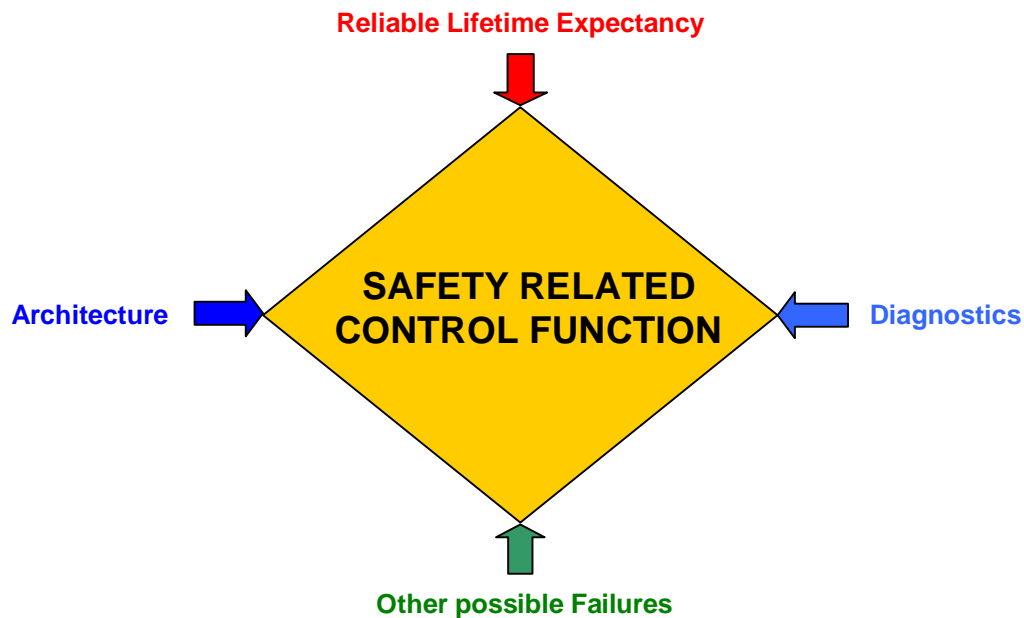


Functional Safety



*An introduction and practical guide to the implementation of
Functional Safety to machinery*

By

Robin J Carver
MIET MInstMC CMIOASH MIIRSM
Chartered Safety Practitioner

Version 1.11
Dated February 2008

Functional Safety

An introduction and practical guide to the implementation of Functional Safety to machinery

Introduction

“Functional Safety” – will it be the long awaited panacea to all machinery safety related control problems? Will it revolutionise the machinery industry? Probably not but it will give designers a little more flexibility in their choice of equipment and enable the design to incorporate some programmed elements.

This guide aims to help the designer to understand the origins and principals of functional safety, identify the standards available for guidance and give practical advice on designing, applying, verifying and validating a “functional” safety related control system to machinery. It is also intended to reveal the meanings of the plethora of new abbreviations, so much loved by sales engineers in selling their wears.

The guide is specifically aimed at the safety of machinery (as covered by European Standard EN 62061). The application of functional safety applied to the safety of process systems (as covered by European Standard EN 61511) is different and does not include process systems within its scope.

Situation prior to 2002 (publication of EN 60204-1)

The use of electronics for the control of machinery took off in the late 1960's with the development and application of programmable logic controllers (PLC's) and industrial computers. Devices such as the Texas 5TI, the ITT Director and the Sprecher+Schue, Sestep 400 propelled the industry into the programmable age. Unfortunately, at this early stage such controllers were slow, prone to failure due to unreliable system checks and vulnerable to component failure. Component reliability being a particular concern as electronic components were prone to fail ON (generally the unsafe state) unlike electro-mechanical components which had a propensity to fail OFF (generally the safe state). Given these factors the use of electronics and programmable electronics in safety related applications was generally considered unacceptable in industrial machinery applications. This was

confirmed by the publication of EN60204-1 Safety of Machinery: Electrical equipment of machines. Until its revision in 2005 it stated that: “...[safety systems].....operation shall not be dependant on electronic logic or the transmission of commands over a communications network or link” [EN60204-1:1997 – Emergency Operations - Clause 9.2.5.4]

In reality electronics was being employed in many safety related devices e.g. Light Curtains, Laser Scanners, etc. based on specific product related standards. The industry demanded the use of electronics and programmable electronics in safety related applications and manufactures were responding to the demand by producing electronic and programmable safety devices without the guidance of any recognized standard. Thus standards had to be drawn up to give sound guidance to both the designers and potential users and programmers of such systems. To this end a “generic” International Standard was drawn up by the IEC. This was IEC 61508 “Functional safety of electrical/electronic/programmable electronic safety-related systems” and this standard was adopted in the European Union as EN 61508 in 2002.

A little about Standards

Before going further, it is important to understand the purpose of a Standard. A standard is defined as a published specification that establishes a common norm and is a recognised document that defines good practice. Standards are designed for voluntary use and do not usually impose any regulation, however, laws and regulations may refer to certain Standards making compliance with them compulsory.

European Harmonised Standards have been adopted throughout the European Union to give guidance in complying with the essential requirements of European Directives. They are also known as “EuroNorms” and carry the nomenclature prefix “EN”. (note: a “Normal” is the term for standard in most languages other than English). The European standards for Safety of Machinery are prepared to give guidance in complying with the essential requirements of European Machinery and associated Directives. These standards are not mandatory.

Effect of the publication of EN 61508

EN 61508:2002, “Functional safety of electrical/electronic/programmable electronic safety-related systems (E/E/PESs)” is in seven parts and sets out a generic approach for all safety lifecycle activities for systems comprised of electrical and/or electronic and/or programmable electronic components that are used to perform safety functions. A major objective of this “generic” standard is to facilitate the development of application sector standards.

The introduction to the standard recognizes that in most situations, safety is achieved by a number of protective systems which rely on many technologies (for example mechanical, hydraulic, pneumatic, electrical, electronic, programmable electronic). The introduction goes on to state that any safety strategy must therefore consider not only all the elements within an individual system (for example sensors, controlling devices and actuators) but also all the safety-related systems making up the total combination of safety-related systems. Therefore, while this Standard is concerned with electrical and/or electronic and/or programmable electronic components that are used to perform safety functions, it may also provide a framework within which safety-related systems based on other technologies may be considered.

The machinery sector standard developed in conjunction with EN 61508 is EN 62061:2005 “Safety of machinery - Functional safety of electrical/electronic/programmable electronic safety-related systems” and much of this document is based on this standard. As with EN 61508 the standard was drawn up by the IEC as an international standard and was adopted in the European Union in 2005.

With synergy to the safety of machinery sector standard is the standard for functional safety of safety instrumented systems for the process industry (EN 61511). Other industry sector functional safety standards include that for Nuclear power plants: Instrumentation and control for systems important to safety, Railway control and protection systems, etc.

To complement the publishing of EN 61508 other standards have been updated or, in some cases, replaced or in the process of replacement. These include:-

- EN ISO 12100 replacing EN 292
 - To provide designers with an overall framework and guidance to enable them to produce machines that are safe.

- EN ISO 14121 to replace EN 1050
 - general principles for Risk Assessment

- EN IEC 62061 NEW
 - Requirements for the design, integration & validation of Safety Related Electrical, Electronic & Programmable Electronic Control Systems for Machines.

- EN ISO 13849 to replace EN 954
 - Specifies characteristics & categories required for Safety Related Parts of Control Systems (SRP/CS) – all technologies

- EN 60204:2005 updated from EN 60204-1:1997
 - Application of electrical & electronic systems to machines

In addition to the “generic” standard EN 61508, two standards have a particular influence on the safety of machinery.

They are:-

EN 62061:2005 “Safety of machinery - Functional safety of electrical/electronic/programmable electronic safety-related systems.”

and

EN 13849-1:2006 “Safety of machinery -- Safety-related parts of control systems -- Part 1: General principles for design.”

Overview of EN 62061

EN 62061:2005 “Safety of machinery - Functional safety of electrical/electronic/programmable electronic safety-related systems” is the EN 61508 industry sector related standard for machinery.

It has six significant objectives:-

1. Management of functional safety (Clause 4)

Specifying the management and technical activities which are necessary for the achievement of the required functional safety of the safety-related parts of the control system (SRECS).

2. Requirements for the specification of safety-related control functions (Clause 5)

Sets out the procedures to specify the requirements for safety-related control functions. These requirements are expressed in terms of functional requirements specification, and safety integrity requirement specification.

3. Design and integration of the safety related electrical control system (Clause 6)

Specifying the selection criteria and/or the design and implementation methods of the SRECS to meet the functional safety requirements.

This includes:

- selection of the system architecture,
- selection of the safety-related hardware and software,
- design of hardware and software,
- verification that the designed hardware and software meets the functional safety requirements.

4. Information for use of the machine (Clause 7)

Specifying the requirements for the information for use of the SRECS, which has to be supplied with the machine.

This includes:

- provision of the user manual and procedures,
- provision of the maintenance manual and procedures.

5. Validation of the safety related electrical control system (Clause 8)

Specifying the requirements for the validation process that has to be applied on the SRECS. This includes inspection and testing of the commissioned SRECS to ensure that it achieves the requirements stated in the safety requirement specification.

6. Modification of the safety related electrical control system (Clause 9)

Specifying the requirements for the modification procedure that has to be applied when modifying the SRECS.

This includes:

- modifications to any SRECS are properly planned and verified prior to making the change;
- the safety requirement specification of the SRECS is satisfied after any modifications have taken place

Overview of EN 13849-1

EN 13849 is intended to provide safety requirements and guidance on the principles for the design and integration of safety-related parts of control systems (SRP/CS) for all kinds of machinery. It applies to all safety-related parts of control systems, regardless of the type of technology and energy used (electrical, hydraulic, pneumatic, mechanical, etc., including the design of software).

It is a very prescriptive standard which specifies methods for the determination of the performance level required for carrying out safety functions and formulated verification methods to establish that the performance levels have been met.

Unlike its predecessor, EN 954-1, EN 13849-1 calls for relatively complex calculations (which the writer considers to be dubious) which would, in practice, involve the designer in a complex verification process even for the simplest of systems. Furthermore, the terminologies and determinations used are not the same as those used in EN 61508 or EN 62061.

It is the writer's opinion that EN 13849-1 will be of little practical use to the designers of safety-related parts of control systems and that the principles of EN 62061 should be followed even when dealing with multi technology based systems. Thus a continuity of technique and terminology will be maintained.

What's changed?

EN 954-1 "Safety of machinery - Safety-related parts of control systems" (to be superseded by EN 13849-1) called for a qualitative approach to verification of the suitability of the safety related parts of the control system. It recommended an appropriate architecture (the need for redundancy and diagnostics in the structure – the Category) and determined reliability by simply calling for well-tried components and well-tried safety principles. This was probably (and arguably still is) sufficient when using simple and basic electro-mechanical type hardware due principally to its "fail to safe state" tendencies, but becomes more uncertain when component & software rich electronic techniques are employed. EN 61508 calls for a quantitative determination of the system specifying and verifying the reliability and the necessary architecture matching the degree of component

reliability. The programmable element has to be taken into account. The configuration can so easily be changed by a few key strokes as opposed to rewiring and the accessibility and competence of the involved parties must be taken into account and controlled.

Functional Safety for machinery – The practicalities

Whilst sounding very exotic “functional safety” applied to machinery is little different to that we have been using for years. The implication is that the safety function is built into the functional system. This may be true with process systems but machinery is generally much simpler.

Machinery safety vs Process safety

For machinery, in the event of an unsafe situation or emergency the usual safe action is simply to turn off power. (*“if it hurts – stop doing it, type logic!”*).

Process systems are often more complex. Turning of the power to, say a mixer, may be a safe option at one stage of a process, but as the process progresses the product may become more volatile and stopping the mixer in this stage may now become the unsafe option.

In machinery the potentially unsafe state may be detectable by the opening of an interlock switch or the breaking of a light curtain. Again in a process system the potential unsafe condition may be more difficult to determine, it being intimated by an unacceptable rate of rise of a temperature or pressure, a situation where decision logic may have to be employed.

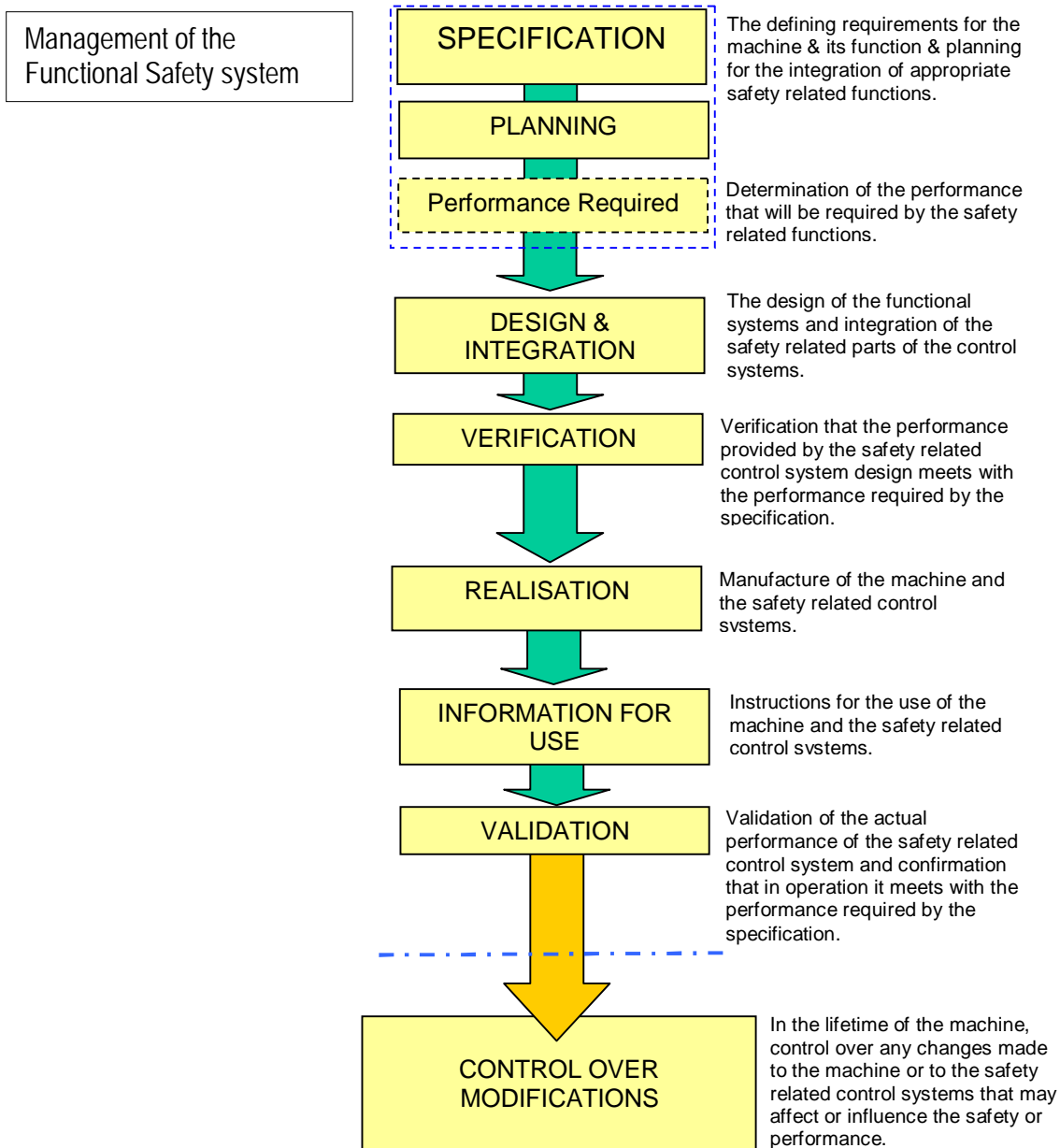
Machinery safety is, in most cases on the periphery of the functional system acting like a protective “shell”. In practice machinery functional safety remains broadly unchanged but the use of electronics and programmable “safety relays” is possible where the conventional “safety relays” were used before.

Application of the principals of EN 62061 to machinery allows the designer to employ a wide range of components and technologies in the safety related control system design and reinforce component reliability (which was never fully taken into account under EN 954-1) with the “architecture” of the system (which was, under EN 954-1, using the Category system). Not all components and configurations will be

acceptable but by using the verification and validation techniques the designer will be able to determine their suitability in the application.

The principles described in the following are based on the framework guidance given by EN 62061 but, on occasion drawing on the beneficial parts of EN 13849-1 where it offers “*reasonably practicable*” advice.

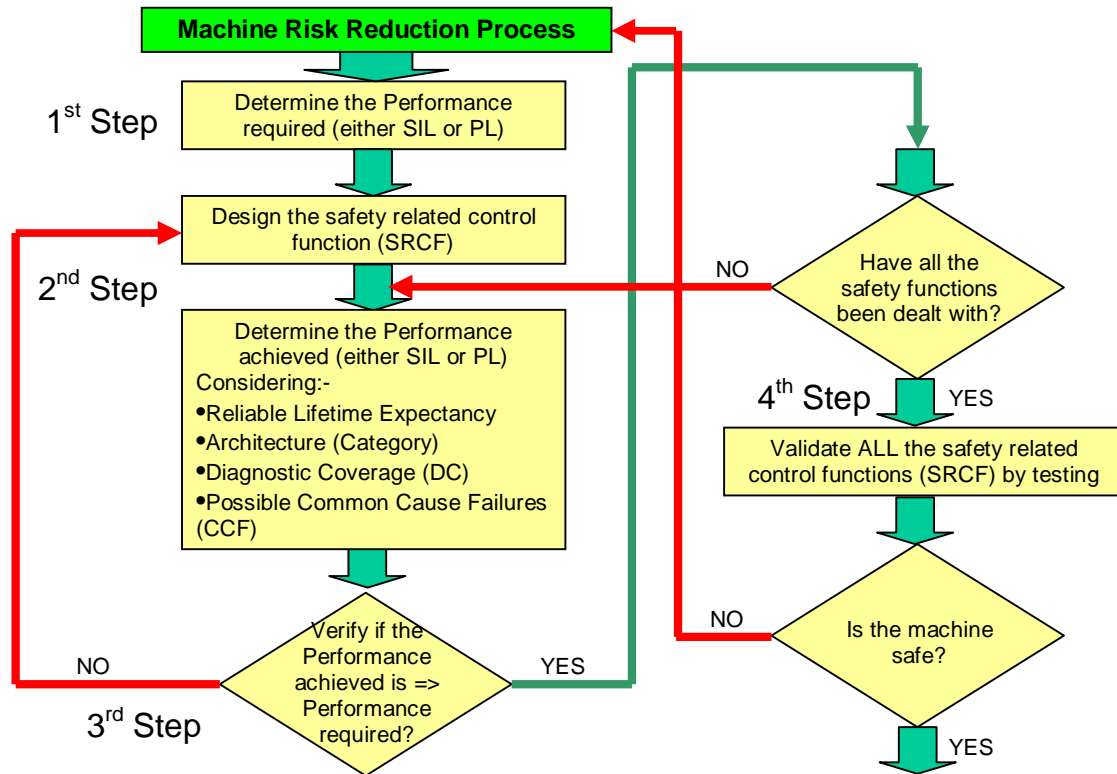
Quantified safety for machinery requires a systematic managed approach.



4 Step Procedures

The specification is vital in the design and development of any machine and planning is a key to the successful realisation of the safety related control system.

The process may be seen as a 4 step procedure:-



Step 1 – Determine the Performance Required

The first action in the design of any safety related control system is to determine the level of integrity of the system that will be required (the performance required). This is primarily the responsibility of the machine designer based on the systematic process of risk assessment and risk reduction as prescribed in EN ISO 12100-1:2003 (clause 5.4).

In EN 62061 this is called the Safety Integrity Level or SIL and requires a SIL determination for the safety of the machine or particular part of the machine. (confusingly under EN 13849-1 a different system & terminology is used – Performance level or PL).

SIL is a measure of safety system performance, or probability of failure on demand (PFD).

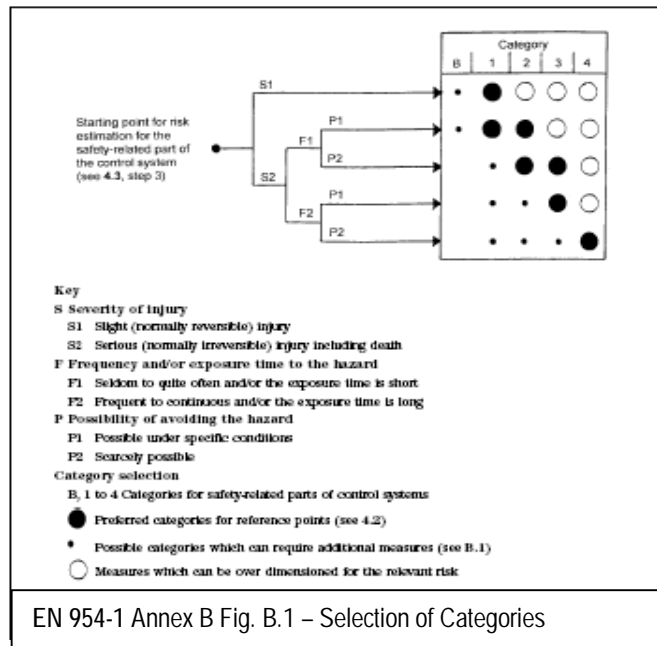
SIL is a quantifiable measure as follows:-

SIL 1	≥10 ⁻⁶ to < 10 ⁻⁵ (or 1 failure in 100,000 h)
SIL 2	≥10 ⁻⁷ to < 10 ⁻⁶ (or 1 failure in 1,000,000 h)
SIL 3	≥10 ⁻⁸ to < 10 ⁻⁷ (or 1 failure in 10,000,000 h)

A SIL 4 exists but is not applied to machinery as it refers to the safety integrity level required where the consequence of a failure could result in a major disaster and/or multiple fatalities.

Determining the Performance required (or required SIL rating) for a machine

Those familiar with EN 954-1 will recognise the chart given in Annex B which uses a simple risk assessment determination network to indicate a desired system architecture, “the category” :-



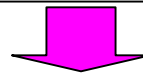
Determining the required SIL rating

That for SIL rating determination suggested in EN 62061 is more quantitative and uses a more complex Risk Assessment strategy:-

Frequency of Exposure		Probability of Harm		Possibility of Avoiding	
	Fr		Pr		Av
Many times an hour	5	Very likely	5	Impossible	5
Hourly	5	Likely	4	Possible	3
Daily	4	Possible	3	Likely	1
Weekly	3	Rare	2		
Yearly	2	Negligible	1		



Sum of:- Fr + Pr + Av

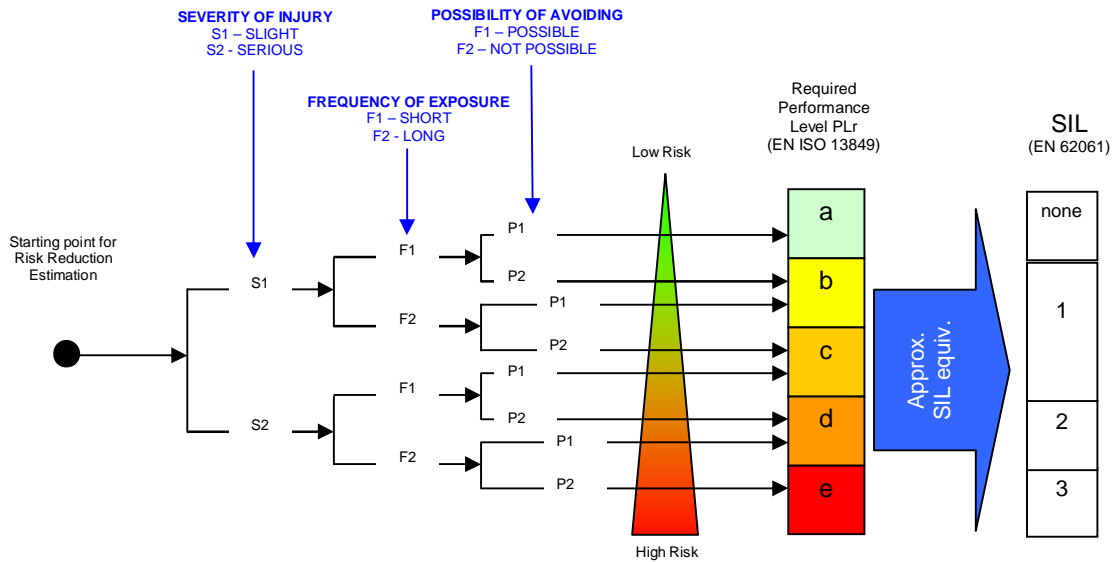


Severity of any Injury		Result range				
	Se		4 to 7	8 to 10	11 to 13	14 to 15
Death, loss of limb(s), etc.	4		SIL2	SIL2	SIL3	SIL3
Loss of finger(s) etc.	3			SIL1	SIL2	SIL3
Reversible - Hospital	2				SIL1	SIL2
Reversible – First Aid	1					SIL1

Alternative - Determining the required Performance Level (PL_r)

Similar to the system used to determine the “Category” under EN 954-1 the Performance Level required (PL_r) in EN 13849-1 (Annex A - Figure A.1) uses a chart. Unlike the EN 954-1 chart, the performance level is based on a hierarchy of risk and follows a common format with ISO 14121-1 (Safety of Machinery – Risk Assessment).

Determining the required PL_r rating



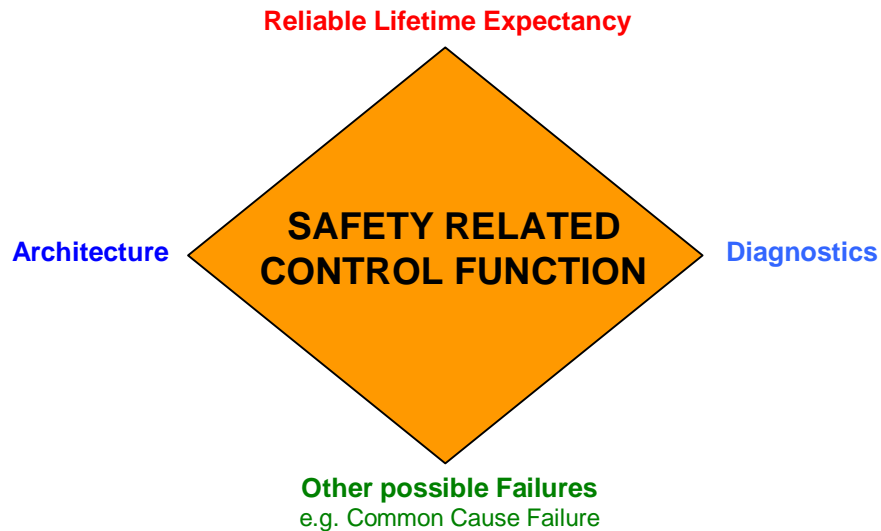
Step 2 – Determining the performance achieved by the design

Having determined the required performance level, either as the SIL required or the PL required, the next step is to design the safety related control function (SRCF) and then determine the Performance that the SRCF can achieve (again either as SIL or PL).

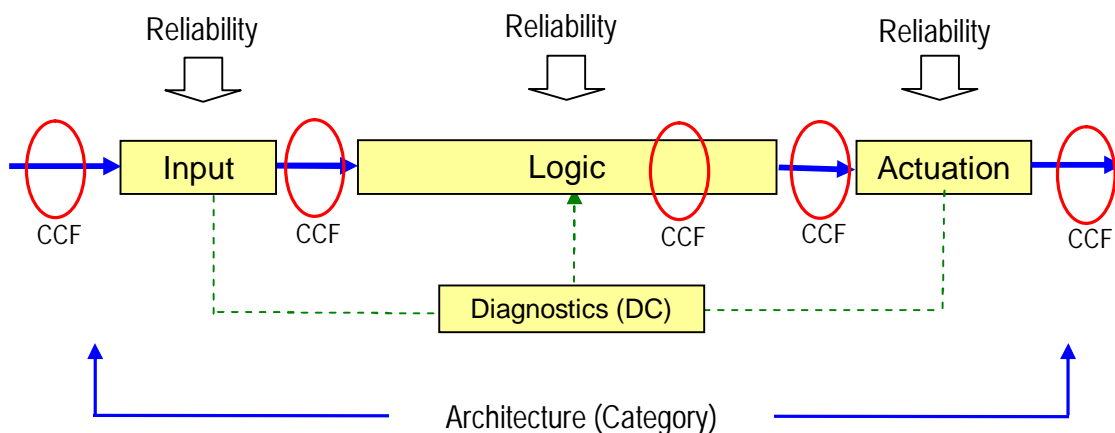
The following factors must be determined and quantified:-

- a). Reliable Lifetime Expectancy
- b). Architecture (Category)
- c). Diagnostic Coverage (DC)
- d). Possible Common Cause Failures (CCF)

Elements of a Safety Related Control Function



Elements of a Safety Related Control Function in a system logic



Reliable Lifetime Expectancy

The reliability of the components used in the safety system is crucial. Under EN 954-1 the demand was simply for the use of proven components and principles. In functional safety this must be proven and quantified. EN62061 [6.7.2] states that “*for electromechanical subsystems, the probability of failure should be estimated taking into account the number of operating cycles declared by the manufacturer and the duty cycle of the application.*” ISO 13849-1 determines reliability using Mean Time to Dangerous Failure (MTTF_d) figures which are, in the opinion of the writer, dubious at best and few suppliers are able to give MTTF_d's for their products. Most suppliers of electromechanical components, however, specify the number of operations for the lifetime anticipated and from this the life expectancy of a component may be calculated if the duty demand is reasonably predictable. The “no. of ops” figures given are usually reliable as they are based on the manufacturer’s practical endurance tests.

Example:-

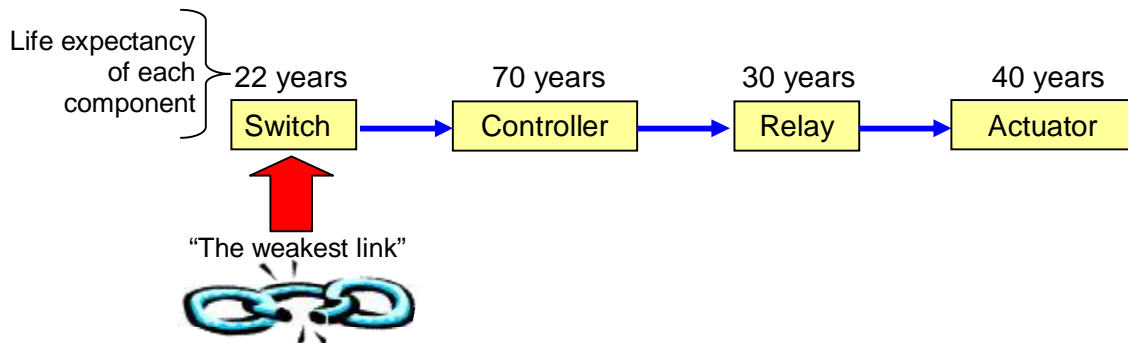
A safety component, a safety switch, used on a machine protecting a moving guard used to give access for cleaning the machine approximately 4 times a day:-

- Manufacturers declared number of operations for the safety switch:-
= 500,000 operations
- Estimated number of operation of the safety switch per hour:-
= 4
- Estimated use of the machine per day:-
= 16 hours
- Estimated use of the machine per year:-
= 350 days

Therefore the safety switch *life expectancy* = $500,000 / (4 \times 16 \times 350 \text{ days})$
= 22 years

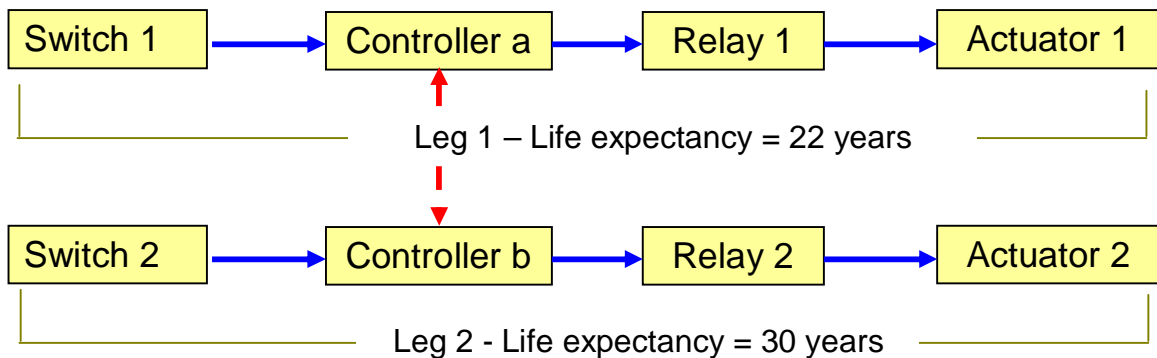
Note: This assumes ideal conditions. It may have to be reduced to take into account the conditions in use.

The *life expectancy* of the total safety related control function (SRCF) could be limited to the weakest component – the lowest life expectancy (based on operations). This will be its “*weakest link*”.



Therefore the anticipated life expectancy for the safety related control function (SRCF) could be considered to be the lowest of these values, in this case 22 years.

The *life expectancy* of a “dual” “redundant” part of SRCF could be the mean of each leg:-



Therefore the anticipated (lowest) life expectancy for the SRCF as a whole
 = $(22 + 30)/2 = 26$ years

Clearly, this assumes the manufactures anticipated conditions for use of the components and these may be the “ideal” conditions. The factors may have to be modified (probably reduced) to take into account the conditions in actual use.

EN62061 (6.2.3) States:- *The design of the safety system shall take into account human capabilities and limitations including reasonably foreseeable misuse.....*

These could include:-

- The environment, e.g. dirty, abrasive, chemicals, etc.
- Level of maintenance,
- User competence, e.g. rough handling, misuse, etc.
- Production demand, e.g. bypassing of safety functions,

It may be necessary to *factor* the life expectancy for the SRCF as a whole to take into account such foreseeable conditions.

For example:-

= **Life expectancy x factor** (say 80 – 90% as appropriate)

Finally, and for simplicity, the Reliable Life Expectancy estimate for the SRCF may be broken down into three basic periods of anticipated reliability (these are based on EN ISO 13849-1):-

Denotation of Life Expectancy	Reliable Life Expectancy (in years)
Low	3 years to c 10 years
Medium	10 years to c 30 years
High	30 years to c 100 years

Architecture

The architecture is structure of the safety related control system and in combination with the Diagnostic Coverage (DC) which is the ability of the system to detect faults in itself has the same “Category” format as detailed in EN954-1.

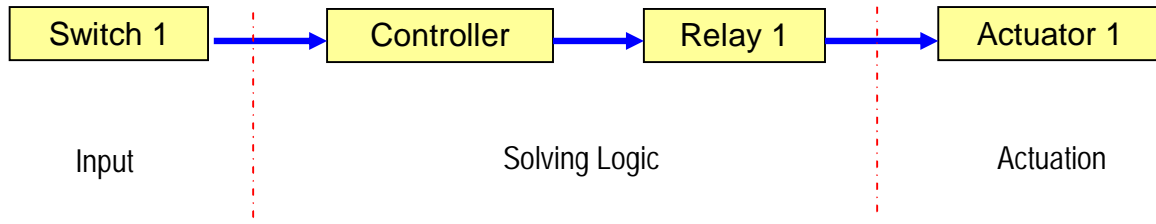
Category	System behaviour	Principle	HFT (Note 1)
B	A fault can to the loss of the safety function. <i>Not considered appropriate for industrial machines</i>	Components	0
1	A fault can lead to the loss of the safety function but probability lower than for B.	Components	0
2	A fault is detected by a check but may lose the safety function between the checks.	Components & Structure	0
3	When the single fault occurs the safety function is always performed. Some, but not all faults will be detected.	Components & Structure	1
4	When the single fault occurs the safety function is always performed. The faults will be detected in time to prevent the loss of the safety function.	Components & Structure	1 or >1

Note 1:

HFT (Hardware Fault Tolerance) – the ability of a safety system to continue to perform its required function in the presence of faults or failures.

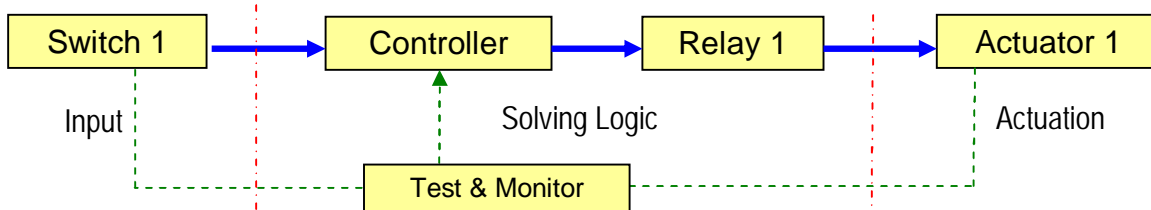
Category B and 1 are dependant only on the reliability of the components used, and will not be tolerant of any failure hence any one component failure may lead to a loss of the safety function (Hardware fault tolerance (HFT) = 0)

Block architecture for a Category 1 safety system



Category 2 is similarly is dependant on both the reliability of the components used and its structure includes some diagnostics which whilst may not be tolerant of any one component failure the fault may be detected and a warning given.

Block architecture for a Category 2 safety system



Categories 3 and 4 are dependant on both the reliability of the components used and its structure which includes redundancy such that it is tolerant of component failure and includes some diagnostics which may detect the fault and prevent the system from continuing if a fault is present. (Hardware fault tolerance (HFT) = 1 or more)

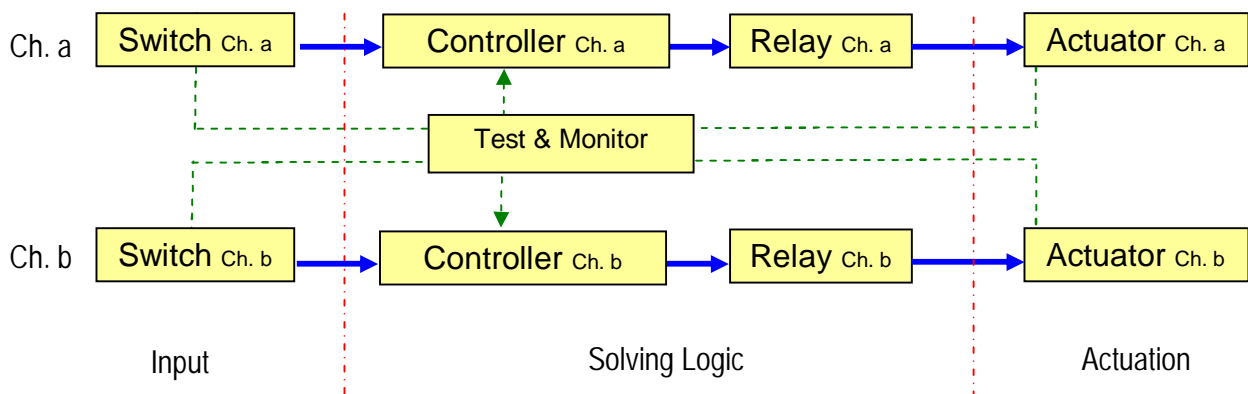
A Category 3 system allows that:-

- when the single fault occurs the safety function is always performed,
- some but not all faults will be detected,
- an accumulation of undetected faults can lead to the loss of the safety function.

A Category 4 system allows that:-

- a single fault in any of the safety-related parts does not lead to a loss of the safety function,
- and**
- the single fault is detected at or before the next demand upon the safety functions, e.g. immediately, at switch on, or at end of a machine operating cycle,
 - **but** if this detection is not possible, then an accumulation of undetected faults shall not lead to the loss of the safety function.

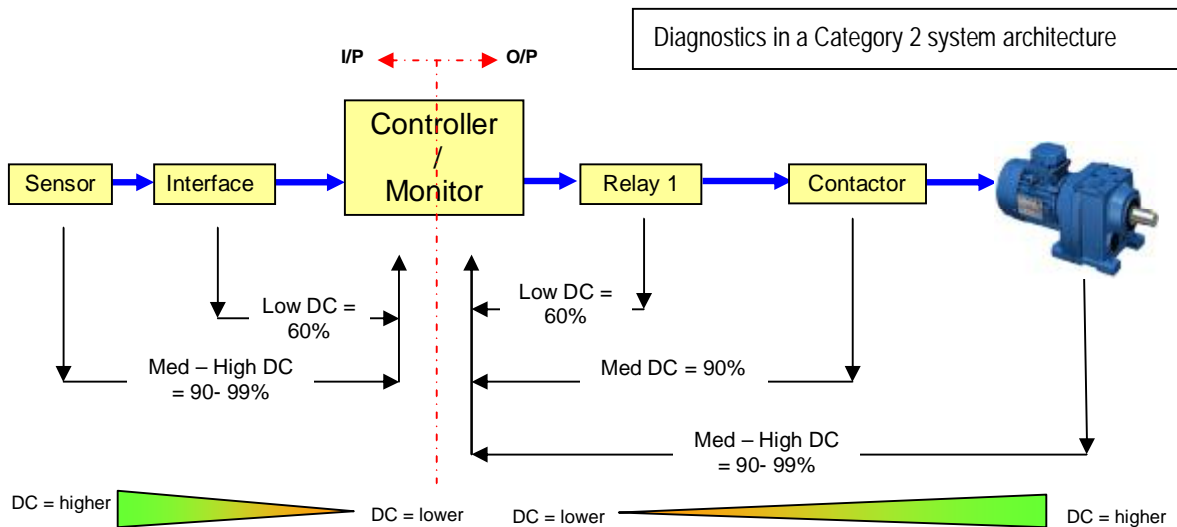
Block architecture for a Category 3 & 4 safety system



Diagnostic Coverage (DC)

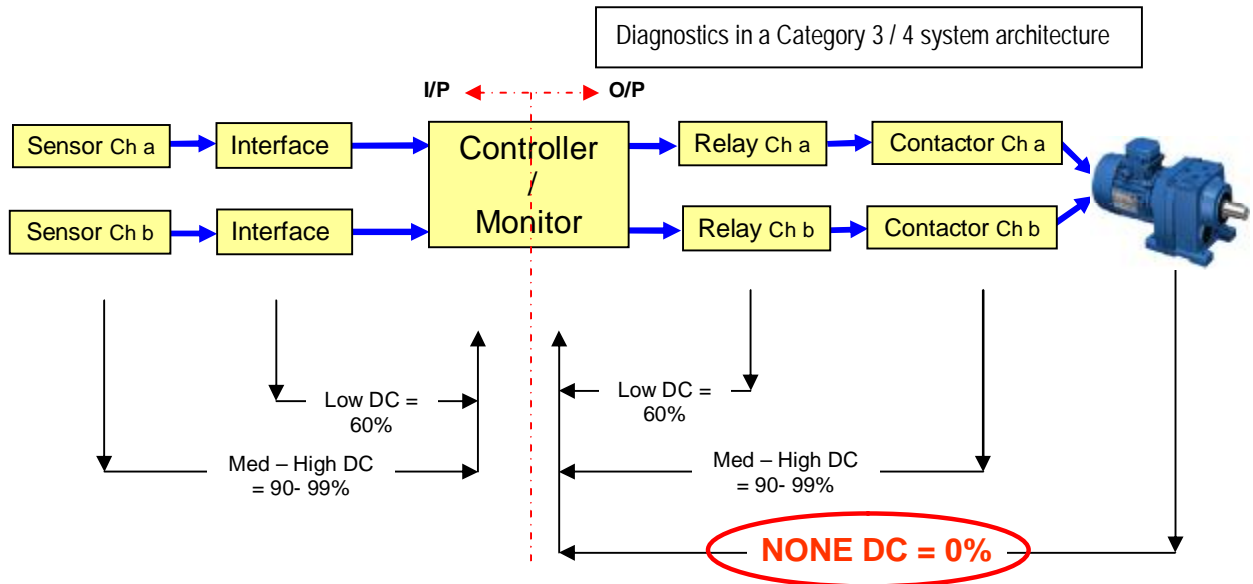
Diagnostic in a safety related control function is the ability of the system to detect faults in itself. The ability of a safety system to detect faults is required for all architectures above Category 1 and, generally, it is required that most system faults should be detected at or before the next demand upon the safety functions, e.g. immediately, at switch on, or at end of a machine operating cycle.

Clearly, detection of a fault in a category 2 architecture which is dependant on the reliability of the components and does not include any redundancy and hence has a HFT (Hardware Fault Tolerance) of 0, cannot protect the system other than warn the user that a fault has occurred. The further out from the controller/monitor the diagnostic test is conducted the more effective is the coverage (DC).



In a Category 3 or 4 system architecture, the redundancy could “mask” any fault, as the redundant protection would “back up” the operation of the safety function. For example, in a system with redundant motor contactors in series, a failure of one of the contactors due to welding of contacts would not be obvious because of the continued operation of the second contactor. Without diagnostics the fault would not be apparent until the second contactor failed and the system has become unsafe. Diagnostics should detect this first failure and prevent continued operation before the next demand on the safety function.

As with a Category 2 system the further out from the controller/monitor the diagnostic test is conducted the more effective is the coverage (DC), however, it is important to note that because of the redundancy in a Category 3/4 system, monitoring of the final action, e.g. the rotation of the motor etc. would **not** effectively contribute to the diagnostics as, again, the redundancy would “mask” any fault at this point. Hence the diagnostic coverage (DC) would be 0% as it would be unable to detect a failure.



The percentage values given are arbitrary (based on EN ISO 13849-1) and for simplicity, the Diagnostic Coverage (DC) estimate may be broken down into four basic levels:-

Denotation of DC	Typical configuration	Range of DC
None	No monitoring	0%
Low	Monitoring of the input sources or intermediate output only (e.g. internal DC within a Safety PLC only)	60%
Medium	Monitoring of most input sources & the final significant control outputs.	90%
High	Monitoring of all the input sources & the final control outputs and the control wiring integrity.	99%

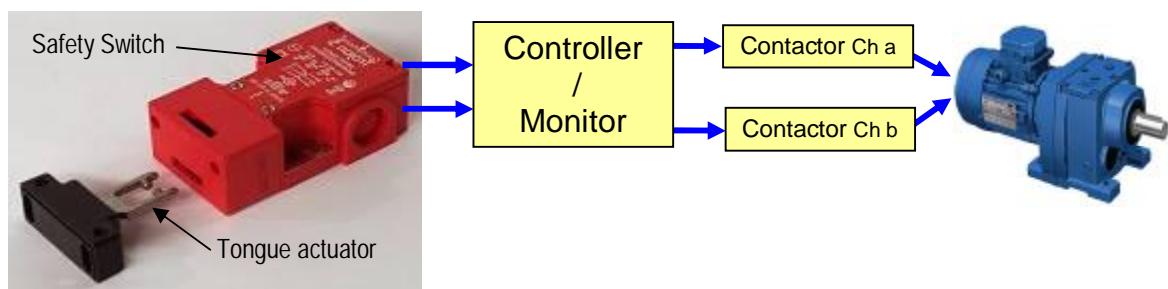
Low Diagnostic Coverage is of little practical use as it means that monitoring in a safety related system is not comprehensive and the possibility of an undetected failure remains a significant factor. A “Safety” PLC may have a “High” self diagnostic denotation but if the diagnostics is not extended throughout the complete safety related part of the control system then the system denotation should be assessed as “Low”. It is a possibility that a system using an inferred Diagnostic Coverage such as the monitoring of an analogue signal limit value, e.g. a linear valve actuator with positioner, tripping a 4 to 20mA signal at 4mA, may be employed but its reliability may be assessed such that it falls into a “Medium” denotation as a Diagnostic Coverage function.

Common Cause Failures (CCF)

Common Cause Failure CCF is the occurrence of more than one failure event due to the same common cause. In particular the possibility of a failure in a redundant (Category 3 of 4) system which has a common effect on both channels.

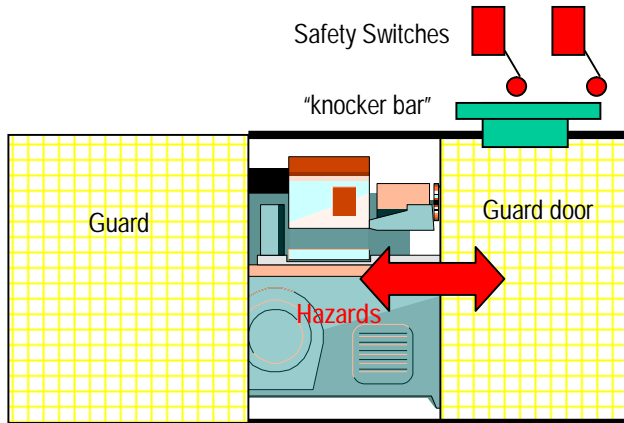
Example 1

A typical example would be a “tongue” operated safety interlock on a guard door. The switch has redundant switch contacts wired into a Category 3 or 4 safety related control system. The SRCS has a HFT of 1 so that if the single fault occurs in the electrical system the safety function is always performed. However, if an operator placed a single spare “tongue” into the switch the system will perform correctly but the guard door is no longer protected by the safety system having been bypassed by a “common cause”.



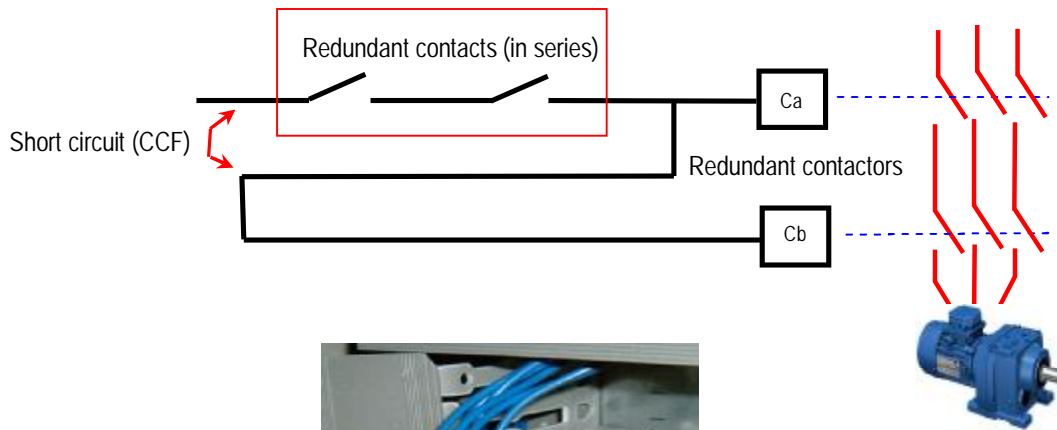
Example 2

Two redundant door switches on a guard door operated by a common “knocker bar”. If the “knocker bar” comes loose and/or falls off monitoring of the guard door is lost.



Example 3

Within the safety circuit there are 2 redundant contacts in series. A single common short circuit (chafing of wiring, pcb track failure, deliberate bypassing, etc.) could render the system unsafe.



An example of a CCF where a single wire had been deliberately re-terminated to bypass a redundant pair of safety contacts resulting in a serious accident.

By its nature quantifying possible common cause failure is difficult. EN ISO 13849-1 attempts to quantify CCF by a generalised “scoring” system. In practice good engineering practice employed at the design, manufacture and installation stages of the safety related control systems should help reduce the possibilities of common cause failure.

These would include:-

Design

Resources & Competence

- Manufactures & maintainers given the time and resources to undertake the work competently with adequate control including verification & validation of the design, commissioning, use and modification.
- Designers & maintainers adequately experienced & trained and with the knowledge to understand the causes and consequences of common cause failures.

Diversity

- Different techniques and/or technologies and/or physical principles used, typically:
 - First channel programmable electronic and second channel hardwired,
 - Components from different manufactures.
 - Kind of initiation, e.g. 1 set of n/o contacts and 1 set of n/c contacts

Analysis

- Design stage failure mode and effect analysis to identify and avoid potential common-cause failures.
- Examination of the reasons, likelihood and possible methods by which the systems could be defeated by the users – reduction of the need to defeat systems and/or selection of components to reduce the likelihood.

Manufacture & Installation

Separation and segregation

- Physical separation between signal paths.
- Separation in wiring/piping.
- Sufficient clearances at terminations.
- Prevention of incorrect placement of components (e.g. coding pins on plug-in components)

- Prevention of chaffing of insulation especially where wire looms are subject to movement (e.g. wiring of components on panel doors or moving actuators)

Environmental

- Prevention of signal corruption by electromagnetic interference by complying with manufactures recommendations for electromagnetic compatibility (EMC), good engineering practice and testing in accordance with appropriate standards.
- Prevention of contamination in fluidic systems: filtration of the pressure medium, prevention of dirt intake, drainage of compressed air, e.g. in compliance with the component manufacturers' requirements concerning purity of the pressure medium.
- Considering all relevant environmental influences such as, temperature, shock, vibration, humidity, dirt

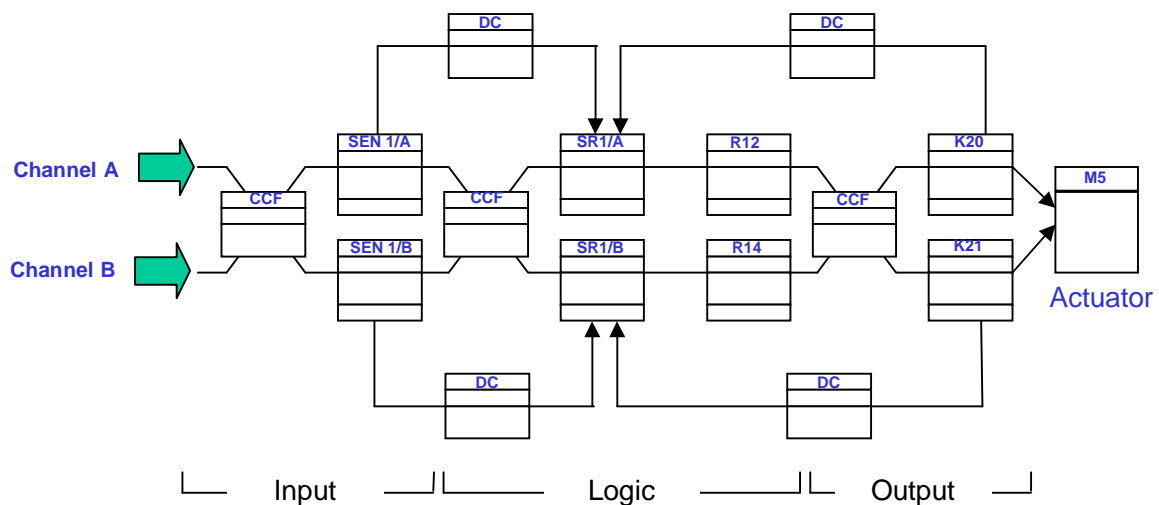
Step 3 – Verification

Definition: verification

Confirmation by examination and provision of objective evidence that the (general) requirements (for safety related systems) have been fulfilled. (EN61508-4 (3.8.1))

Arguably the most practical way of bringing these factors together (Reliable Lifetime Expectancy, Architecture (Category), Diagnostic Coverage (DC) & Possible Common Cause Failures (CCF)) is by a Flow diagrammatic FMEA (Failure Mode & Effect Analysis).

For a simple safety related system this could be laid out diagrammatically as follows and the data added:-



It is intended that such a representation will draw the verifier's attention to the general elements of the safety system and their characteristics to be assessed.

Component Information

Each of the data boxes contains the component information required for the verification.

SEN 1/A

Contains the data for channel A of a redundant half of the safety switch (ref: SEN 1/A).. e.g.:-

Ident:	SEN 1/A
Part:	Rockwell Trojan T15 2 channel Safety Switch
Description:	Channel A of a Cat 4 capable Main gate door interlock with 2 redundant output contacts
No. of operations:	1,000,000
Based on manufactures data sheet	

SR1/A

Contains the data for channel A of a redundant half of the safety relay (ref: SR1/A). e.g.:-

Ident:	SR 1/A
Part:	Rockwell MSR127 Safety Relay
Description:	Channel A of a Cat 4 capable Safety Relay with 3 redundant output contacts.
No. of operations:	1,000,000
Based on manufactures data sheet	

If this element was a programmable function in a safety PLC using validated firmware and hardware, correctly programmed and configured, then it would be impractical to undertake a full evaluation and the manufacturers declared SIL rating should be used as a part of the complete system evaluation.

K20

Contains the data for a motor contactor forming channel A of a redundant half of a series output configuration (ref: K20). e.g.:-

Ident:	K20
Part:	Telemecanique LC1-K0610 Contactor & Overload Assy.
Description:	
Contactor with positively driven contacts & monitoring	
No. of operations:	500,000
Based on manufactures data sheet for AC3	

DC

Contains the data for Diagnostic Coverage for the Input & Output monitoring for each channel. e.g.:-

INPUT DIAGNOSTIC COVERAGE	
Description:	
Mutual monitoring of positively driven contacts of SEN 1/A & B by Safety Relay SR 1	
DC Estimate:	High (99%)
Includes monitoring of contacts & wiring	

OUTPUT DIAGNOSTIC COVERAGE	
Description:	
Monitoring of positively driven contacts of contactors K20 & K21 by Safety Relay SR 1	
DC Estimate:	High (99%)
Monitoring of final drive function	

CCF

Contains the data for any potential Common Cause Failure. e.g.:-

COMMON CAUSE FAILURE	
Description:	
Use of dummy "Tongue" switch actuator to bypass safety switch SEN 1	

Description:
Shorting of wiring at terminal block X12

Analysis of system

From the component information gathered for the parts of the safety system the characteristics of the system may be analysed. In this instance for each of two channels in a redundant (Category 3 / 4 architecture).

In this particular system the operator will open the Main Gate (monitored by SEN1) to remove the finished component whenever the 15 minute process cycle is complete. Therefore the demand on the system is estimated to be 4 ops/hr, 16 hours per day for 350 days a year. Clearly, from the number of operations the system is capable of sustaining and the estimated demand, the estimated life of the system may be established for each channel:-

ANALYSIS OF CHANNEL A	
No. of Ops (Lowest)	500,000
DEMAND (per Year)	$4 \times 16 \times 350^* = 22400$
EST. LIFE (years) (Ops/Demand)	$500,000/22400 = 22$
DIAGNOSTIC COVERAGE (A)	I/P: High (99%) O/P: High (99%)

ANALYSIS OF CHANNEL B	
No. of Ops (Lowest)	500,000
DEMAND (per Year)	$4 \times 16 \times 350^* = 22400$
EST. LIFE (years) (Ops/Demand)	$500,000/22400 = 22$
DIAGNOSTIC COVERAGE (A)	I/P: High (99%) O/P: High (99%)

ANALYSIS OF TOTAL SRCF (Channel A + B)		
Subject	Calculation	Denotation
ARCHITECTURE	2 Channel (Asymmetric)	Cat 3
No. of Ops (Lowest)	500,000	
MEAN EST. LIFE (years) [(Chan A + Chan B)/2]	$(22+22)/2$ $= 22 \text{ years}$	
FACTOR (Use & Environment de-rate)	None (100%)	
REASON for Factoring	Sound working environment anticipated	
MEAN EST. LIFE (Factored)	$22 \times 100\% = 22 \text{ years}$	Medium
DIAGNOSTIC COVERAGE (Lowest)	99%	High
COMMENTS		

Thus the performance achieved by the Safety Related Control Function (SRCF) design is **Category 3** architecture with a **Medium** Life Expectancy with a **High** Diagnostic Coverage.

Finally, the performance achieved by the Safety Related Control Function (SRCF) design must be compared with the required performance level, either as the SIL required or the PL required, as determined in Step 2.

Adapted from EN ISO13849-1 Table 4			Architecture			
Performance Level (PL) [EN ISO 13849]	Safety Integrity Level (SIL) [EN62061]		Cat 1	Cat 2	Cat 3	Cat 4
a		Life expectancy				
b	SIL 1		Med	Low		
c	SIL 1		High	Med	Low	
d	SIL 2			High	Med	
e	SIL 3				High	High
Diagnostic Coverage (DCavg)			None to Low	Medium	Medium	High

In this instance the Safety Related Control Function (SRCF) design with a **Category 3** architecture, **Medium** Life Expectancy and a **High** Diagnostic Coverage can achieve a PL of “d” or a SIL 2. Clearly, if the required performance was “e” or SIL 3 then this could be achieved by selecting components with a **High** Life Expectancy. This could be achieved by selecting contactors K20 & K21 capable of a higher number of operations.

Step 4 – Validation

Definition: validation

*Confirmation by examination and provision of objective evidence that the particular requirements for a **specific intended use** are fulfilled. (EN61508-4 (3.8.2).*

Validation is the activity of demonstrating that the safety-related system under consideration, before or after installation, meets in all respects the safety

requirements specification for that safety-related system. (from EN61508-4 (3.8.2 – Note 3).

This is the final step in the design/manufacture process; ultimately, is the safety related control system and all its functions safe and reliable and fit for purpose in protection the users and all that may be affected by the machinery.

The purpose of Validation is to confirm that both the design and the construction of the safety related parts of the control system meet with:-

- the specification,
- the applicable standards (where applied)
- basic safety principles
- well tried practice
- sound engineering practice

Mechanical, electrical, pneumatic and hydraulic controls must be included in the Validation process.

A Validation plan is required and which must:-

- Confirm compliance with the specification document.
- Confirm the validity of the drawings, time sequence charts, parts lists, etc.
- Confirm the foreseen operational & environmental conditions
- Confirm that Basic Safety Principles have been observed
- Confirm that Well-tried Safety Principles have been observed
- Confirm that Well-tried components have been used
- Review the scope and relevance of the fault assumptions and fault exclusions that have been considered
- Apply all fault simulations, tests and analysis that are necessary
- Confirmation that the documentation supplied to the users is accurate, complete and fit for purpose.

The Validation must be recorded.

Information for Use

All documents shall have titles or names indicating the scope of the contents and should have a revision index (version numbers, etc.) to make it possible to identify different versions of the document.

All documentation shall:

- be accurate and concise;
- be easy to understand by those persons having to make use of it;
- suit the purpose for which it is intended;
- be accessible and maintainable.

Note:

Reference to BS 4884 parts 1 to 3 – “*Technical manuals. Specification for presentation of essential information*” could be helpful.

Design Record Documentation

The design and structure of the safety related parts of the control system must be fully documented to record the considerations included in the system:-.

- safety function(s) provided by the SRP/CS;
- the design rationale (e.g. risk assessment, faults considered, faults excluded, FMEA, etc.);
- the characteristics of each safety function (SIL or PL, Category, Diagnostics, reliability) ;
- environmental conditions considered;
- the CCF's considered;
- measures taken against reasonably foreseeable misuse;
- the technology or technologies used;
- design & software documentation;
- verification & validation records;
- chronological documentation (e.g. a logbook) of the change request procedures including:-
 - identified hazards which can be affected;
 - description of the change request (hardware and/or software);
 - reason(s) for the change request;
 - decision made (and authorization for each decision);
 - re-verification and revalidation;
 - all documents affected by the change request activities;
 - all activities which were carried out during the change process and those responsible.

In general, this documentation is for the manufacturer's internal record purposes and not necessarily be distributed to the machine user in such detail.

User Documentation

Information which is important for the safe use of the safety related control system should be provided to the user. Typically this should include:

- safety function(s) provided by the SRP/CS;
- the design rationale (e.g. faults considered, faults excluded);
- environmental conditions considered;
- the performance level (either SIL or PL);
- the limits of the safety-related parts;
- essential information for maintaining the integrity of the SRP/CS (e.g. in the event of modification, maintenance and repair);
- clear descriptions of the SRP/CS, interfaces and protective devices;
- response time;
- operating limits (including environmental conditions);
- indications and alarms;
- muting and suspension of safety functions;
- control modes;
- maintenance & maintenance check lists;
- means for easy and safe trouble shooting;

Abbreviations

Cat	Category (based on EN954-1)
CCF	Common Cause Failure(s)
DC	Diagnostic Coverage
DC _{avg}	Average diagnostic coverage
EMC	Electromagnetic Compatibility
FMEA	Failure Mode & Effect Analysis
HFT	Hardware fault tolerance
I/O	Input/Output
<i>PFH_D</i>	Probability of dangerous Failure per Hour
PL	Performance level
PL _r	Performance level required
PLC	Programmable Logic Controller
MTTF	Mean Time To Failure
MTTF _d	Mean Time To Dangerous Failure
SFF	Safe Failure Fraction
SIL	Safety Integrity Level
SRECS	Safety-Related Electrical Control System
SRCF	Safety-Related Control Function
SRP/CS	Safety-related part of a control system

Notes About the Author:

The author of this report is Robin J Carver who is a qualified safety systems engineer and a Chartered Health and Safety Practitioner with over 40 years experience in the design and assessment of industrial machines.

Robin is involved in aiding and assisting companies with the safety of machinery including CE Marking, PUWER98 and general aspects of workplace safety.

A member of the British Standards Institution, Robin is a BSI committee member, serving on the BSI Safety of Machinery – MCE/003 and the Safety of Machinery, Electro-technical Aspects - GEL/44 panels.

Robin is a Member of the Institute of Engineering and Technology, Member of the Institute of Measurement & Control, a Chartered Member of the Institute of Occupational Health and Safety and Member of the International Institute of Risk and Safety Management and is committed to a programme of “continued professional development”.