Session: 14

SIL or PL? What is the difference?

Stewart Robinson MIET MInstMC
Consultant Engineer, Pilz Automation Technology UK Ltd.

EN ISO 13849-1 and EN 62061

Having two different standards for safety related controls that are both harmonised to the Machinery Directive has left many people confused about which standard should be applied in a particular application. This practical and hard hitting presentation will define the key differences in the standards and more importantly, explain the similarities in the general requirements. You will understand how the correct application of either standard will produce the same result.

Evaluation of hardware performance according to the architectures and reliability requirements described in the standards will be compared using a practical safety function as an example. We will conclude with a valuable checklist of how to apply both standards to your next assessment of machinery safety.

Introduction

In this paper we are considering some of the requirements of the standards that deal with hardware selection and verification. It must be remembered that the standards contain much more than we have time to discuss here, in particular we will not be exploring the requirements of the standards to reduce the possibilities of systematic errors that could occur at any point in the safety lifecycle. We will also not discuss the requirements of the standards with respect to safety-related software.

EN ISO 13849-1 (Safety of machinery, Safety related parts of control systems, General principles for design) is a harmonised European standard and the standard that it has replaced, EN 954-1 (Safety of machinery, Safety related parts of control systems, General principles for design), will be completely withdrawn at the end of 2011. EN 62061 (Safety of machinery, functional safety of safety-related electrical, electronic and programmable electronic control systems) is also harmonised to the Machinery Directive. It is a machinery sector standard based on the requirements of IEC 61508.

From a users point of view if you are implementing safety related controls using electrical/electronic/programmable electronic systems there is no clear distinction as to which of the standards should be used for any particular application (EN ISO 13849-1 is not “technology specific” and can be used as guidance for non-electrical technologies). The choice will be influenced by quite a number of factors, however whichever of the standards you choose to follow the main steps, and the outcomes, are pretty much the same.

The choice

In the UK there was a considerable body of opinion that the use of EN ISO 13849-1 should be restricted to low complexity safety systems, and that EN 62061 should be chosen for systems that used “Safety PLCs”, indeed the national foreword to the BS editions of the standards almost said as much. However the choices as far as the standards themselves are concerned is not that clear. Either standard can be used as guidance for both hardware and application software for systems up to the highest integrity or performance identified in them. So how does a user make the decision? As already mentioned if the safety-related controls use technologies other than E/E/PES then EN ISO 13849-1 is the only choice, but for the vast majority of systems several factors will influence the choice.

It is becoming clear that more use is being made of EN ISO 13849-1, this is probably due to it being the replacement for EN 954-1 and carrying over a lot of the familiar content, but it might also be because it is seen as the more straightforward of the two (not necessarily the case!). Some of the considerations that might influence the choice are:

> Previous knowledge and experience in the design of machinery control systems based upon the concept of Categories described in ISO 13849-1:1999 may mean that the use of ISO 13849-1:2006 is more appropriate;
>
> Control systems based upon media other than electrical may mean that the use of ISO 13849-1 is more appropriate;
>
> Customer requirements to demonstrate the safety integrity of a machine control system in terms of a Safety Integrity Level (SIL) may mean that the use of IEC 62061 is more appropriate;
>
> Control systems of machinery used in, for example, the process industries, where other safety-related systems (such as safety instrumented systems in accordance with IEC 61511) are characterised in terms of SILs may mean that the use of IEC 62061 is more appropriate.
>
> (Source ISO/DTR 23849)

Main steps

Machinery safety starts at the very beginning with the design and development of the machine itself. Wherever possible hazards should be eliminated by design, or fixed safeguards should be in place to avoid exposing people to hazards. EN ISO 12100 gives excellent guidance on these vitally important considerations. It is also worth noting that neither EN ISO 13849-1 nor EN 62061 cover the general electrical safety aspects for machinery, this is the subject of EN 60204.

So it is only once it has been decided that further risk reduction is required from safeguards utilising safety related controls that we should consider the guidance given by either EN ISO 13849-1 or EN 62061.

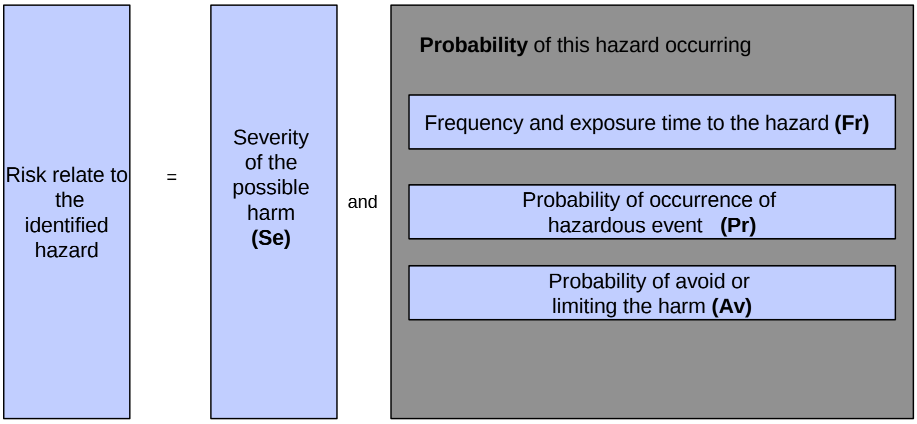
Both standards use the concept of “functional safety” which means specifying the safety requirements in terms of the functional requirements (for example: “When the guard is opened hazardous movement must be stopped”), and the amount of risk reduction required. EN 62061 uses Safety Integrity Levels (SIL), EN ISO 13849-1 uses Performance Levels (PL).

Both standards require the user to follow essentially the same series of steps:

- Assess the Risks
- Allocate the Safety measures
- Design Architecture
- Validate

Both standards have a recommended risk assessment method to help establish the risk reduction that is required from a particular safety function, although the methods are quite different the outcomes should be the same (or very similar) for any given function.

EN 62061 Risk Assessment



EN 62061 has a hybrid (semi-quantified) example that is taken from ISO/TR 14121-2. The severity of possible harm is assessed in one of four levels, the probability of the hazardous event occurring is then assessed by considering 3 further parameters in a range of point scores, these three scores are summed up to give the class (Cl). The class is then plotted against the severity in a simple matrix to establish the SIL target for the function.

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

Severity of Harm (Se)

Irreversible injury	
Death, loss of eye or arm	4 points
Irreversible injury	
Broken limb(s), loss of a finger(s)	3 points
Reversible injury	
Requiring attention from a medical practitioner	2 points
Reversible injury	
Requires first aid on-site	1 point

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 of each exposure is expected to be less than 10 min, this may be reduced by one level.

Probability of occurence (Pr)

This parameter, and the foillowing 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

Possibilty 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 (Cl) this value is mapped against the severity score to give a target Safety Integrity Level (SIL).

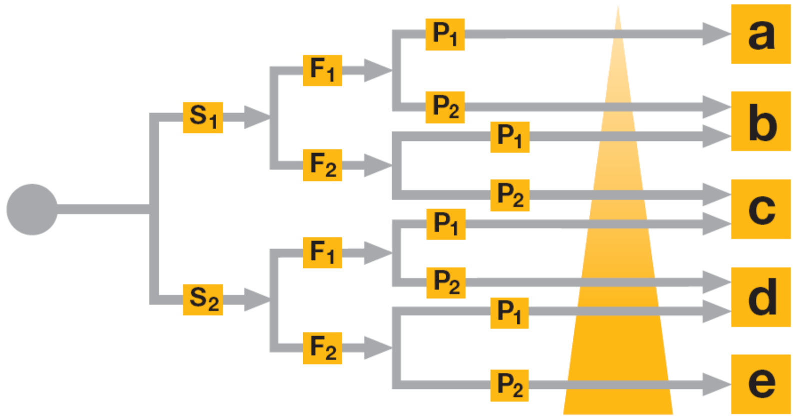
Consequences	Severity	Class Cl				
		4	5-7	8-10	11-13	14-15
Death, losing an eye or arm	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
Permanent, losing fingers	3		(OM)	SIL 1	SIL 2	SIL 3
Reversible, medical attn.	2			(OM)	SIL 1	SIL 2
Reversible, first aid	1				(OM)	SIL 1

Safety Integrity Levels are defined as the average probability of a dangerous failure per hour.

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

EN ISO 13849-1 Risk Assessment

The risk assessment methodology given in EN ISO 13849-1 is in the form of a qualitative risk graph which is an enhanced version of the well known risk graph that was in EN 954-1



The use of this kind of risk assessment tool is well understood even though the process can be subjective and open to wide differences in interpretation. The guidance given in the standard to help with the correct choice of parameters is intended to overcome these shortcomings, the parameters are briefly described as follows.

Severity of injury:

S_1 = Slight (normally reversible injury)
S_2 = Serious (normally irreversible injury or death)

Frequency and/or exposure time to the hazard

F_1 = Seldom to less often and/or the exposure time is short
F_2 = Frequent to continuous and/or the exposure time is long

Possibility of avoiding the hazard or limiting the harm

P_1 = Possible under specific conditions
P_2 = Scarcely possible

Performance level required PL_r

The output of the risk graph indicates a required performance level of a – e, clearly the greater the risk of exposure to a hazard, the higher the performance of the safety related control needs to be.

Performance levels in EN ISO 13849-1 are also defined in terms of the average probability of a dangerous failure per hour.

Performance level (PL)	Average probability of a dangerous failure per hour 1/h
a	$\geq 10^{-5}$ to $< 10^{-4}$
b	$\geq 3 \times 10^{-6}$ to $< 10^{-5}$
c	$\geq 10^{-6}$ to $< 3 \times 10^{-6}$
d	$\geq 10^{-7}$ to $< 10^{-6}$
e	$\geq 10^{-8}$ to $< 10^{-7}$
NOTE Beside the average probability of dangerous failure per hour also other measures are necessary to achieve the PL.	

EN ISO 13849-1: Table 3, clause 4.2.2

Performance level and SIL

There is clearly a correspondence between the SIL required according to EN 62061 and the PL required according to EN ISO 13849-1

EN ISO 13849-1 Performance Level (PL)	Average probability of a dangerous failure per hour [1/h]	EN 62061 Safety Integrity Level (SIL)
a	$\geq 10^{-5}$ to $< 10^{-4}$	no special safety requirements
b	$\geq 3 \times 10^{-6}$ to $< 10^{-5}$	1
c	$\geq 10^{-6}$ to $< 3 \times 10^{-6}$	1
d	$\geq 10^{-7}$ to $< 10^{-6}$	2
e	$\geq 10^{-8}$ to $< 10^{-7}$	3

SIL 3 is directly equivalent to PLe, SIL 2 is directly equivalent to PLd, SIL 1 is equivalent to PLb – PLc

Verification according to hardware reliability

In order to verify that a target SIL or PL has been achieved we need to consider a number of things, these include the hardware architectures of the safety related controls (e.g. single channel or dual channel), the reliability of the components used, the amount of Diagnostic Coverage (DC), and the susceptibility to Common Cause Failures (CCF). These are considered to be the quantifiable aspects.

The terms used are defined as:

T_1 = Proof test interval or lifetime

T_2 = Diagnostic test interval

MTTF = Mean time to failure

$MTTF_d$ = Mean time to dangerous failure

DC = Diagnostic coverage

β = Common cause failure fraction

β_D = Detected common cause failures

λ = Failure rate (per hour)

λ_D = Dangerous failure rate

λ_{DD} = Detected dangerous failure rate

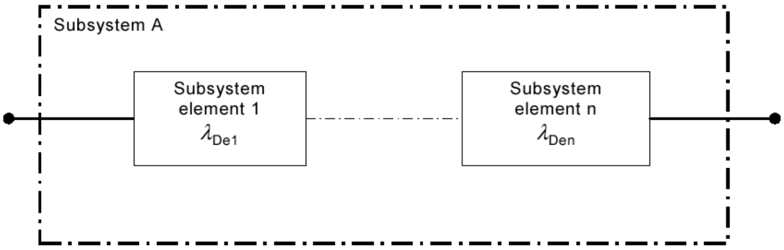
λ_{DU} = Undetected dangerous failure rate

Hardware architectures - EN 62061 Subsystems

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 achieved by a number of different subsystem architectures in a series alignment.

Subsystem A

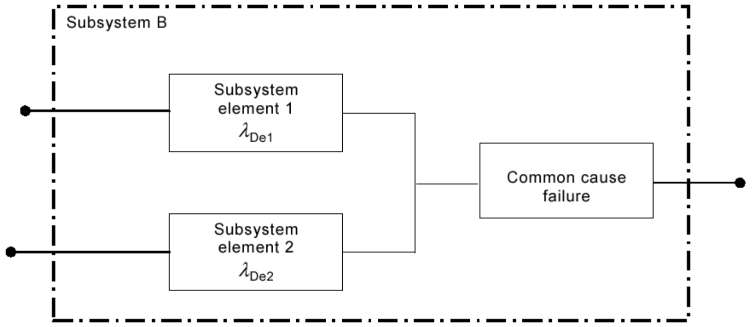


This is a single channel architecture without diagnostics, the sum of the failure rates of the individual elements is the probability of failure of the subsystem.

$$\lambda_{DssA} = \lambda_{De1} + ... + \lambda_{Den}$$

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

Subsystem B

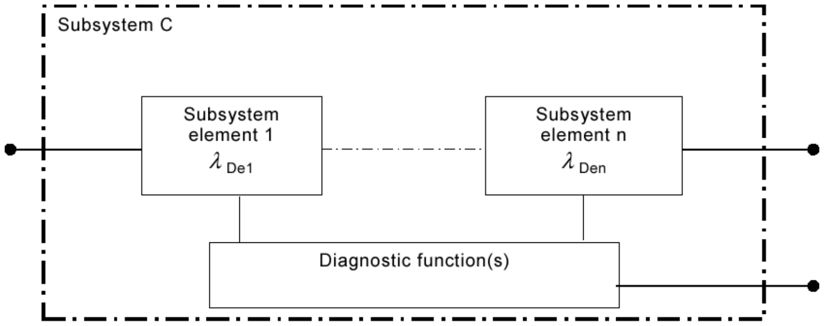


This is a single fault tolerant (redundant) subsystem without a diagnostic function, the probability of dangerous failure of this subsystem can be calculated from the formula:

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

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

Subsystem C

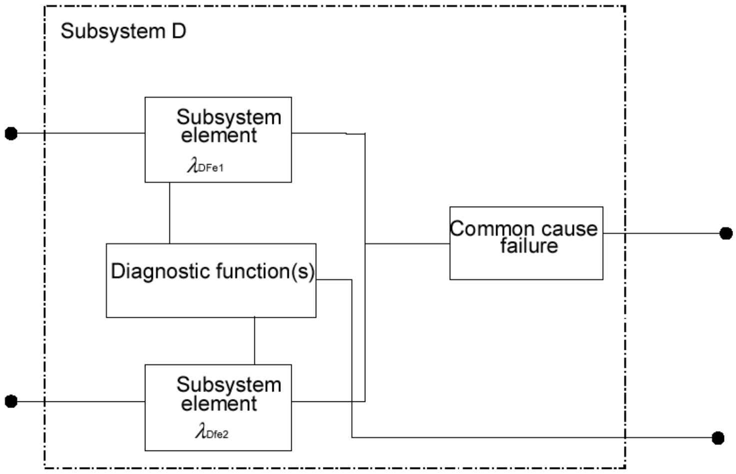


Subsystem C is zero fault tolerant with a diagnostic function, the probability of dangerous failure of this subsystem is:

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

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

Subsystem D



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:

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

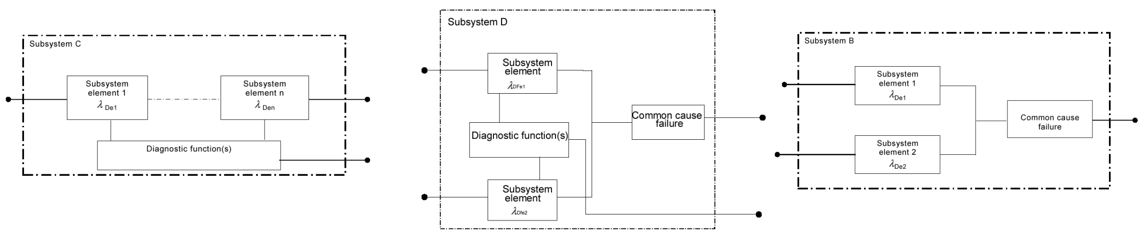
There is also a formula given for subsystem D architectures that have elements with different failure rates:

$$\lambda_{DssD} = (1-\beta)^2\{[\lambda_{De1} \times \lambda_{De2} \times (DC_1 + DC_2)] \times {T_2}/{2} + [\lambda_{De1} \times \lambda_{De2} \times (2 - DC_1 - DC_2)] \times {T_1}/{2}\} + \beta \times (\lambda_{De1} + \lambda_{De2})/2$$

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

Series alignment

It is quite possible that a safety function might be realised by the use of a series alignment of subsystems that have different architectures



Sensor Logic Actuator

For example it is possible that a type C sensor subsystem might be connected to a logic solver that is type D with an actuator subsystem of type B. In this case the individual subsystems would have their PFH_D values calculated using the appropriate formula, the values would then be summed to give the overall PFH_D which would give the SIL achieved by the function (subject to architectural constraints).

Safe failure fraction (SFF)

EN 62061 clause 6.7.6 describes the architectural constraints on hardware safety integrity of subsystems. The highest SIL that can be claimed for a Safety Related Control Function (SRCF) is limited by the hardware fault tolerance and the safe failure fractions of the subsystems that carry out the SRCF.

To calculate the SFF we consider the failure rates and failure modes of the components in the safety related control system.

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

- λ_S = Safe failures
- λ_D = Dangerous failures
- λ = $\lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU}$

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 can be expressed by the formula:

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

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

Safe failure fraction, SFF	**Hardware Fault Tolerance**		
	0	**1**	**2**
< 60%	Not permitted	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

SIL Claim limits (part of EN 62061 table 5)

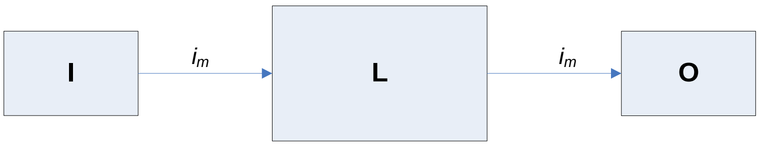
Hardware architectures - EN ISO 13849-1 categories

In 13849 the “designated” architectures of the Safety Related Parts of Control Systems (SRP/CS) correspond to the requirements of the “categories” that are well known from EN 954-1, but there is the inclusion in the standard of reliability block diagrams to provide further explanation. These block diagrams summarise an SRP/CS as comprising of input(s), logic and output(s).

It is quite possible that a safety function might be realised by the use of a series alignment of subsystems that have different architectures

Category B & 1

These are single channel subsystems without diagnostics.



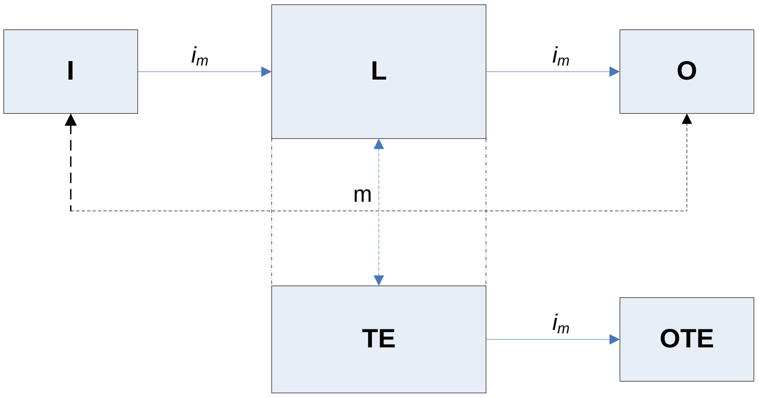
Category B:

Safety-related parts of control systems and/or their protective equipment, as well as their components, shall be designed, constructed, selected, assembled and combined in accordance with relevant standards so that they can withstand the expected influence.

Category 1:

Additionaly for category 1 Well-tried components and well-tried safety principles shall be used.

Category 2

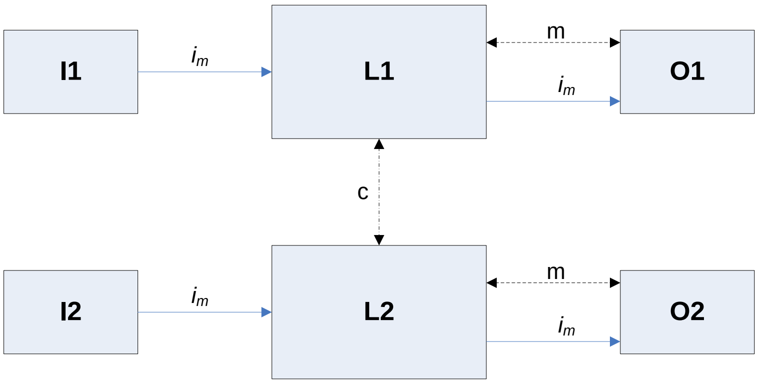


Requirements of B and the use of well-tried safety principles shall apply. Safety functions shall be checked at suitable intervals by the machine control system.

The required test frequency is not clearly specified in the standard, however part of clause 4.5.4 has this assumption:

“for category 2, demand rate ≤ 1/100 test rate”

Category 3 and 4



These are redundant (fault tolerant) architectures with diagnostics.

Category 3

Requirements of B and the use of well-tried safety principles shall apply. Safety-related parts shall be designed so that:

-a single fault in any of these parts does not lead to the loss of the safety function, and

-whenever reasonably practicable the single fault is detected.

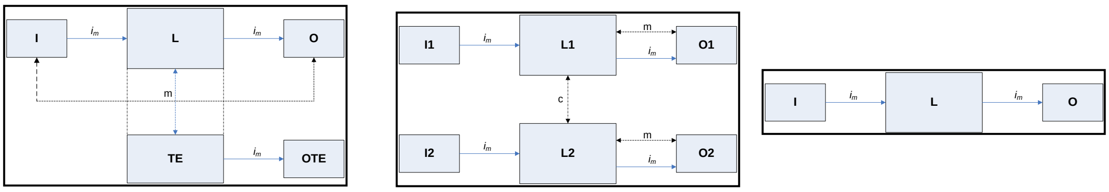
Category 4

In addition to the above

-the single fault is detected at or before the next demand upon the safety function; or an accumulation of faults shall not lead to the loss of the safety function.

Series alignment

It is quite possible that a safety function might be realised by the use of a series alignment of subsystems that have different architectures



Sensor Logic Actuator

For example it is possible that a category 2 sensor subsystem might be connected to a logic solver that is category 3 with an actuator subsystem of category 1. In this case the individual subsystems could have their PFH_D values estimated using the appropriate methods, the values would then be summed to give the overall PFH_D which would give the PL achieved by the function. There may also be other limiting factors to consider.

Verification of PL

EN ISO 13849-1 describes a method of determining the PL achieved by a combination of SRP/CS by estimating:

- the reliability of components as the Mean Time To dangerous Failure ($MTTF_d$)
- the Diagnostic Coverage (DC)
- the Common Cause Factors (CCF)
- the structure (Category)

Mean time to dangerous failure ($MTTF_d$)

The $MTTF_d$ for each channel must be calculated or estimated as part of the verification that a required performance level has been met. The standard summarises $MTTF_d$ into 3 levels, low, medium and high, with a maximum value for a channel of 100 years (the $MTTF_d$ of individual components may be much higher than 100 years).

$MTTF_d$	
Denotation of each channel	**Range of each channel**
Low	3 years ≤ $MTTF_d$ < 10 years
Medium	10 years ≤ $MTTF_d$ < 30 years
High	30 years ≤ $MTTF_d$ ≤ 100 years

Annexes C and D of the standard detail various methods of calculating or estimating the $MTTF_d$.

Diagnostic coverage (DC)

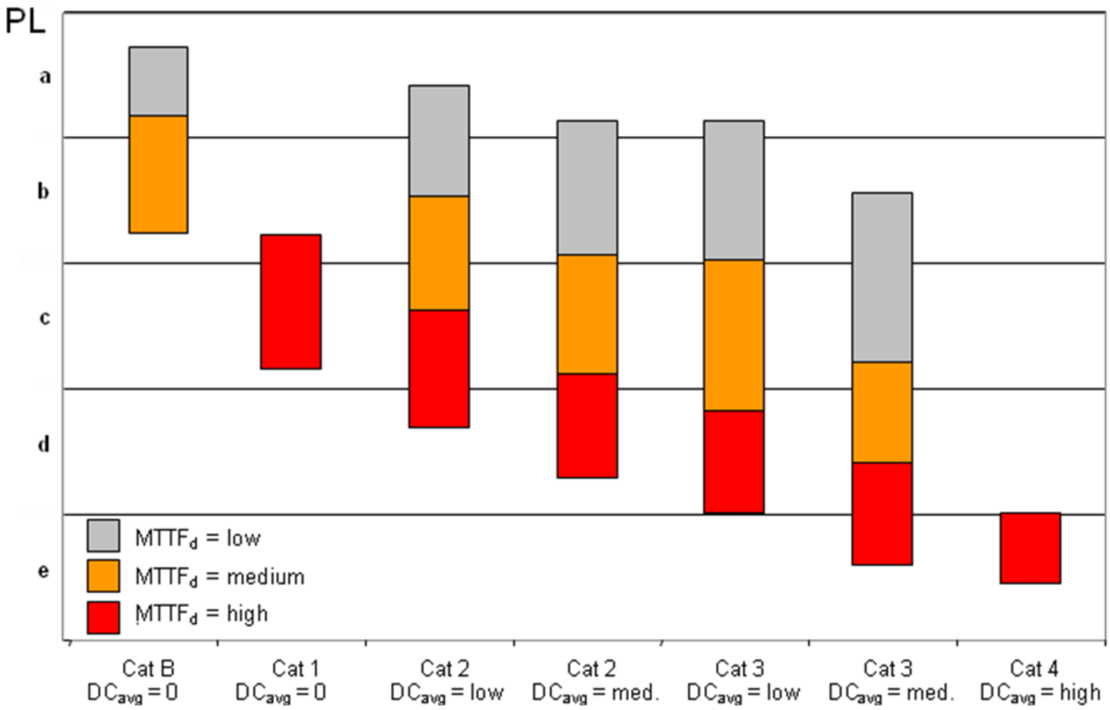
Both standards require the user to quantify the amount of diagnostic coverage of the safety related control functions, this is defined as the decrease in probability of dangerous hardware failures resulting from the operation of the automatic diagnostics tests. Once again this can be defined by a ratio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

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

Annex E of EN ISO 13849-1 has tables listing the most common measures for providing diagnostic coverage for input devices, logic devices, and output devices. It also has a relatively simple formula for the estimation of the average DC of a channel in a safety related control system.

Verifying achieved performance level

To verify that a required performance level has been achieved it is necessary to compare the architecture and the diagnostic coverage with the $MTTF_d$ of each channel. Figure 5 of the standard illustrates this relationship:



Annex K of the standard is a numerical representation of figure 5 and this gives the PFH_D values that correspond to the $MTTF_d$ values for the appropriate category and DC.

Common cause failures (CCF)

Both standards require the user to take account of, and evaluate, the effects of common cause failures, CCF 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."

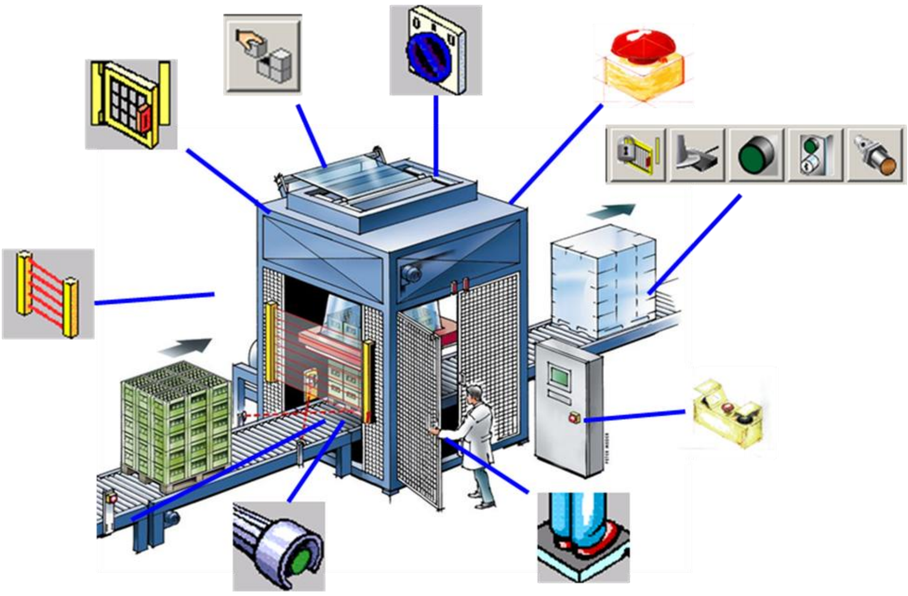
The standards contain similar tables to help the user quantify the amount of CCF that needs to be taken into account, in 13849 it is simply a matter of reaching or exceeding a threshold value. In Annex F of 62061 there is a table to help with the estimation of susceptibility to common cause failures. The output of this methodology gives an estimation of the CCF factor (β) as a percentage of 1%, 2%, 5% or 10%.

Machinery safety related control functions

With increasing complexity of machinery and more automation, and with heightened awareness of safety requirements, there can be fairly complex safety related control requirements even on relatively small machines.

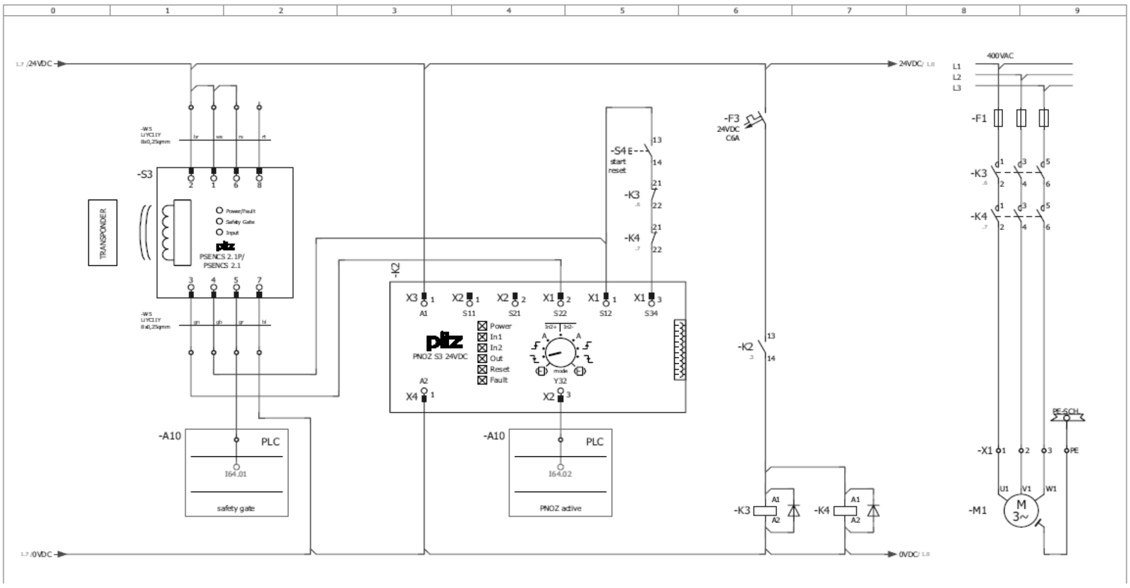
For example consider a wrapping machine that is integrated into a production line. The most significant hazard would probably be coming into contact with the moving parts of the wrapper itself. But there would be quite a number of access points that would need to be protected in a variety of ways, for example:

> There would probably be access doors/gates to allow maintenance and film changing etc. These would need to be interlocked.
>
> The infeed and outfeed conveyors would need to be protected to allow product in and out but detect if there was any other kind of access.
>
> It may be required to run part of the equipment whilst people are exposed to hazards (e.g. threading up whilst changing rolls), this might require safety speed monitoring in conjunction with some kind of “hold to run” enable device, or 2-hand control.
>
> Etc. etc.

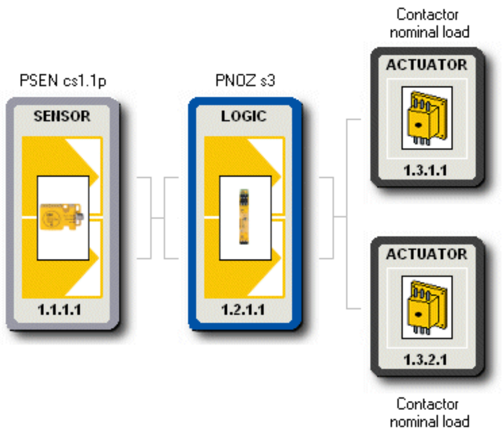


Circuit diagrams

Depending on the type of system chosen the actual circuit wiring for the safety related controls will differ quite considerably, for example if hard wired relays are used the wiring could be quite complex and take up a number of pages of drawings even for quite small machines, if PES systems are used the wiring is likely to be far more straight forward. But whichever type of "logic solver" is used the reliability of the system needs to be analysed for each individual safety function. Let's consider the Safety Related Control Function (SRCF) for a safety gate, the control circuit might be shown thus:



This circuit could be represented by this block diagram:



It would not be unusual for a number of SRCF's on one machine to have the same logic and actuator parts but different sensor parts. Whatever the actual configuration the individual safety functions will have to have their performance verified.

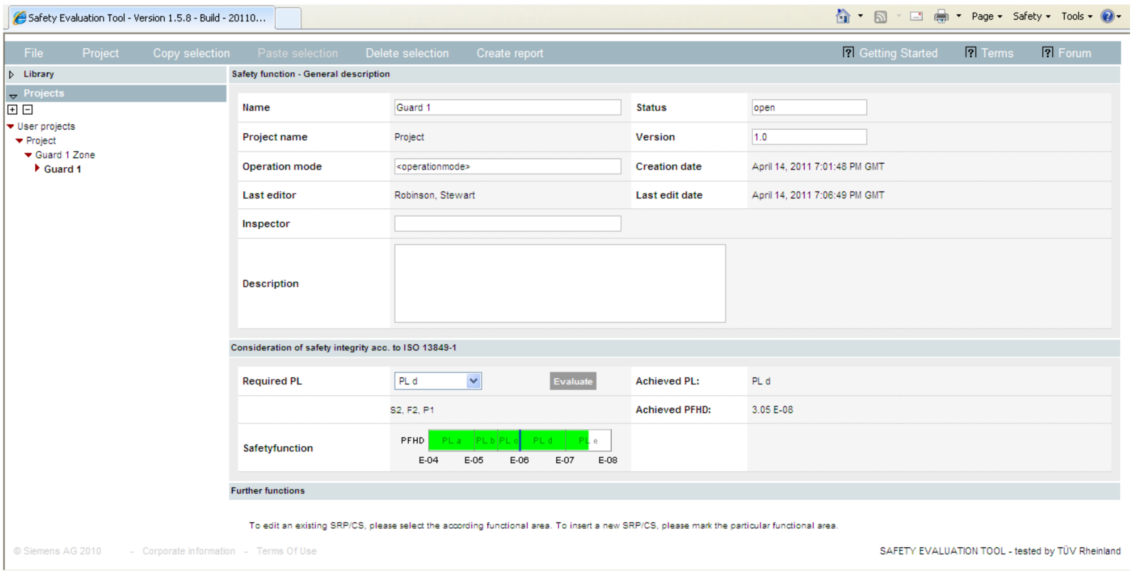
Verification tools

There is clearly some data to collect (e.g. component reliability), and some calculations to perform to demonstrate that the quantifiable aspects of the standards have been met. The calculations could of course be done manually, or be semi-automated by the use of spreadsheets or other commonly available tools. But perhaps the best way of approaching this is to make use of one of the freely available software programs that will not only handle the calculations but also provide some of the documentation that is required to demonstrate that the verification requirements of the standards have been satisfied.

Siemens Safety Evaluation Tool

This is an online tool that requires registration, it allows the user to create reports and save offline versions of projects. It provides a comprehensive library of Siemens safety components. This tool allows for the evaluation of control functions using both EN ISO 13849-1 and EN 62061 standards.

https://www.automation.siemens.com/mcms/safety-integrated/en/machine-safety/safety-evaluation-tool/Pages/Default.aspx



Screen shot showing the overall evaluation of a safety function

Software-Assistant SISTEMA

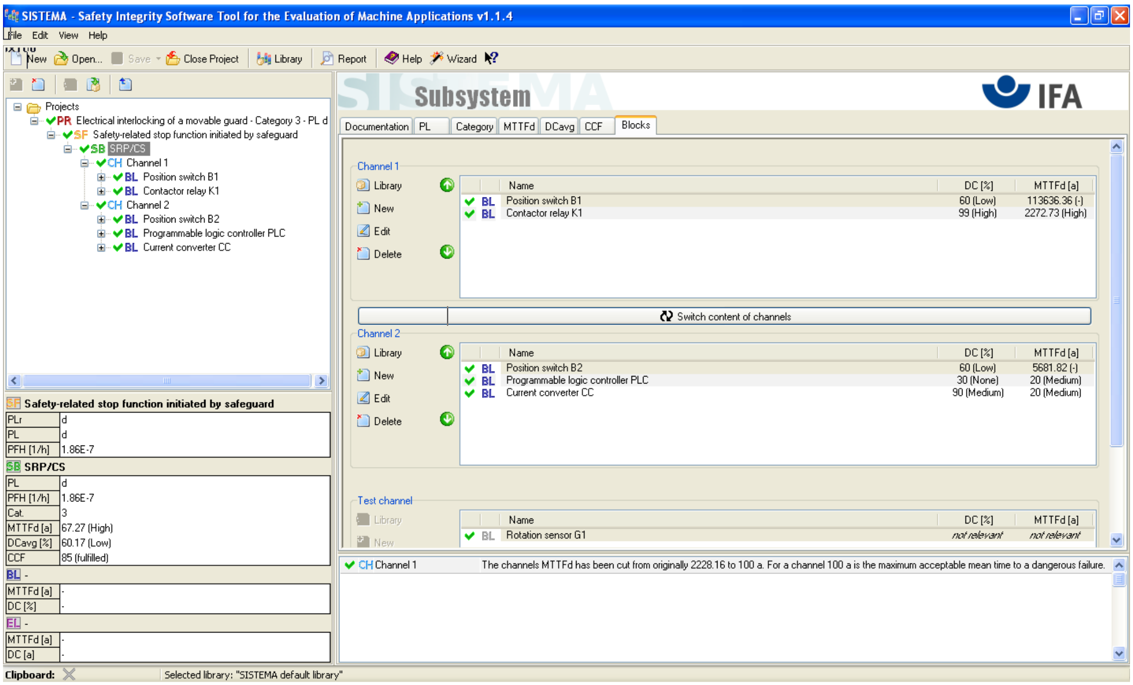
"A Tool for the Easy Application of the Control Standard EN ISO 13849-1"

This tool is provided by the IFA, this is an institute for research and testing of the German Social Accident Insurance in Germany

The "SISTEMA" PC program (Safety Integrity Software Tool for the Evaluation of Machine Applications) clearly describes all aspects of the analysis procedure contained in the standard for determining the probability of failure of control systems. SISTEMA contains all the data needed to assist the user in selecting and managing the parameters which are important for a control system. Use of SISTEMA is intuitive: wizard, help and report functions simplify operation and documentation of the inputs.

The tool can be freely downloaded and installed to run locally. A number of component manufacturers have created libraries of their safety components to use with SISTEMA.

http://www.dguv.de/ifa/en/pra/softwa/sistema/index.jsp



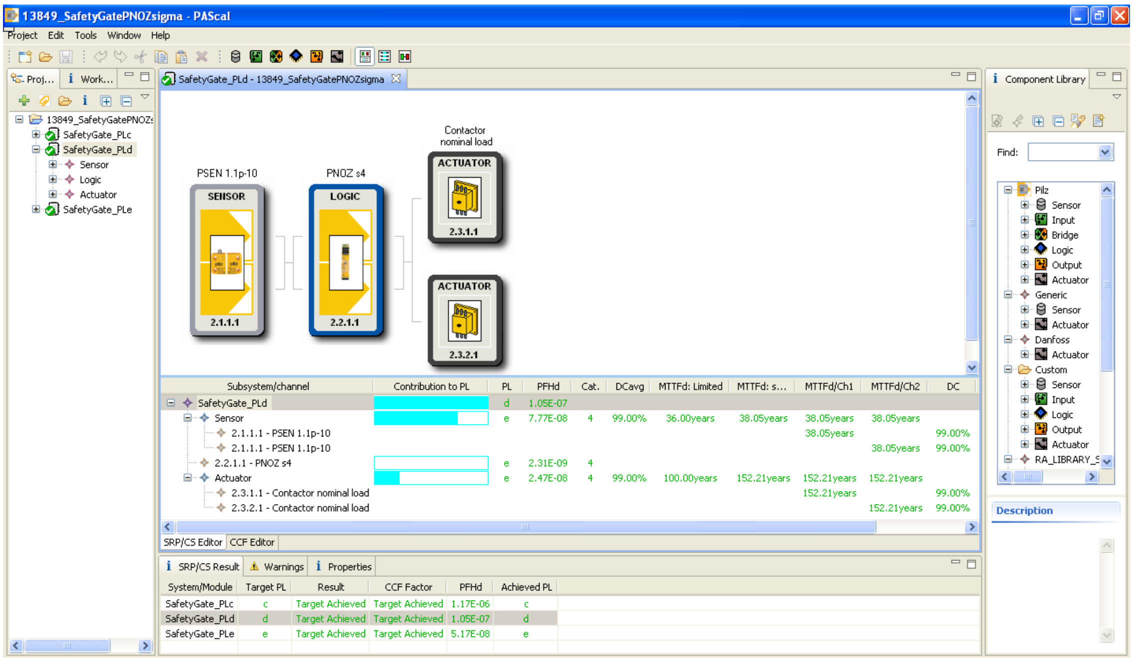
Screen shot showing the overall evaluation of a typical safety function.

Pilz PAScal

The Pilz PAScal Safety Calculator calculates the PL (Performance Level from EN ISO 13849-1) or SIL (Safety Integrity Level from EN 62061) that safety functions on plant and machinery can achieve depending on the components that are used. The results are displayed graphically, so it is easy to see how well the required safety level can be achieved at which points and with which components, or where improvements may be necessary.

The tool can be freely downloaded by registered users of the Pilz website (registration simply requires setting up an email address as a user name, and a password). The tool is then installed and run locally, it provides very useful functionality in it's free to use "demo mode". Applying a licence unlocks even greater functionality. It comes with a comprehensive library of Pilz components and some "generic" components, the import and export of SISTEMA libraries is also supported.

http://www.pilz.com/downloads/restricted/pascal_1.5.2.zip



Screen shot showing the evaluation of a typical safety function

Check list

Item	Reference	Yes	No
Have all risks been reduced as far as possible by safe design of the machine, and the use of fixed safeguards etc?	EN ISO 12100:2010 EN 953:1997		
Have the consequences of systematic failures been fully taken into account?	EN ISO 13849-1 Annex G EN 62061 Clause 6.4		
Have all risks that are to be reduced by Safety Related Controls been identified?	EN ISO 13849-1 Clause 4.4 EN 62061 Clause 5.2		
Have the Safety Requirements for each Safety Related Control Function been correctly specified in terms of functional requirements?	EN ISO 13849-1 Clause 5 EN 62061 Clause 6.6.2.1.6		
Have the Safety Requirements for each Safety Related Control Function been correctly specified in terms of performance requirements?	EN ISO 13849-1 Clause 4.3 and Annex A EN 62061 Clause 6.6.2.1.6 and Annex A		
Has an appropriate architecture for the design of the safety related controls been chosen?	EN ISO 13849-1 Clause 6 EN 62061 Clauses 6.6.2.1.2,3,7		
Is performance data available for safety related components from: 1) The component manufacturer. 2) Reliable generic data	EN ISO 13849-1 Clause 4.5.2 and Annexes C and D EN 62061 Clause 6.7.7.2		

Item	Reference	Yes	No
Has the Diagnostic Coverage provided by the automatic tests been correctly established?	EN ISO 13849-1 Annex E EN 62061 Clause 6.8		
Have the effects of Common Cause Errors been examined and adequate measures to mitigate the consequences put in place?	EN ISO 13849-1 Annex F EN 62061 Clause 6.7.8.3 and Annex F		
Has the performance of the safety related control functions been verified as meeting the required PL or SIL?	EN ISO 13849-1 Clause 4.7 EN 62061 Clause 6.6.3		
Have the requirements for validation been adequately planned and prepared?	EN ISO 13849-2 EN 62061 Clause 8		

N.B. The above table is for guidance on the use of the standards for the selection and design of hardware, and the evaluation of random hardware faults. The requirements for safety related software are not covered in this paper at all, but they are extremely important to consider when Programmable Electronic Systems are being used.

References

EN ISO 12100:2010

Safety of machinery — General principles for design — Risk assessment and risk reduction

ISO/TR 14121-2:2007

Safety of machinery -- Risk assessment -- Part 2: Practical guidance and examples of methods

EN 953:1997

Safety of machinery — Guards — General requirements for the design and construction of fixed and movable guards

EN 62061:2005

Safety of machinery –Functional safety of safety-related electrical, electronic and programmable electronic control systems

EN ISO 13849-1:2008

Safety of machinery - Safety related parts of control systems – Part 1: General principles for design

EN ISO 13849-2:2008

Safety of machinery — Safety-related parts of control systems — Part 2: Validation

EN 60204-1:2006

Safety of machinery — Electrical equipment of machines — Part 1: General requirements