CAPIEL

european coordinating committee of manufacturers of electrical switchgear and controlgear

January, 2017

CAPIEL WHITE PAPER

Edition 2 2017-01-04

Low voltage switchgear and controlgear - safety aspects

Prepared by CAPIEL PG5

- CAPIEL is the Coordinating Committee for the Associations of Manufacturers of Switchgear and Controlgear equipment's for industrial, commercial and similar use in the European Union, that work in the range of voltages until 1 kV a.c. of 1,5 kV d.c.
- The objective of CAPIEL is to promote and to support the common technical, industrial, economical, environmental and political interests of the European low voltage switchgear and controlgear industry (products, systems and assemblies)
- CAPIEL members are national associations representing small, medium and large-sized companies that in total employ more than 100.000 people directly in Europe. Their scope covers all the equipment, product fittings, systems installed and services required for operations of low voltage and control gear (products, systems and assemblies)
- CAPIEL plays an active role in driving emerging technologies and in supporting the values of ethical, environmental, health and safety, innovation for sustainability, quality and fair competition; in accordance with the imperatives of the Treaty of Rome

1 Purpose and audience of this document

The purpose of this document is to

- Promote the use of CAPIEL products in safety applications
- Clarify and harmonize information needed to use CAPIEL products in safety applications

The intended audience for this document is manufacturers of CAPIEL products as well as users.

CAPIEL - 17 rue de l'Amiral Hamelin - 75016 PARIS - France
Téléphone : +33.1.45.05.71.62 - Fax : +33.1.47.04.68.57, Email : deyraud@gimelec.fr

2 Introduction

The Machinery Directive 2006/42/EC has applied since 29th December 2009.

Machine manufacturers should consider how they can demonstrate compliance concerning safety related parts of control system with the Machinery Directive (2006/42/EC) using the following harmonized EN Standards:

- EN ISO 13849
- EN 62061

- To ensure these EN Standards can be applied effectively, CAPIEL manufacturers must provide functional safety related data depending on the type of component to machinery manufacturers, in order to help them to design suitable safety related parts of control systems.
  This document is focused on machinery applications.

- The format of the data provided in this document is relevant for use in the calculation methods given in EN ISO 13849, EN 62061 and EN 61508.

3 Safety components that fall within CAPIEL scope

The Machinery Directive (2006/42/EC) gives the following definition of a safety component:

"Safety component" means a component:
1. which serves to fulfil a safety function,
2. which is independently placed on the market,
3. the failure and/or malfunction of which endangers the safety of persons, and
4. which is not necessary in order for the machinery to function, or for which normal components may be substituted in order for the machinery to function

When a manufacturer declares a product as being a "safety component", the product shall satisfy all applicable requirements of the Machinery Directive.

However, some CAPIEL products may not meet the above definition for a "safety component", but may nevertheless have documented features or functionality that can be used by the machine builder to determine whether they are suitable for functional safety related use in a particular application.

4 Information needed for safety verification process

For each implementation level, different data is required in order for the machine manufacturer to verify the required PL/SIL of the safety functions. The following table shows the data required.

Information to be provided by product manufacturer	Implementation levels							
	Safety control system		Safety subsystem		Safety element		Generic element	
	TB	WB	TB	WB	TB	WB	TB	WB
SIL and/or PL	■	■						
SILCL and/or PL			■	■				
PFH_D and/or PFD	■	■	■	■				
Operation limit		1)		1)		2)		2)
$MTTF_D$ or MTTF and RDF					■			
B_{10D} or B_{10} and RDF						■		
MTBF							□	
B_{10}								□
T_M	■	■	■	■	■	■	□	□

■ *Mandatory field, data required,*

□ *Optional field, data optional (application-specific),*

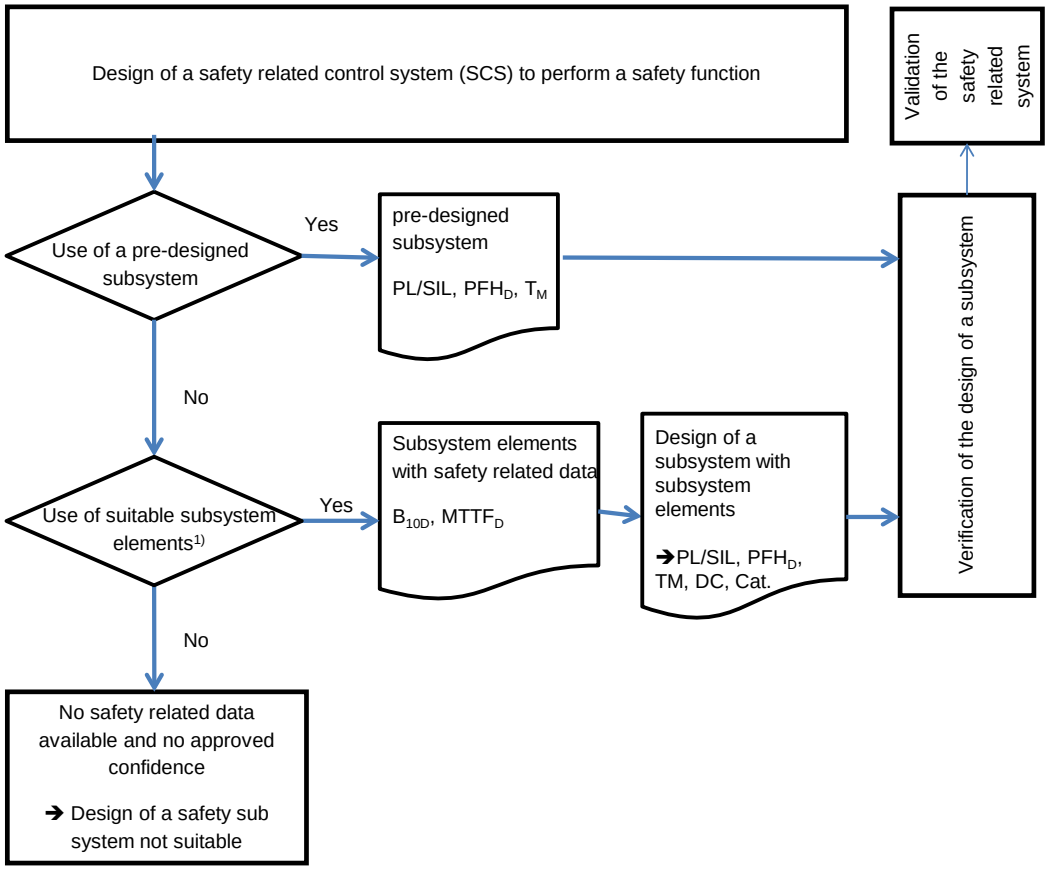
TB *Time based, e.g. electronic products*

WB *Wear based, e.g. electro-mechanical products*

PL *Performance Level (EN ISO 13849)*
SIL *Safety Integrity Level (EN 61508)*
SILCL *Safety Integrity Level Claim Limit (EN 62061)*
PFH_D *Probability Failure per Hour (EN 62061)*
T_M *Mission time (EN ISO 13849)*
MTBF *Mean Time Between Failure (EN ISO 13849)*

$MTTF_d$ *Mean Time To Dangerous Failure (EN ISO 13849)*
RDF *Ratio of Dangerous Failures*
B_{10} *10% of the devices failed (EN ISO 13849)*
B_{10d} *10% of the devices failed dangerous (EN ISO 13849)*
PFD *Probability of failure on Demand (EN 61511)*
Operation limit *maximum number of operations that is used in the calculation on the PFH_D*

1) PFH_D value valid up to the operation limits of the different components
   Example: electrical life time, number of operations per hour, 50% of nominal current
2) Operation limits as declared by the manufacturer



1) Note: subsystem elements corresponding to the CAPIEL Brochure are safety elements (with safety related date) and generic elements (without safety related data).

Device	**Complexity (IEC 61508)**	**Criteria/Requirements**
Electro-mechanical devices	Type A [1)]	Developed in accordance to a product standard (IEC 60947 series) providing safety related data (B_{10D}, T_M) Additional requirements according ISO 13849-2 using basic safety principles, well tried components, fault exclusion
Electronic devices	Type B [1)]	Developed in accordance to a safety standard (ISO 13849, IEC 62061, IEC 61508) ($MTTF_D$, T_M)

1) IEC 61508-2

7.4.4.1.2 An element can be regarded as type A if, for the components required to achieve the safety function
a) the failure modes of all constituent components are well defined; and
b) the behaviour of the element under fault conditions can be completely determined; and
c) there is sufficient dependable failure data to show that the claimed rates of failure for detected and undetected dangerous failures are met (see 7.4.9.3 to 7.4.9.5).

7.4.4.1.3 An element shall be regarded as type B if, for the components required to achieve the safety function,
a) the failure mode of at least one constituent component is not well defined; or
b) the behaviour of the element under fault conditions cannot be completely determined; or
c) there is insufficient dependable failure data to support claims for rates of failure for detected and undetected dangerous failures (see 7.4.9.3 to 7.4.9.5).
NOTE *This means that if at least one of the components of an element itself satisfies the conditions for a type B element then that element will be regarded as type B rather than type A.*

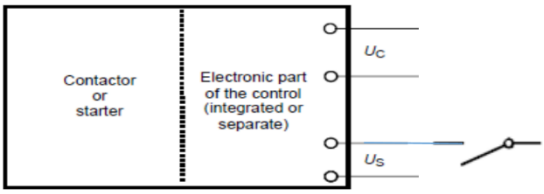
5 Safety elements

Safety evaluation of electromechanical devices containing electronics.

1. If the electronics has no impact on the safety integrity, the device is considered to be a mechanical device only. (B_{10D})

   Example: Contactor with electronic controlled coil

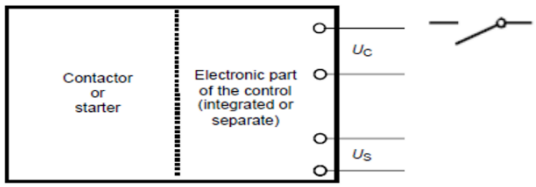
   The position of rest for a contactor is the safe state, and the magnet cannot be kept closed without supply voltage.



2. If the electronics does have an impact on the safety integrity, both the mechanical part and the electronic part have to be considered. ($MTTF_D$+B_{10D} or λ_D)

   Example: Contactor with electronic controlled coil

   The magnet is operated through the electronic.



U_c= control voltage
U_s= supply voltage

6 Failure rates of components for high demand application

6.1 Terms/definitions

reliability (performance)
ability of an item to perform a required function under given conditions for a given time interval

NOTE The useful life may be expressed in number of operations.
[IEC 60300-2;2004 3.9]

overall lifetime
lifetime of the device which should not be exceeded in order to maintain the validity of the estimated failure rates due to random hardware failures

NOTE 1 Overall lifetime covers also periods of non-use e.g. storage. The overall lifetime is expressed in number of years

NOTE 2 It corresponds to T_1 according to EN 62061 and to T_M according to EN ISO 13849-1.
[EN 62061:2005]

functional safety
part of the safety of the machine and the machine control system. It depends on the correct functioning of the safety control system, other safety-related systems, and external risk reduction facilities.
[EN 62061:2005]

dangerous failure
failure of a safety control system that has the potential to cause a hazard or non-functional state.
[EN 62061:2005]

probability of dangerous failure per hour PFH_D
average probability of dangerous failure within 1h.
[EN 62061:2005, 3.2.28]

probability of failure on demand PFD
average probability of failure on demand PFD_{avg}
[EN 61511-1, 3.1]

systematic failure
a failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors
NOTE 1 – Corrective maintenance without modification will usually not eliminate the failure cause.
NOTE 2 – A systematic failure can be induced at will by simulating the failure cause.
[IEV 191-04-19]

6.2 Durability testing

In order to address random hardware failure, the method is based on results given by continuous monitoring of the devices under the appropriate durability tests given by the product standard. (e.g. IEC 60947-4-1, Annex K Contactors)

Table 1 – Typical failure modes of switching devices

Failure modes	Characteristics for a switching contact
Failure to open	current remaining after the time for normal opening operation
Failure to close	no current in one or more poles after the normal time to close
Insulation failure	insulation failure between any poles or the frame and the poles

6.3 Evaluation of Data

The reliability data are obtained by modelling the test result data from the durability testing with the Weibull distribution according to EN 61649 using a confidence level of 60%.

6.4 Reliability data

The useful lifetime in terms of number of operation cycles is obtained with the lower limit value of B_{10} by the graphical method or the numerical method.
The failure rate per operation λ_u can be calculated using the simplified formula.

$$\lambda_u = 1 / (10 \times B_{10})$$

For a given application where the number of operation per hour *c* is lower than the maximum switching rate, the failure rate, λ, expressed in “per hour”, is given by the failure rate, expressed in “per operation”, λ_u, multiplied by *c*:

$$\lambda = \lambda_u \times c$$

The value for RDF (ratio between dangerous failures and total failures) for each of the failure modes of Table 1 is defined by the relevant product standard. Table 2 gives typical values for RDF. When RDF is determined by the manufacturer, the minimum percentage allowed for the value of RDF is 20%. In the case where no data is available and it is not possible or practicable by these methods to determine the value for RDF then, 50% of the failures should be used.

Table 2 – Typical B_{10D} values for electromechanical components (operating in high or continuous demand mode)

A failure to open the circuit is considered as a dangerous failure in this table. Values are based on tests made in laboratories by CAPIEL manufacturers. The values given are target values that typical components are expected to achieve based on testing, which can be used if the supplier has not provided a value. It is the responsibility of the manufacturer to provide the actual values.

Electromechanical components	**Contact load, utilization category**	**Typical B_{10} values**	**Typical B_{10D} values**	**RDF**	
(only devices with positive opening contacts allowed)					
EMERGENCY STOP DEVICES (push buttons) - Turn-to-release (and key release) - Pull-to-release	1) 1)	20 000 20 000	100 000 100 000	20% 20%	
Cable-operated switches for EMERGENCY STOP function	1)	20 000	100 000	20%	
Hinge switches	1)	20 000	100 000	20%	
Pushbuttons (momentary)	2)	20 000	100 000	20%	4)
Position Switches - Standard version - with separate actuator - with solenoid interlocking, spring forced lock	2) 1) 1)	4 00 000 400 000 200 000	20 000 000 2 000 000 1 000 000	20% 20% 20%	4) 4) 4)
-Contactor Relays	3) AC-15/-14	10 000 000 200 000	20 000 000 400 000	50% 50%	5) 6)
Contactors / Motor Starters - for motorswitching ≤ 100A	3) AC-3	10 000 000 1 000 000	20 000 000 1 300 000	50% 73%	5) 6)
Contactors / Motor Starters - for motorswitching >100A, ≤500A	3) AC-3	1 500 000 300 000	3 000 000 400 000	50% 73%	5) 6)

1) mainly limited by mechanical wear
2) mainly limited by contact wear
3) maximum value of B_{10} if the current is lower than 1% of rated current
4) Ratio of dangerous failure: 50% at usage of the NO contact (one positively driven contact shall be used additionally at least in a redundant architecture; the single use of a NO contact is not allowed)
5) The diagnostic coverage of the subsystem incorporating a contactor with mirror contacts can be 99% if an appropriate fault reaction function(s) is provided
6) The values given are based on 50% of rated current (based on the common practice for output devices used in safety related systems)

The B_{10D} value used in ISO 13849-1:2015 can be determined as follows.

$B_{10D} = B_{10}/RDF$

Ratio of dangerous failures is minimum 20%

6.5 Calculation example

A movable protective guard is monitored by means of a position switch with a separate actuator.
This guard is opened four times per hour.

The total failure rate of the position switch is as follows:
$\lambda_D = 0.1 * C / B_{10D}$ [failure / h]
$\lambda_D = 0.1 * 4 / 1\,000\,000 = 4 * 10^{-7}$ [failure / h]

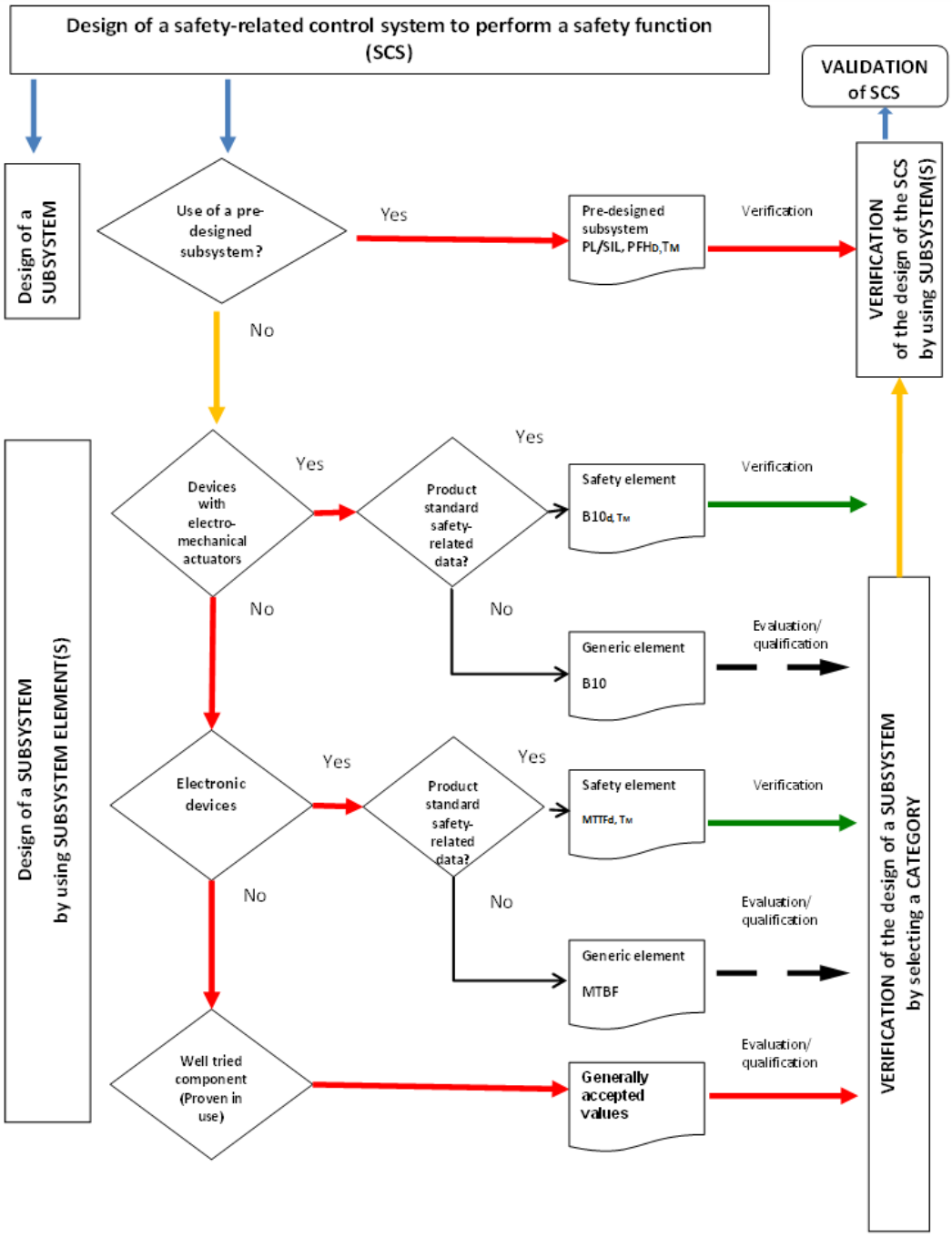
7 Operating in low demand mode

In low demand applications, it is recommended that 100 FIT is used as the dangerous failure rate for electromechanical components, if the supplier has not provided a value.

8 Standards referred to in this document

EN 61508	Functional safety of electrical/electronic/programmable electronic safety-related systems
EN 62061	Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems
EN ISO 13849-1	Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design
EN ISO 13849-2	Safety of machinery - Safety-related parts of control systems - Part 2: Validation
EN 60947-x-x	Low-voltage switchgear and controlgear –
EN 61649	Weibull analysis

ANNEX



= Manufacturer of the machine

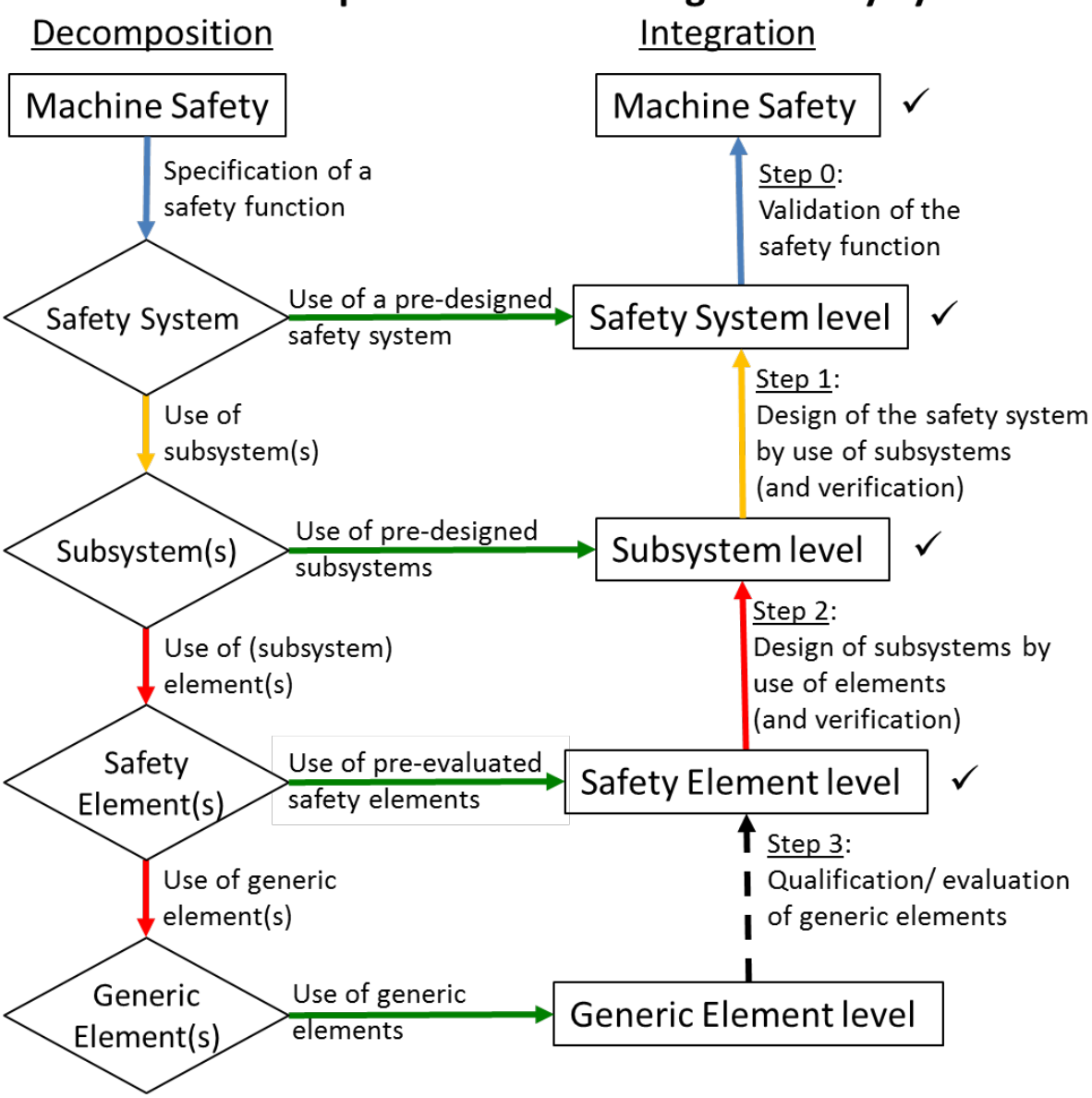
= Designer of the SCS

= Designer of the subsystem

= Use of entities that are designed by the manufacturer of the entity, all activities below this line are done by the manufacturer of the entity, the instructions of the manufacturer have to be obeyed

= can actually only be done by the manufacturer of the element

Activities and responsibilities to design a Safety System



Typically done by:

✓ = all activities are done till here

- = Manufacturer of a machine
- = Designer of a safety system
- = Designer of a subsystem
- = Use of entities that are designed by the manufacturer of the entity, all activities below this line are done by the manufacturer of the entity, the instructions of the manufacturer have to be obeyed
- = can actually only be done by the manufacturer of the element