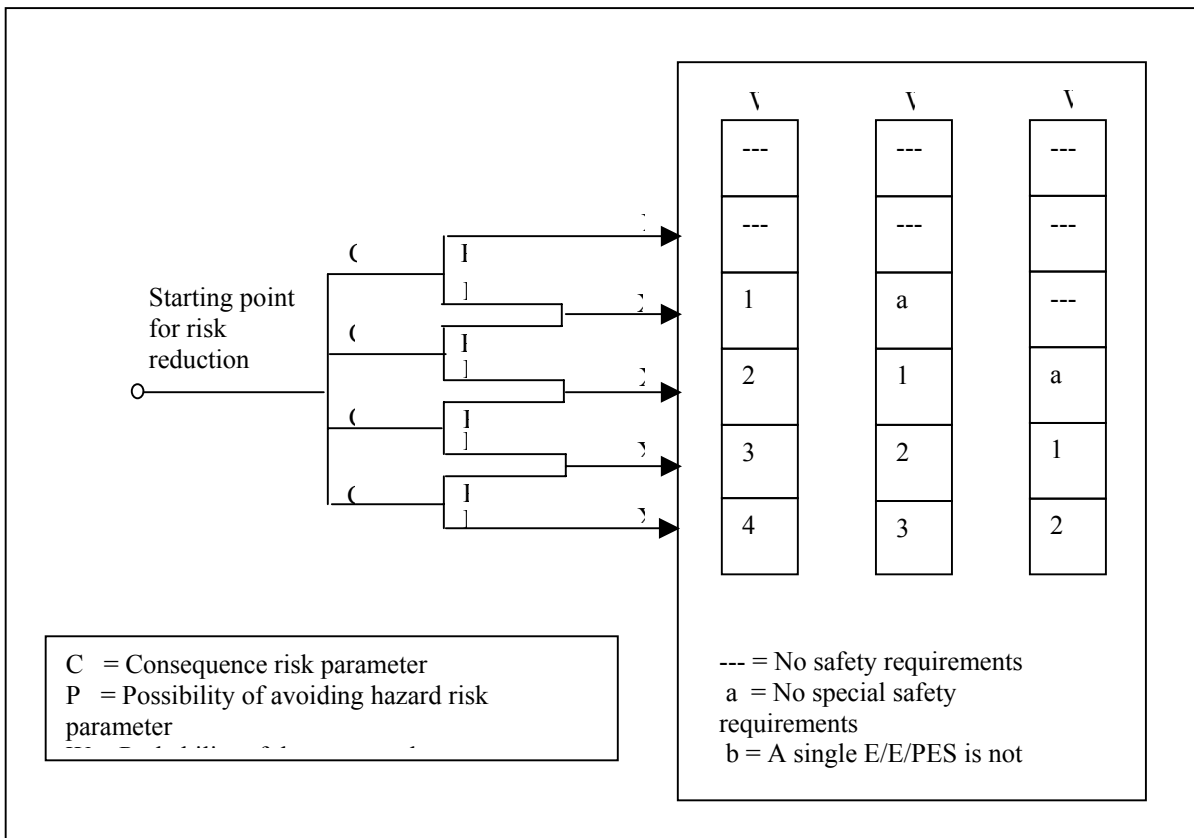
- Consequences of the final event in terms of money (costs of repair and lost production)
- Probability of the final event to take place without a Safety Integrated System (SIS) in terms of frequency, e.g. once in 3 years.
- Possibility of avoiding the hazardous event in case the SIS fails.

6. As in case A)

7. As in case A), but

- use the risk graph (see below) for economical losses instead of the qualitative / semi-qualitative risk graph.

RISK GRAPH FOR ECONOMIC LOSSES



Risk parameters:

Consequence, parameter C

C	Total loss (Cost of repair + production loss)
C _A	Between 20 k€ and 200 k€
C _B	Between 200 k€ and 2.0 M€
C _C	Between 2.0 M€ and 20 M€
C _D	More than 20 M€

Parameter P

P	Conditions for selection of P parameter
P _A	P _A is selected, if facilities exist for alerting the operator, when the SIS fails and independent means are provided to shut down. The time between the alarm and the possible hazardous event is sufficient for the necessary actions.
P _B	P _B is selected, if all above conditions are not satisfied.

Demand rate W

W	Demand rate
W ₁	Less often than once in 33 years
W ₂	Between once in 33 years and once in 3.3 years
W ₃	Between once in 3.3 years and 3 times a year