

## Session Eleven:

# **There's Nothing SILly about Machine Safety – Hardware Safety Integrity for SRECS according to BS EN 62061**

**Stewart Robinson**

Safety Systems Specialist: Pilz Automation Technology UK

---

This presentation will discuss some of the requirements of BS EN 62061 “Safety of machinery. Functional safety of safety-related electrical, electronic and programmable electronic control systems”. The topics will include the integrity required, and achieved, by the hardware of a Safety Related Electrical Control Systems (SRECS). It is important to note that in this session we are only discussing a small part of the standard, to claim compliance with the standard the complete content should be studied, in particular the parts that deal with the requirements for systematic integrity that need to be addressed at the various parts of the safety lifecycle.

The standard is a “functional” safety standard, this means that where the reduction of risks related to a particular hazard is allocated to a SRECS then the risk reduction becomes a “Safety Related Control Function” (SRCF). The SRCF must be specified both in terms of the function that it performs and how well the function needs to perform. Clause 5.2.1.3 of the standard states:

Specifications of each SRCF shall comprise:

- Functional requirements specification;
- Safety integrity requirements specification.

The functional requirements should include a concise description of the actions to be performed (for example “bring hazardous movement to a stop and prevent unexpected start-up”). And where appropriate details like the operating mode of the machine when the function is active; the frequency of operation; the required response time etc. (see clause 5.2.3.1).

## Determination of the safety integrity required for a Safety Related Control Function (SRCF)

Clause 5.2.4.1 of the standard:

“The safety integrity requirements for each SRCF shall be derived from the risk assessment to ensure the necessary risk reduction can be achieved. In this standard, a safety integrity requirement is expressed as a target failure value for the probability of dangerous failure per hour of each SRCF”.

Clause 5.2.4.2:

“The safety integrity requirements for each SRCF shall be specified in terms of a SIL in accordance with Table 3 and documented. An example of a methodology is given in Annex A”

The risk assessment methodology given in Annex A of the standard is a semi-quantified (hybrid) example that is taken from EN ISO 14121-2 “Safety of machinery - Risk assessment -- Part 2: Practical guidance and examples of methods”

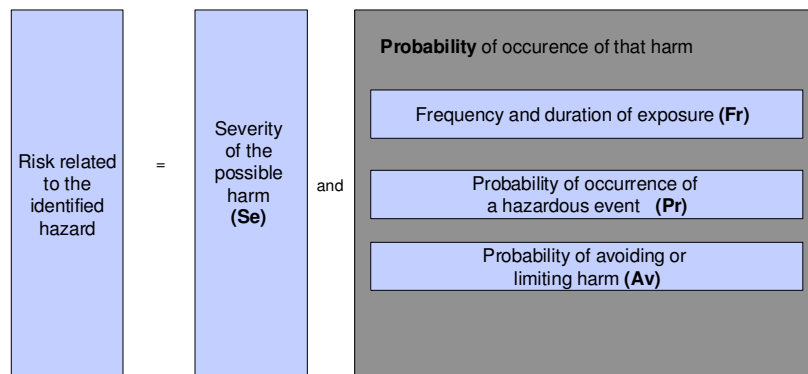


Figure 1 – Parameters used in Risk Assessment

The individual parameters are calibrated to make them appropriate for machinery based hazards and reflect the performance of conventional machinery controls.

### Severity of Harm (Se)

Irreversible injury	4 points
Death, loss of eye or arm	
Irreversible injury	3 points

Broken limb, loss of a finger

Reversible injury 2 points

Requires further medical attention from doctor

Reversible injury 1 point

Requires first aid on-site

**Frequency and exposure time (Fr)**

Frequency (duration > 10 min)

≥ 1h 5 points

< 1h to ≥ 1 day 5 \* points

< 1 day to ≥ 2 weeks 4 \* points

< 2 weeks to ≥ 1 year 3 \* points

< 1 year 2 \* points

\* If the duration is less than 10 min, this may be reduced by one level

**Probability of occurrence (Pr)**

This parameter, and the following parameter (Av) require more careful consideration and the standard contains some detailed explanations about the various choices.

Common	5 points
Likely	4 points
Possible	3 points
Rarely	2 points
Negligible	1 point

**Possibility of avoiding or limiting harm (Av)**

Impossible	5 points
Rarely	3 points
Probable	1 point

The sum of the Fr, Pr and Av parameters determines the class of probability of harm (Cl) this value is mapped against the severity score to give a target Safety Integrity Level (SIL).

Severity (Se)	Class (Cl)				
	4	5-7	8-10	11-13	14-15
4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
3		(OM)	SIL 1	SIL 2	SIL 3
2			(OM)	SIL 1	SIL 2
1				(OM)	SIL 1

Figure 2 - SIL assignment matrix

## Safety Integrity Level - SIL

One of the most important concepts is that of a Safety Integrity Level (SIL), in 62061 safety related control functions need to be defined by the functional performance required and by the SIL as the probability of dangerous failures per hour ( $PFH_D$ )

Safety Integrity Level	Probability of a dangerous failure per hour ( $PFH_D$ )
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

Figure 3 - Probability of dangerous failure per hour - SIL

## Component performance data

In order to be able to calculate the SIL achieved in a SRCF it is essential to have reliable performance data for the components that are used. This data needs to be in the form of the failure rate ( $\lambda$ ) expressed as probability of failures per hour. If the components used are certified safety devices it is quite likely that the manufacturer or supplier will publish the performance data required, however sometimes the failure rate needs to be calculated or derived from other reliable performance data (e.g. the mechanical or electrical life of a component). In addition to the failure rate it is also necessary to establish such things as the Diagnostic Coverage (DC) in a subsystem and the Common Cause Factor ( $\beta$ ) in multi-channel subsystems, more on these topics later.

## Hardware architectures according to “subsystems” descriptions

BS EN 62061 defines a number of basic subsystem architectures to help with the estimation of the probability of random hardware failures, these are subsystems A, B, C, and D. A safety related control function might be comprised of a number of different subsystem architectures in series.

### Subsystem A

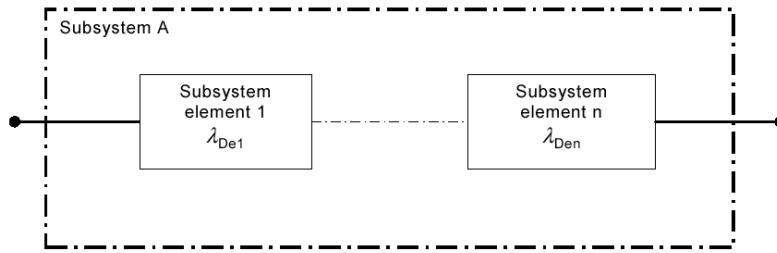


Figure 4 - Subsystem A logical representation

This is a single channel architecture without diagnostics, the sum of the failure rates of the individual elements is the probability of failure of the subsystem.

### Subsystem B

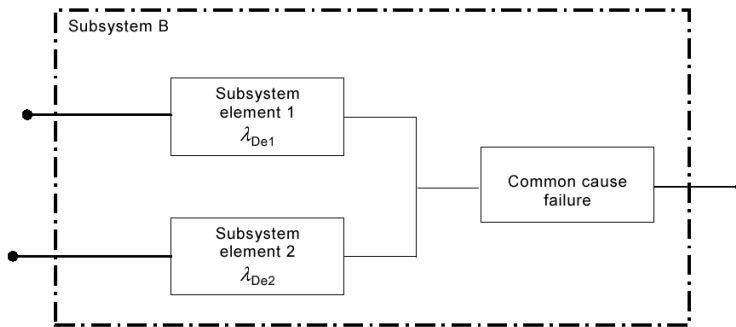


Figure 5 - Subsystem B logical representation

This is a single fault tolerant (redundant) subsystem without a diagnostic function, the probability of dangerous failure of this subsystem is:

$$\lambda_{DssB} = (1 - \beta)^2 \times \lambda_{De1} \times \lambda_{De2} \times T_1 + \beta \times (\lambda_{De1} + \lambda_{De2}) / 2$$

$$PFH_{DssB} = \lambda_{DssB} \times 1h$$

### Subsystem C

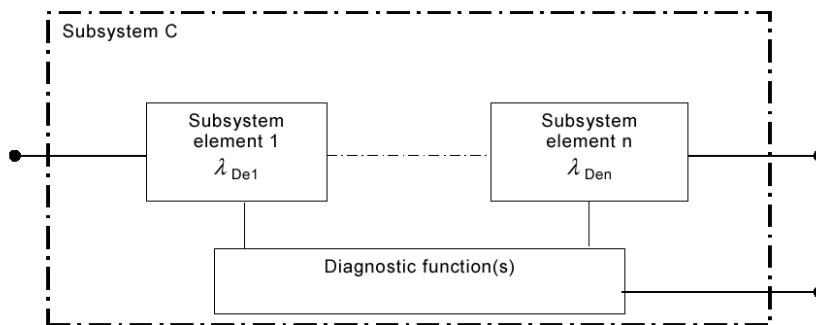


Figure 6 - Subsystem C logical representation

Subsystem C is zero fault tolerant with a diagnostic function, the probability of dangerous failure of this subsystem is:

$$\lambda_{DssC} = \lambda_{De1}(1 - DC_1) + \dots + \lambda_{Den}(1 - DC_n)$$

$$PFH_{DssC} = \lambda_{DssC} \times 1h$$

### Subsystem D

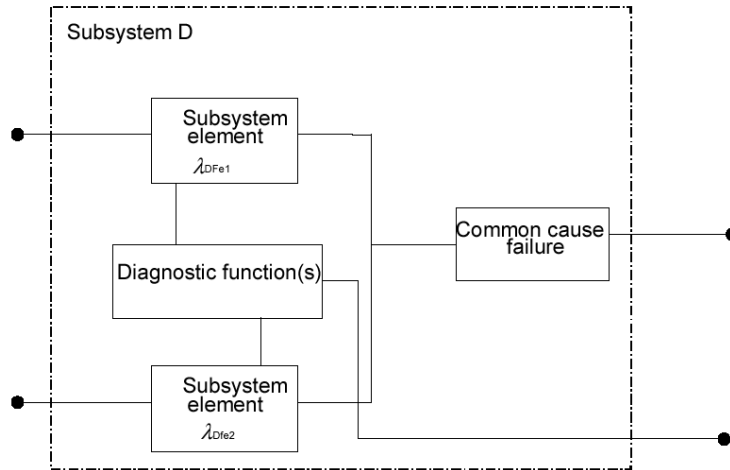


Figure 7 - Subsystem D logical representation

Subsystem D is single fault tolerant with diagnostic functions, the overall probability of dangerous failures of this subsystem is influenced by the design of the subsystem elements, for example if the subsystem elements have the same design the formula is:

$$\lambda_{DssD} = (1 - \beta)^2 \{ [\lambda_{De}^2 \times 2 \times DC] \times \frac{T_2}{2} + [\lambda_{De}^2 \times (1 - DC)] \times T_1 \} + \beta \times \lambda_{De}$$

$$PFH_{DssD} = \lambda_{DssD} \times 1h$$

## Evaluation of the safe failure fraction (SFF) of a subsystem

BS EN 62061 clause 6.7.6 describes the architectural constraints on hardware safety integrity of subsystems.

To calculate this we have to look at the failure rate and failure mode of the components in the safety related control system.

The symbol for failure rate is  $\lambda$  (lambda) which is normally expressed in failures/hour. Failures can be summarised as safe and non-safe (dangerous), and as detected and undetected.

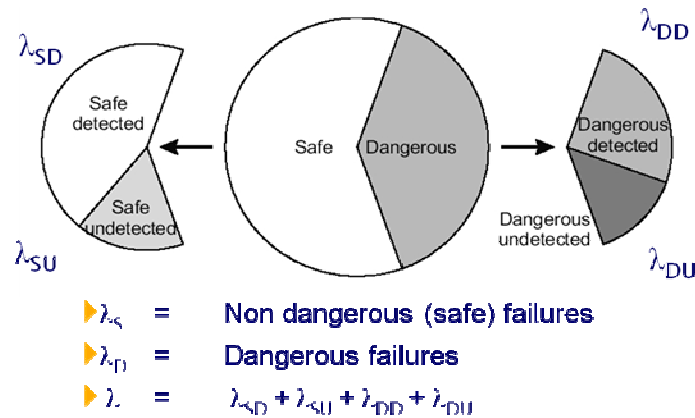


Figure 8 - Sum of all failures

The most critical part of this, from the safety integrity point of view, is how many dangerous undetected failures there might be compared to other failures. This is the Safe Failure Fraction (SFF) and is usually expressed as a percentage. SFF is given by:

$$SFF = \frac{\sum \lambda_{SD} + \sum \lambda_{SU} + \sum \lambda_{DD}}{\sum \lambda_{total}}$$

## Architectural constraints on subsystems that impose SIL Claim Limits (SILCL)

The safe failure fraction of a subsystem in conjunction with the hardware fault tolerance imposes a SIL claim limit (SILCL) for the safety related control function using that subsystem.

Safe Failure Fraction, SFF	Hardware Fault Tolerance		
	0	1	2
< 60%	Not allowed (with some exceptions)	SIL 1	SIL 2
60 % - <90 %	SIL 1	SIL 2	SIL 3
90 % - <99 %	SIL 2	SIL 3	SIL 3
≥99 %	SIL 2	SIL 3	SIL 3

Figure 9 - Architectural constraints on subsystems

## Diagnostic coverage (DC)

The standard requires the user to quantify the amount of diagnostic coverage of the safety related control functions, this is defined as the decrease in probability of dangerous hardware failures resulting from the operation of the automatic diagnostics tests. Once again this can be derived from a ratio of failure rates, in this case it is the relationship between dangerous detected failures and total dangerous failures.

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_{Dtotal}}$$

## Common cause errors in SRECS

It is also necessary to take account of, and evaluate, the effects of common cause failures, (CCF), this is defined as:

Failure which is the result of one or more events and which causes simultaneous failures of two or more separate channels in a multi-channel system, leading to the failure of a safety related control function

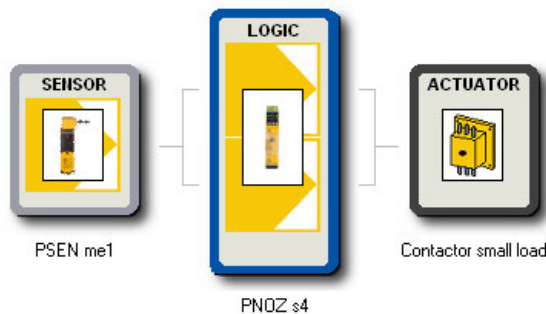
In Annex F of 62061 there is a methodology for the estimation of susceptibility to common cause failures. This uses a table listing typical measures that are used to combat common cause errors, for each measure used a score is given. The total score claimed gives an estimation of the CCF factor ( $\beta$ ) as a percentage of 1%, 2%, 5% or 10%.

## Determination of the safety performance of a Safety Related Control Function by the evaluation of the probability of random hardware failures.

As seen earlier each subsystem has it's own formula for calculating the probability of dangerous failures per hour of that subsystem, however the complete SRCF will be made up of a number of subsystems working together. As a minimum this would usually be at least 3 subsystems, the sensor part, the logic part and the actuator part. This can be represented in a block diagram



In a typical machinery safety function this might be something like a guard switch for the sensor part, a “safety relay” for the logic part, and a contactor for the actuator part.

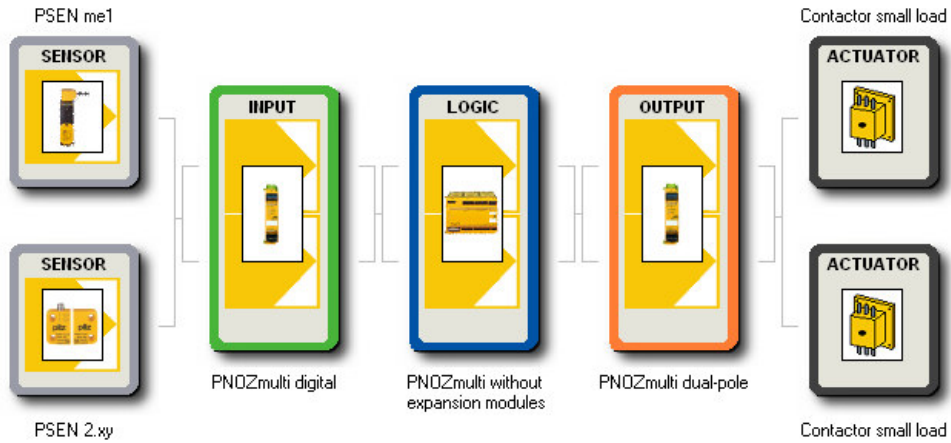


Each part could have a different subsystem architecture, for example a single guard switch could be electrically connected as either subsystem A (single channel), or subsystem D (dual channel with feasibility checking). The logic part is most likely to be subsystem D. The actuator (if it is a single device) could be subsystem A or subsystem C depending on whether or not any diagnostic functions are implemented.

The overall  $PFH_D$  is the sum of the  $PFH_D$ 's of the individual subsystems:

$$PFH_{D_{total}} = PFH_{D_{ss1}} + PFH_{D_{ss2}} + PFH_{D_{ss3}} + \dots + PFH_{D_{ssn}}$$

It is not unusual for the make up of a SRCF to be more complex particularly when the logic part is a programmable electronic system (typically a safety PLC), and when the principle of hardware fault tolerance has been employed throughout the system



Once again each subsystem part needs to be evaluated separately and the overall  $PFH_D$  calculated by the sum of the  $PFH_D$ 's of the individual subsystems.

### Example/Exercise

Estimate the SIL achieved by a SRCF using component manufacturer's data sheets

### References

BS EN 62061:2005 Safety of machinery. Functional safety of safety-related electrical, electronic and programmable electronic control systems

BS EN ISO 14121-1:2007 Safety of machinery. Risk assessment. Principles

ISO/TR 14121-2:2007 Safety of machinery -- Risk assessment -- Part 2: Practical guidance and examples of methods