CHEMICAL ENGINEERING TRANSACTIONS

VOL. 48, 2016

A publication of
AIDIC
The Italian Association
of Chemical Engineering
Online at www.aidic.it/cet

Guest Editors: Eddy de Rademaeker, Peter Schmelzer
Copyright © 2016, AIDIC Servizi S.r.l.,
ISBN 978-88-95608-39-6; **ISSN** 2283-9216

DOI: 10.3303/CET1648084

“Process Safety Architecture” System Neutral Solution Comparison

Franz Handermann
Siemens AG, Oestliche Rheinbrueckenstr. 50, 76187 Karlsruhe, Germany
franz.handermann@siemens.com

There are many different solutions of safety systems on the marked. We will see the difference and advantage of the architecture of safety related components also the corresponding definition in the international safety standards. The aim is to give an overview of the safety life cycle from the analysis, realization to the operation phase and the basic knowledge for future decisions of safety related solutions.

1. Safety, Risk and Failures

Safety is freedom from unacceptable risk. Risk is the probability that an undesirable event will occur. It involves two questions: 1) How often could it happen? 2) What are the consequences if it does happen?
Studies and failure analysis have shown that most incidents are caused by incomplete or faulty specifications in safety automation very early in the project phase. Fortunately, there are international safety standards that will help guard against these systematically human failures.

2. International Standard for Functional Safety

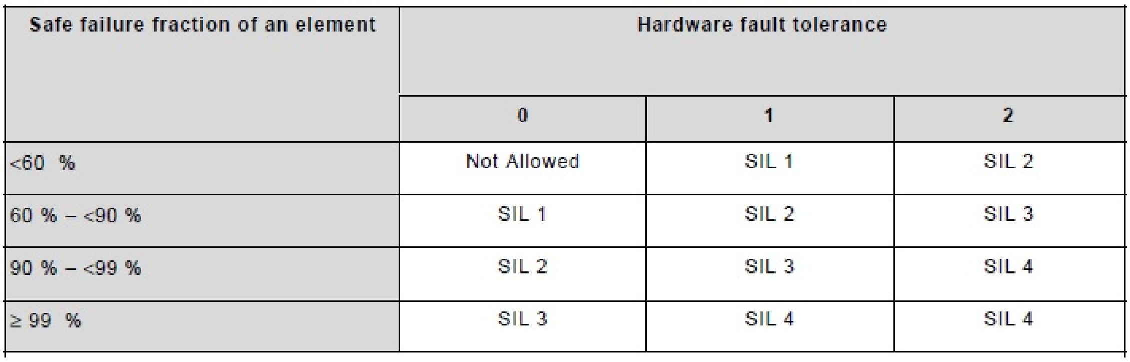
The International Electrotechnical Commission (IEC) published the international standard IEC 61508, which is the umbrella standard for “functional safety of electrical/electronic/programmable electronic (E/E/PE) safety-related systems”. This standard contains the definition of and rules for developing safety-related devices for all business sectors.
Also the international standard IEC 61511, which is the sector specific standard for “functional safety – safety instrumented systems (SIS)” for the process industry sector was created as a “child” standard of IEC 61508. This standard is mainly a guideline on how to use and develop a process safety application.
Manufacturers and suppliers of safety related devices follow the IEC 61508 standard, while safety instrumented system designers, integrators and end users follow IEC 61511.

3. IEC 61508 safety related development of SIS components

In the normative part two and three of IEC 61508 provides the guidelines and definitions related to the development of safety related components. A main requirement is the hardware fault tolerance (HFT) and the safe failure fraction (SFF).
There is a variety of different solutions for safety systems on the market. The oldest safety systems are voting-based, while the newer, more modern safety systems are based on a high diagnosis. The developments are normally with HFT=0 and SFF>99% or with HFT=1 and SFF>90%. To fulfill an SFF>99%, the diagnosis must be very detailed and of high quality.
Siemens used both paths in its development work. For components with the HFT=0 and SFF>99% Siemens developed its own microprocessors (ASIC) with well-known failure modes. In the ASIC a diversity code runs in different timer. At the end a very high quality diagnosis checks the identical results. We can identify this solution as a diagnosis based safety solution with a software fault tolerance of SFT=1.

Please cite this article as: Handermann F., 2016, �because"process safety architectures‟ system neutral solution comparison, Chemical Engineering Transactions, 48, 499-504 DOI:10.3303/CET1648084

Table 1) IEC 61508-2, Maximum allowable safety integrity level (SIL) for a safety function (SIF) carried out by a type B safety-related element or subsystem



Safe failure fraction of an element	Hardware fault tolerance		
	0	1	2
<60 %	Not Allowed	SIL 1	SIL 2
60 % – <90 %	SIL 1	SIL 2	SIL 3
90 % – <99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

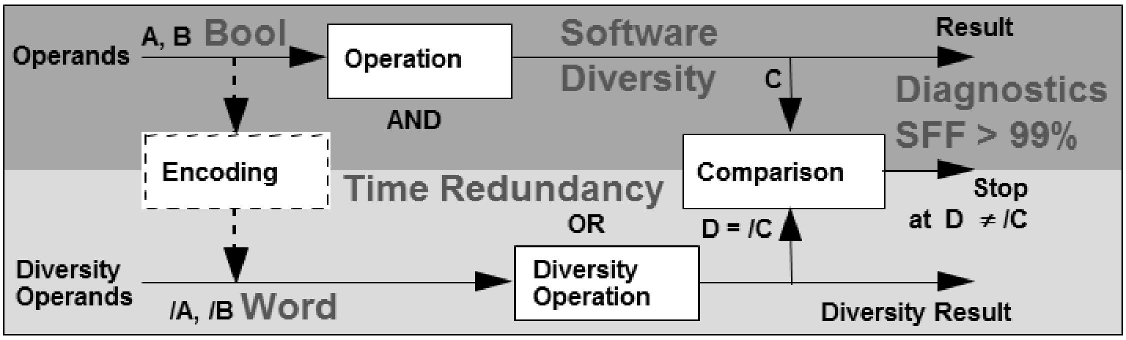


Figure 1) Internal structure SIMATIC controller

On the other hand most safety systems with an HFT=1 use standard microprocessors that are available on the market and that are also used in computers or home appliances.
The same operating system and identically compiled safety application run in all microprocessors. Additional diagnostics check to ensure that the same results are obtained in all microprocessors. If there is a difference the diagnosis switches the components or the faulty parts to a safe state.

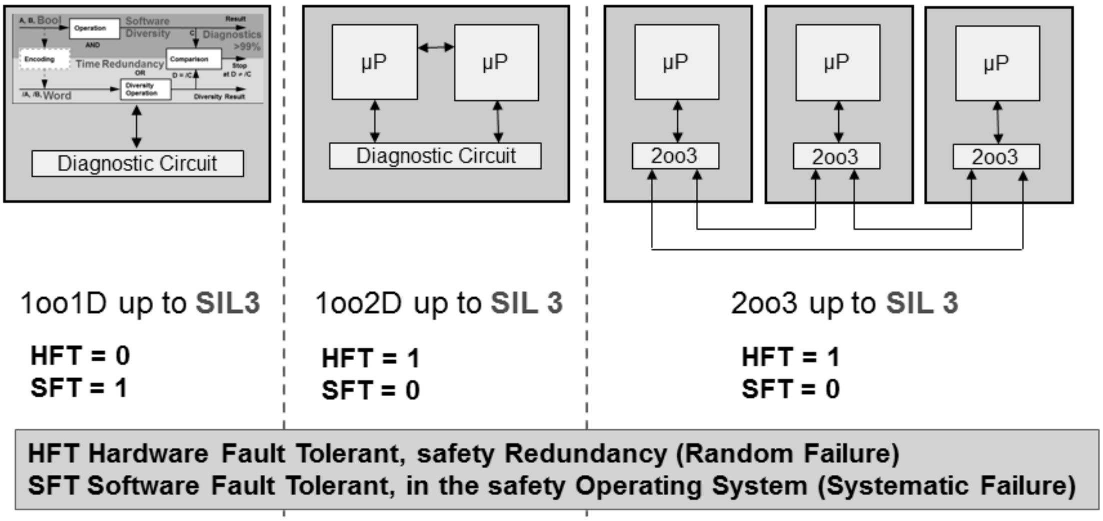


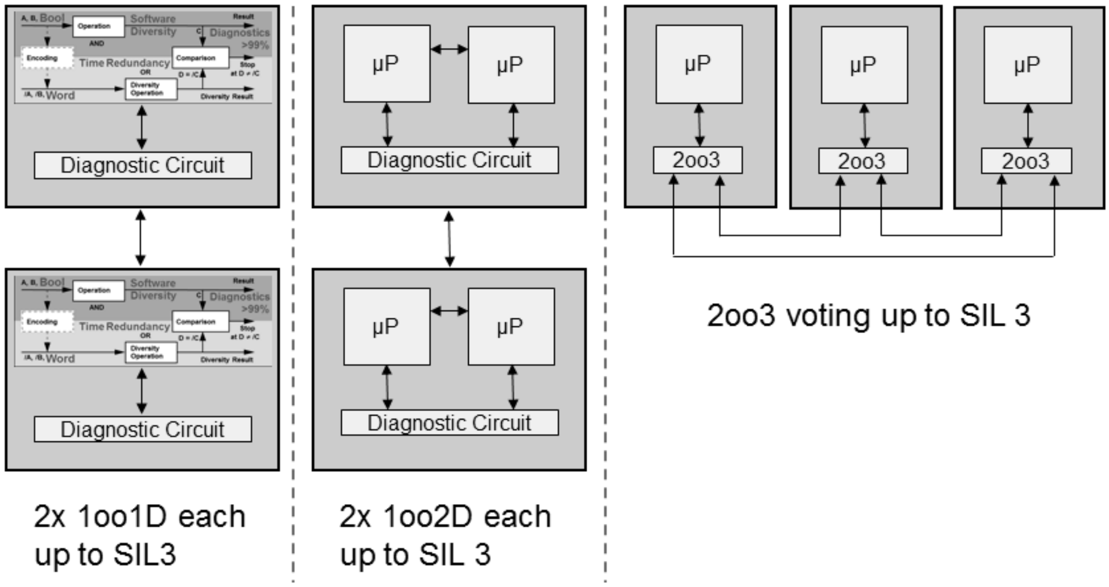
Figure 2) Different architectures of safety related controller

In the illustration above, the following IEC 61508 architectures are shown 1oo1, 1oo2, 2oo2, 1oo2D, 2oo3, 1oo3. Requirements like dual, triple, TMR, quad, QMR are basically marketing names from companies. They are not real safety requirements. We can find no clear description or definition of what is behind these abbreviations.

The question is: Which are the correct requirements for safety applications and the safety components used?

It makes a lot of sense to focus on specifying the necessary safety integrity of the system from the input to the output, rather than falling in the marketing trap of tying a design to a specific technology.

For continuously running plants, additional availability requirements apply. Thus, the requirement might be a one fault tolerance structure at the controller and communication level. Finally inputs and outputs, field instrumentation, and all availability requirements according to the criticality of the loop (SIF) should be clearly indicated.



2oo3 voting up to SIL 3

2x 1oo1D each up to SIL3

2x 1oo2D each up to SIL 3

Figure 3) Different architectures of safety related and available controller

In the architectures shown above, diagnostic- based safety systems (SIS) are used. In this case, an SIL 3 certified controller is used. A second controller is in 2oo2 “hot stand by” - but only for the availability. Any failure in one controller can be tolerated without tripping the plant.

The voting- based safety systems (SIS) are in a 2oo3 structure. The system needs two controllers with the same results to ensure that the safety resulting output can be trusted. The third controller is for availability.

It is also not allowed to run a voting system 2oo3 unlimited with one internal failure like only two running controllers or a failure in any safe output loop.

A 1oo2D controller cannot be run with only one microprocessor. The controller must shut down if there is an internal failure because the controller is a SIL 3 certified component.

4. Safety Life Cycle

Both safety standards follow a safety life-cycle. IEC 61508 and IEC 61511 include a “management of functional safety” with the requirements of the organization, risk evaluation, planning, implementation, assessment and SIS configuration management.

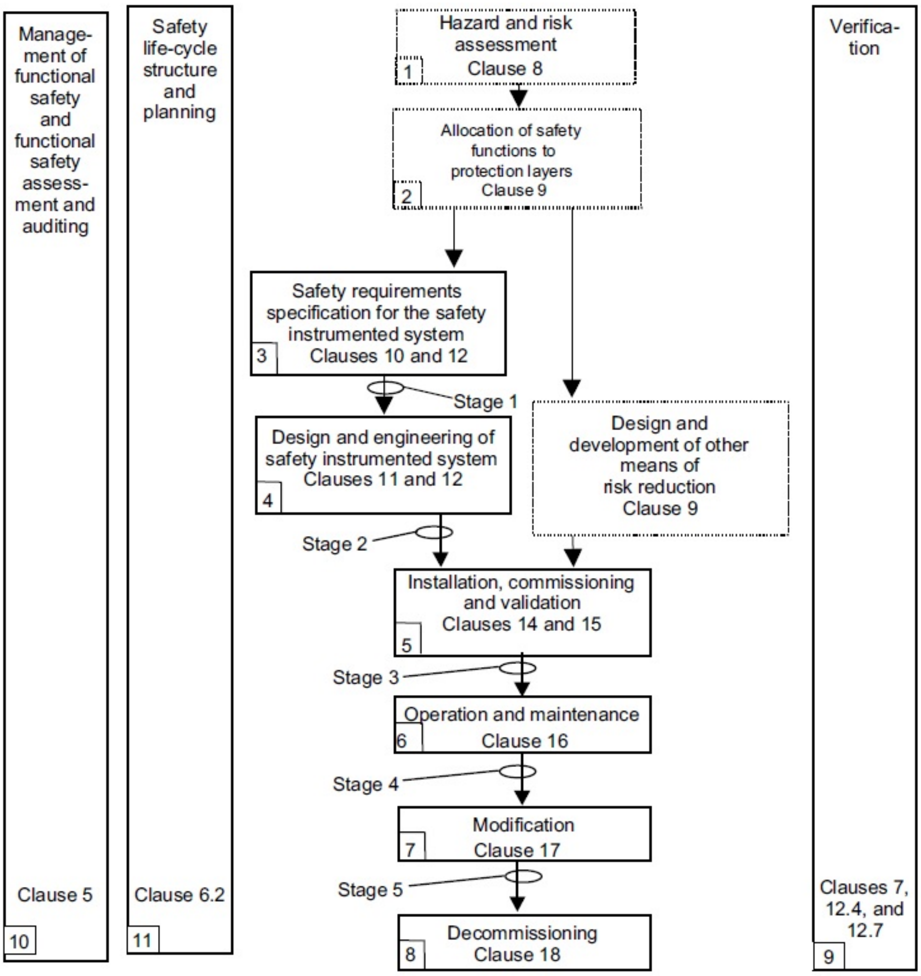

Manage-ment of functional safety and functional safety assess-ment and auditing
Clause 5
10
Safety life-cycle structure and planning
Clause 6.2
11
Hazard and risk assessment
Clause 8
1
Allocation of safety functions to protection layers
Clause 9
2
Safety requirements specification for the safety instrumented system
Clauses 10 and 12
3
Stage 1
Design and engineering of safety instrumented system
Clauses 11 and 12
4
Design and development of other means of risk reduction
Clause 9
Stage 2
Installation, commissioning and validation
Clauses 14 and 15
5
Stage 3
Operation and maintenance
Clause 16
6
Stage 4
Modification
Clause 17
7
Stage 5
Decommissioning
Clause 18
8
Verifica-tion
Clauses 7, 12.4, and 12.7
9

Figure 4) IEC 61511-1, SIS safety life-cycle phases

The safety life-cycle is split into three parts: the analysis (phase 1-3), the realization (phase 4-5) and the operation (phase 6-8).

5. Defining the required safety level (SIL)

The first requirement is to identify the process risks through a process hazard and risk analysis (PHA). This risk is then compared to the maximum level of risk that would make such operation acceptable. Independent protection layers (non SIF) are then applied to reduce the risk. If the targeted acceptable risk level is not achieved, then SIF can be implemented to reduce or eliminate the gap.
The risks of the hazards we define the safety integrity level (SIL) that means the allocation about a necessary risk reduction down below a tolerable rest risk.

Table 2) IEC 61511-1, Safety integrity requirements: Average probability of dangerous failure on demand PFD$_{avg}$

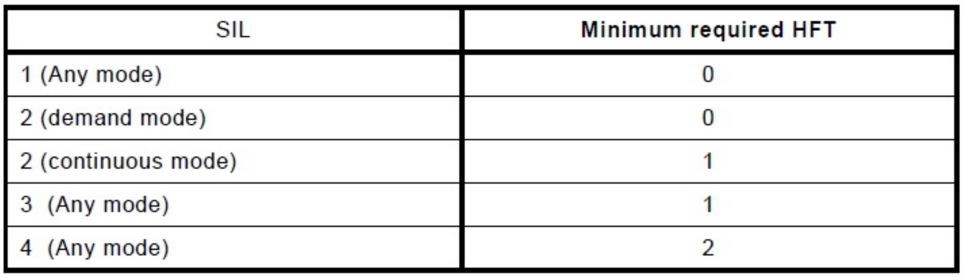
DEMAND MODE OF OPERATION		
Safety integrity level (SIL)	PFD$_{avg}$	Required risk reduction
4	$\geq 10^{-5}$ to $< 10^{-4}$	>10 000 to ≤100 000
3	$\geq 10^{-4}$ to $< 10^{-3}$	>1 000 to ≤10 000
2	$\geq 10^{-3}$ to $< 10^{-2}$	>100 to ≤1 000
1	$\geq 10^{-2}$ to $< 10^{-1}$	>10 to ≤100

This is because we could use different risk reduction measures to achieve this necessary risk reduction – for example, mechanical protection systems, safety instrumented system (SIS).
If we use an SIS we can do the SIL classification for each safety loop “safety instrumented function” (SIF).
The most important document in this process is the “safety requirement specification” (SRS). You can find all definitions and requirements of all SIFs with the required SIL. An SRS should include definitions like the safety state of the loops, the common cause failures, the demand rate, the proof-test intervals, the response time, the trip points, the spurious trip rate (STR), interfaces between SIS and the “basic process control system” (BPCS), mean time to repair (MTTR), environmental conditions, application software,…etc.
The SRS is the interface between the process world and the automation world.
With this document we can start to develop and engineer our SIS solution.

6. Achieving the required safety level (SIL)

The IEC 61511 standard provides three options for achieving the safety requirements. The components and subsystems selected as part of a safety instrumented system (SIS) for SIL 1 to SIL 3 applications must be in accordance with
-Development according to IEC 61508-2 and IEC 61508-3, as appropriate, or
-Requirements for hardware fault tolerance (HFT) or
-Requirements for the selection of components and subsystems based on prior use.

The hardware fault tolerance (HFT) is by definition the number of failures that can be tolerated without losing the safety function.



SIL	**Minimum required HFT**
1 (Any mode)	0
2 (demand mode)	0
2 (continuous mode)	1
3 (Any mode)	1
4 (Any mode)	2

Table 3) IEC 61511-1, Minimum hardware fault tolerance HFT requirements according to SIL

Architectures like 1oo1, 1oo2, 2oo2, 2oo3 are frequently used to fulfill the required SIL (risk reduction) for the safety loops (SIF) and to fulfill the additional requirement, based on availability.
In a continuously running plant, tripping the production because of an internal failure of automation components is not allowed also not according an internal failure of the safety system (SIS).
For example if the requirement is a risk reduction of three orders of magnitude (SIL 3), then an SIL 3 SIF is required. This cannot be achieved with a single field instrument; a redundant architecture is needed to archive SIL 3. This could be achieved with redundant HFT=1 SIL 2 certified sensors. These should be voting sensors in the architecture 1oo2 structure and we need both to achieve the required safety performance or SIL.
There are some limitations to this kind of application - such as time between inspections, maintenance, operating system, etc. However, all such safety data of components must be published in the safety manual of the component.
If the requirement is SIL 3 together with a high availability of the loop we need maybe three sensors two for safety and a third for availability. The structure of the safety loop is now 2oo3 which can degrade after an internal failure into a 1oo2 without tripping.
After engineering the architectures of the SIF we need to calculate the probability of failure on demand (PFD) and verify the required SIL from the SRS with our engineered architecture (*Table 2, IEC 61511-1*).

7. SIF architecture comparison

In the following architecture examples we can see the flexibility and scalability of modern safety systems.
The internal structure of the system allows a mixing of all architectures in the field instrumentation level as required. The processing of the field values in the safety automation system is also flexible with certified function blocks for all usable architectures.
2oo3 architectures are also frequently used if the field instrumentation requires a proof test interval of the components that is less than the allowed minimum maintenance interval of the plant. Now the proof test can

be realized without a loop trip. Normally certified functions are available in the safety systems for all these architectures.

Be careful about availability requirements from the end customers because the bottleneck in safety automation relates mainly to the limits in networks, power supplies and fuse distributions.

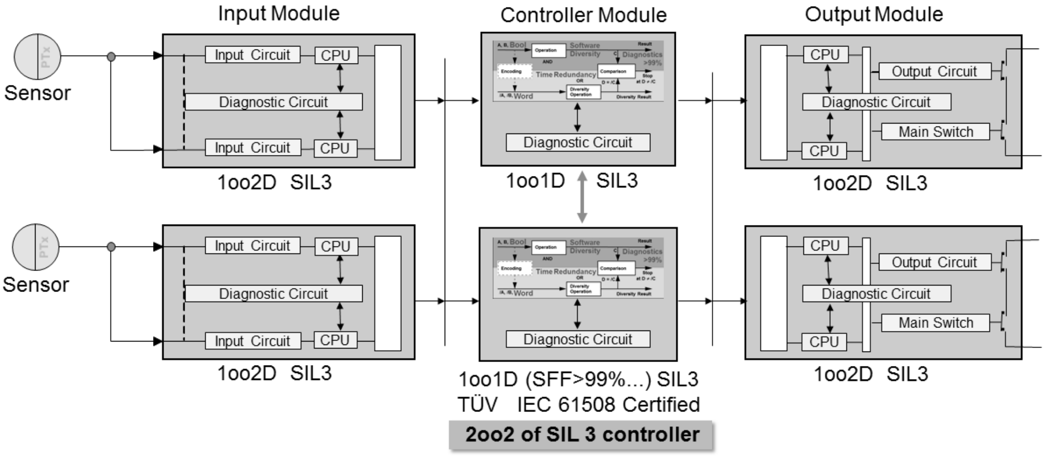


Figure 5) Example of a redundant safety instrumented function (SIF)

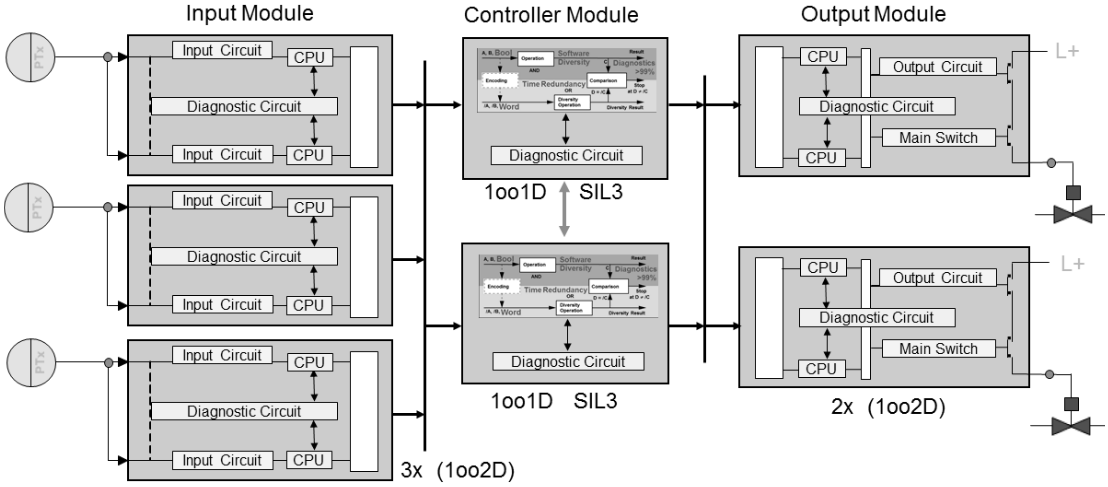


Figure 6) Example of a flexible redundant safety instrumented function (SIF)

8. Conclusions

For safety applications it is better to use diagnosis. Diagnosis can reduce dangerous failures of components in your SIS.

A certified automation system according to IEC 61508 is essential for a safety application.

Safety and availability are independent issues. Redundancy could be used for reliability in a hot standby mode. Field instrumentation voting for safety is independent of device voting for availability.

Use a flexible modular redundancy concept with a high level of flexibility and scalability.

Follow the requirements according to IEC 61511.

Reference

INTERNATIONAL ELECTROTECHNICAL COMMISSION
IEC 61508 edition 2.0 2010 Functional safety of E/E/PE electronic safety-related system
IEC FDIS 61511 edition 2.0 2015 Functional safety – SIS for the process industry sector