

Diverse redundancy used in SIS technology to achieve higher safety integrity

Edgar C. Ramirez
Safety System Business Driver

ABB Inc.
A110, 4411 6th Street SE
Calgary, Alberta, Canada T2G 4E8
Tel:+1403 225 5501
E-mail:edgar.c.ramirez@ca.abb.com

Abstract

SIS logic solver technologies use hardware fault tolerance to improve safety integrity. Higher integrity levels can usually be achieved by implementing identical or diverse redundancy. Diverse redundancy refers to the use of two or more different systems, which are built using different components, algorithms, electronics, design methodology etc. to perform the same task. One benefit of diverse redundancy is the increased capabilities to reduce common mode and systematic failures such as those caused by design flaws. The use of diversity is an effective defense against hidden dangerous faults. Logic solver technologies that use internal diverse redundancy have been developed for applications up to SIL 3

1. Introduction

Diverse redundancy is one of the mechanisms recommended in the IEC 61508 and IEC 61511 standards to increase safety integrity of programmable electronic systems, including logic solvers and field devices. This paper presents a brief analysis of the effects of diversity on the performance of safety related systems is presented as compared to observed performance of alternative technologies. The discussion also covers effects on availability. A summary of the requirements to achieve safety integrity is presented, followed by a discussion on how diverse redundancy can improve the safety integrity, illustrated with an example.

2. How SIS technologies achieve high integrity

There are four main requirements to satisfy in order to achieve safety integrity¹ required to reduce risks in processes through the use of safety instrumented functions [2]: hardware safety integrity, measured in terms of probability of failure on demand² (PFD), system behavior in detection of a fault, constraints from architecture, and control of systematic failures.

- Hardware safety integrity refers to the ability to control dangerous hardware random failures, and is expressed as a PFD value.
- Safety-related systems need to be capable of taking fail-safe action, which is a system's ability to react in a safe and predetermined way (e.g. shutdown) under any failure mode.
- Any constraints resulting from the complete system architecture must be assessed, and the implications on the SIL rating documented. Maximum SIL rating is limited by Safe Failure Fraction (SFF) and Hardware Fault Tolerance, according to Table 3 in [2] shown below.
- Systematic safety integrity refers to failures that may arise due to the system development process, safety instrumented function design and implementation, including all aspect of its lifecycle safety management.

Table 1. Hardware safety integrity: architectural constraints on type B³ safety-related subsystems (Table 3 in [2]).

Safe failure fraction SFF	Hardware fault tolerance (see note)		
	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

Note: A hardware fault tolerance of N means that N + 1 faults could cause a loss of the safety function

¹ Safety integrity is the probability of a safety-related system satisfactorily performing the required functions under all the stated conditions within a stated period of time [1].

² In this document the discussion centers on processes operating in the low demand mode of operation, as defined in [7], which is the most common case considered for safety related systems in the process industries.

³ Type B subsystems are those for which: the failure of at least one component is not well defined; or the behavior of the subsystem under fault conditions cannot be completely determined; or there is insufficient dependable failure data from field experience to support claims for rates of failure for detected and undetected dangerous failures [2].

The safe failure fraction of a subsystem is calculated as:

$$SFF = (\sum \lambda_s + \sum \lambda_{DD}) / (\sum \lambda_s + \sum \lambda_D)$$

Where

$\sum \lambda_s$ is the total probability of safe failures;

$\sum \lambda_D$ is the total probability of dangerous failures; and

$\sum \lambda_{DD}$ is the total probability of dangerous failures detected by the diagnostic tests.

From the above equation it can be appreciated that the safe failure fraction can be increased by uncovering more dangerous undetected failures and thus reducing the total probability of dangerous failures.

Redundant processing is used to achieve hardware fault tolerance, and in this way allow claiming increased hardware safety integrity according to Tables 2 and 3 in [2]. Under this provision it is understood that upon the occurrence of a fault, a fault-tolerant system will still have the capability to perform its required function, i.e. bring the process to a safe state.

Voting is often used as a means to detect discrepancies in the processing results of redundant channels, thus it can be considered a mechanism to increase diagnostic coverage. If the voting mechanism becomes unavailable due to failures developing in a channel, the system is said to enter a degraded mode. In this condition the system that depends on voting may have reduced safety integrity.

Redundant systems that loose the voting mechanism due to failure in one channel may have go to a safe state if not repaired in the allocated Mean Time To Restoration (MTTR). Therefore redundancy does not necessarily secure increased availability⁴, as a system that depends on voting to achieve high integrity can only continue to operate for a limited time in degraded mode. Availability is increased if the system can continue operating at the required safety integrity. In the event of failure(s) this is achieved either by repairing within the MTTR or by including a mechanism to maintain the required safety integrity despite the failure, for instance by switching-over to a stand-by system.

Modern safety-related systems are designed to achieve higher safety integrity by increasing SFF, while avoiding dependence on voting mechanisms. Safety-related systems are being designed to achieve high safety integrity through rigorous Failure Modes and Effects Analysis (FMEA) that allows diagnostics coverage close to 100 %.

The use of redundancy requires calculations of the PFD for redundant channels considering the effect of common cause⁵ failures. For systems that use N redundant channels the following equation can be used:

$$PFD_{Total} = (PFD_A \times PFD_B \times \dots \times PFD_N) + \beta \times PFD_{Worst_of_A, B, \dots, N}$$

⁴ Availability is defined in [3] as the ability of a functional unit to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval, assuming that the required external resources are provided.

⁵ A common cause failure is defined in [4] as a failure which is the result of one or more events, causing coincident failures of two or more separate channels in a multiple channel system, leading to a system failure.

Where the β factor is used to calculate the rate of common cause failures applicable to two or more channels operating in parallel. As noted from the equation, the probability of common cause failures may become the dominant factor in determining the overall probability of failure of a multichannel system.

3. Diverse processing used to achieve high safety integrity

The use of diverse redundant mechanisms to process the same information allows to achieve higher safety integrity than identical redundant mechanisms. In this section some of the effects of diversity on common mode failures, common cause failures, and systematic failures are discussed.

3.1 Effects of diversity on common mode failures

Common mode failures are defined in [4] as the failure of two or more channels in the same way, causing the same erroneous result.

Channel

A channel is defined in [4] as an element or group of elements that independently perform(s) a function

An effective defense against common mode failures is the use of diverse redundancy. Diversity can be used to expose dangerous faults in a channel through comparison with a redundant diverse channel. Should there be a discrepancy between the two channels the system as a whole may take a safe action. Systems with identical redundancy may be exposed to hidden common mode dangerous failure in the redundant channels preventing them from taking a safe action on demand.

Common mode failures can turn into common cause failure if causing system failure. For example, consider a manufacturing problem in the same batch of electronic component that causes identical failures (i.e. common mode failures) in all redundant digital outputs of a logic solver, preventing the system from performing its function. Diverse redundancy could prevent this type of failures, as different type of electronic components would not develop the same failure.

3.2 Effects of diversity on common cause failures

Diversity leads to a reduction in probability of failure due to common cause failures, due to a reduced β factor as compared to the factor for identical redundancy. The methodology discussed in Annex D of [5] states that diversity is one of the most effective mechanisms to reduce the β factor. One reason for this is that common cause failures of diverse channels are likely to be non-simultaneous, thus increasing the probability of the diagnostic tests detecting the failure.

The case presented in Table D-5 of [5] shows $\beta = 2\%$ for a system using diverse programmable electronics (e.g. a SIS logic solver), and $\beta = 5\%$ for an identical redundant system.

Table D-4 in [5] shows that for sensors and final elements the β factor can vary from 1% to 10%. Lower β values are achieved by systems with diversity, separation, and more frequent diagnostic tests.

3.3 Effects of diversity on systematic failures

The effects of systematic failures can be better controlled through the use of diversity.

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, etc. [1].

As an example, software may include errors that will manifest when the same specific piece of code is executed in the same circumstances.

Consider that diverse redundant elements are designed, configured, and manufactured through different methodologies and using different components, design processes and by different teams. Diverse channels have different features, behavior and reliability data. In this situation diversity prevents systematic failures from affecting the redundant channels in the system.

Among other applications, diversity has been used to implement SIS logic solvers currently rated up to SIL 3. In the following example, a digital output module is described that uses two diverse technologies embedded in a single module, see Figure 1. Module A contains two diverse redundant processing units: Field Programmable Logic Arrays (FPGA) and Microcontrollers (MCU). When the FPGA and MCU receive an output command from the logic solver CPU, they process the signal using different hardware and firmware from each other. The output signal is then sent to the field device through wiring terminals of Channel X in the Mounting Terminal Unit (MTU). Module B refers to a second digital output module that can be mounted in the same MTU and remain stand-by to increase availability, as discussed in the next section.

Some aspects of the design and manufacture processes for this implementation of two diverse technologies in a system are as follows:

- Different development process
 - Different product design methods
 - Different development teams
 - Different coding guidelines
- Diverse technologies
 - Different software design tools and compilers
 - Information is processed using different circuitry technologies: Field-Programmable Gate Arrays (FPGA) vs. Microcontrollers (MCU)
- Different manufacturers of electronic components

However, as the requirement specification for development is still the same, this may remain a source of systematic failures.

This implementation of diverse processing has resulted in a reduction of dangerous undetected failures in favor of safe failures, with SFF values achieved over 99.9 % [6], and meeting requirements for SIL 3 applications.

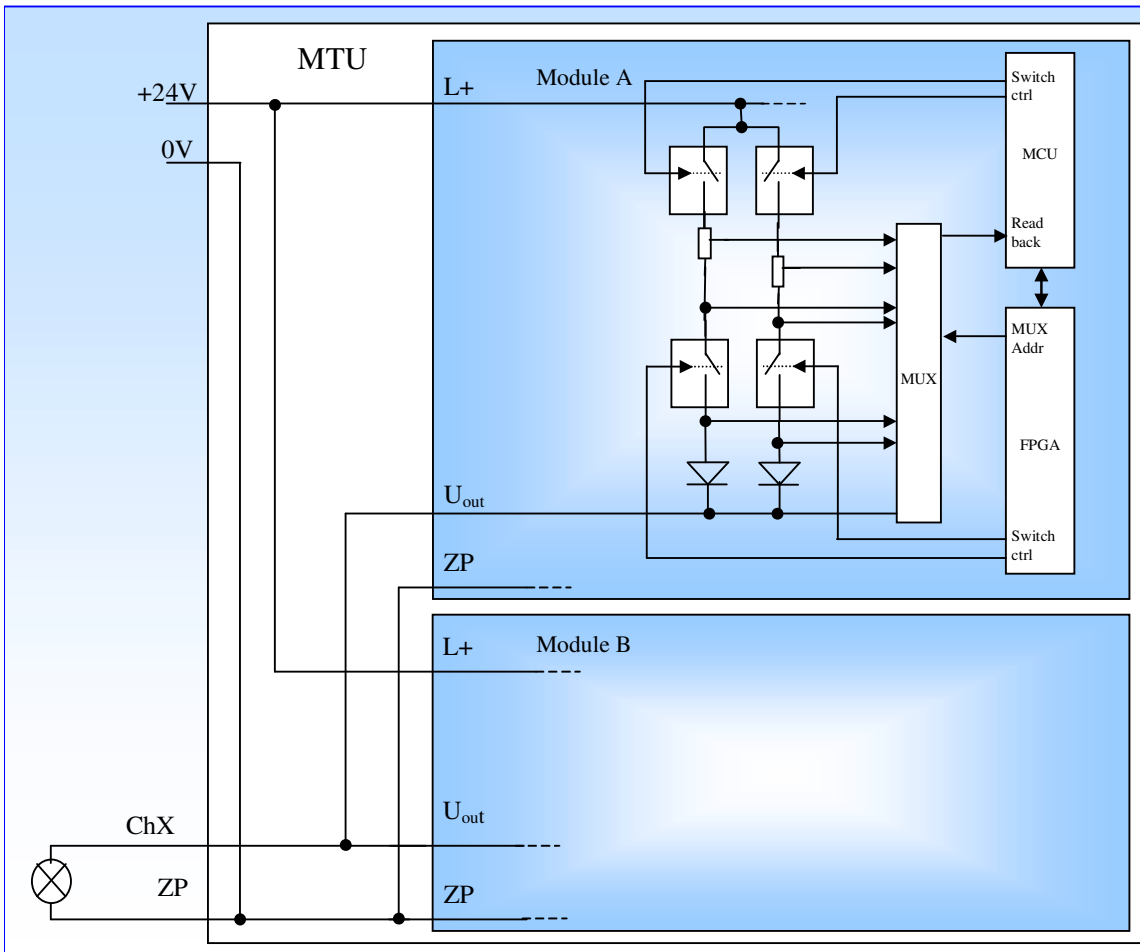


Figure 1. Example of on-board diversity for digital outputs board using FPGA and MCU circuitry

3.4 How to increase availability

High availability has been sought through parallel redundancy of channels in SIS logic solvers and field devices. Availability of safety related systems is increased by maintaining the required safety integrity while keeping the process operational.

When using the diverse processing scheme availability can be increased through hot stand-by redundancy. Consider the architecture in Figure 2. While the main processing units in processors and I/O modules operate with internal diversity, if a failure develops in one of the processors or I/O modules, the unit transfers control to the hot stand-by unit. Both on-line and stand-by units are rated to the required safety integrity level, and once the switch over is complete the unit can continue operating without time restrictions.

The scheme described for the use of diversity offers advantages over logic solver implementations based on identical redundancy to increase availability. Redundant systems that depend on voting to uncover faults and maintain safety integrity usually enter a degraded mode of operation when developing a failure. While the safety integrity is maintained during the period stipulated by the MTTR, these systems must go to a safe state (i.e. shutdown) if not repaired within this period. This effectively means that their availability is limited as these systems

will not be able to continue performing their required function and the process may be forced into an unwanted shutdown.

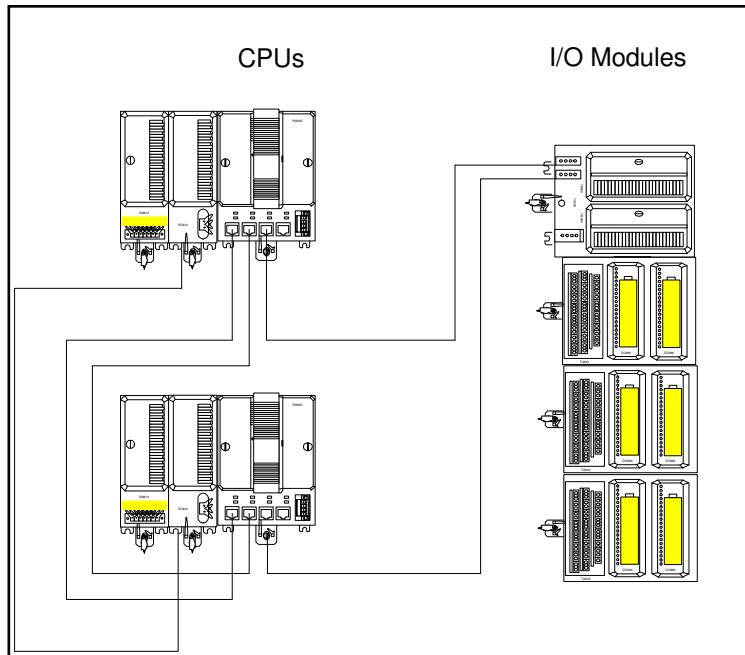


Figure 2. Logic solver architecture with internal diversity and stand-by redundancy

3.5 Diversity of SIS field devices

The discussion presented in this document applies to SIS logic solvers as well as field devices. The use of SIS diverse redundant instruments and final control elements may enable similar benefits as those discussed for logic solvers:

- Redundant diverse field equipment can also help unmask additional dangerous undetected faults, thus increasing Safe Failure Fraction. This may allow field devices meet higher safety integrity requirements.
- Reduction of common mode failures in redundant field equipment.
- The calculation techniques used in [5] show that SIS field devices can benefit from larger reduction of the probability of failure due to common cause failures when using diversity.
- Systematic failures can also be better controlled through the use of diverse field equipment.

To increase availability each redundant field device should meet the required safety integrity level. In this way in case that one of the field devices develops a failure the remaining channel(s) can continue functioning maintaining the required safety integrity level, without being forced to enter a safe state if not repaired within MTTR.

As with all SIS project implementations, the design needs to be validated to ensure compliance with safety integrity requirements.

4. Practical Implications: how diversity can help improve safety integrity in SIS projects

What benefits are there for users of safety related systems based on diversity?

End users benefit from high availability that can help maintain operation and high integrity even if failures affect main components of safety related systems such as processors. The main benefit is the ability to maintain risk reduction capabilities and reduce unwanted shutdowns.

The use of diverse redundant SIS field equipment increases safety integrity by reducing common cause and systematic failures, and increasing Safe Failure Fraction. The main benefit here is the ability to achieve higher safety integrity through the contribution of diversity.

The control of systematic failures may be elusive and hard to achieve. The use of diverse equipment provides users a mechanism to reduce the quantity of system components that need to be subject to systematic failure control. Diverse hardware is recommended in Tables A.16 and A.17 in [2] as a measure to control systematic failures in SIL 3 and SIL 4 systems.

The use of diverse field equipment may require different maintenance procedures and tests intervals of the diverse redundant devices. However the use of identical redundancy may result in a need to use more redundant channels to achieve the same safety integrity level. This also leads to increased maintenance requirements, as the system will have more components that need to be looked after.

5. Summary

The use of diverse hardware and software to implement SIS Programmable Electronic Systems as recommended by the IEC 61508 standard can contribute to significant improvements in the performance of safety related systems. Diverse redundancy may enable increased safety integrity through:

- Increased safe failure fraction due to unmasking of undetected dangerous failures
- Prevention of common mode failures
- Reduced probability of failure due to common cause failures
- Reduction of systematic failures.

Increased availability is achieved through the allocation of redundant hot stand-by components that independently meet the required safety integrity level.

The diversity and hot stand-by redundancy schemes discussed are applicable to both SIS logic solvers and field devices.

The main benefit for end users through the combined use of diversity and hot stand-by redundancy in safety-related systems is the ability to achieve higher risk reduction capabilities while ensuring continuity in operations.

References

- 1 International Standard IEC 61508-4 “Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations” First edition, 1998-12.
- 2 International Standard IEC 61508-2 “Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems” First edition, 2000-05.
- 3 International Standard ISO/IEC 2382-14 “Information technology – Vocabulary – Part 14: reliability, maintainability and availability”, Second edition, 1997-12-01.
- 4 International Standard IEC 61511-1 “Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and software requirement”, First edition, 2003-01.
- 5 International Standard IEC 61508-6 “Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3”, First edition, 2000-04.
- 6 ABB Industrial^{IT} 800xA – Safety System version 5.0. “Reliability and Availability AC800M High Integrity”, Document Number 3BSE034876R5001, October 2006.
- 7 International Standard IEC 61508-1 “Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements” First edition, 1998-12.
- 8 Prew R., “Integrated but separated – Advances in integrated safety control”, ABB Review Automation Systems Special Report, 2007.