Impact of IEC 61508 Standards on Intelligent Electrical Networks and Safety Improvement

by Michel Bonnet, Maximilien Laforge, and Jean-Baptiste Samuel

Executive summary

Improper integration of Intelligent Electronic Devices (IED) into medium / high voltage electrical networks can impact both network performance and safety. Now, standards such as IEC 61508 provide a framework from which new safety risks can be managed. This paper simplifies the complexity of integrating new devices into existing grid networks by explaining how to implement IEC safety and maintenance standards. Examples are presented for how to minimize cost and maximize safety benefits.

998-2095-02-21-14AR0

Schneider Electric

Introduction

Over the last several years utilities have replaced electro-mechanical technologies with new programmable electronic systems. While utilities have benefitted from the new technologies, it is difficult for operations personnel to determine every possible failure scenario and to predict issue-related network behaviors. The stakes are high as the tolerance for medium / high voltage electrical network downtime continues to erode. Costs are too high for both customers and utilities when network failures occur. In addition, the need to maintain safe network operation is a growing concern given the increase in complexity of the emerging networks.

These programmable electronic systems (also referred to as Intelligent Electronic Devices or IEDs), are characterized by failure modes that are different from the traditional electro-mechanical relays. The IEDs contain hundreds of electronic components and have software embedded into their microprocessors. This results in increased network complexity.

The risks are real. According to a study conducted by the UK Health and Safety Executive[1] 65% of incidents involving process control systems occur during the specification, design, installation and commissioning phases of the product implementation. The rest occur during the maintenance and modification that take place after commissioning (see **Table 1**).

Table 1
Results of a study commissioned by the UK Health and Safety Executive

IED failure categories	Percentage of total	Design vs. Operation
Specification	44%	65% (Design)
Design and implementation	15%	
Installation & commissioning	6%	
Operation & maintenance	15%	35% (Operation)
Modification after commissioning	20%	
	100%	100%

For effective management of IED devices, risk reduction can be best achieved through the execution of robust design principles. Fortunately, industry standards such as IEC 61508 have been introduced that provide guidance on how to improve modern electrical network safety performance. This paper interprets the IEC 61508 standard and provides guidance for how to maintain high levels of safety when deploying IEDs on electric networks.

Step 1: Balance cost vs. safety

The goal is not to overload the network with IED redundant devices but to install just enough to both minimize cost and establish the proper level of safety. Some industries, like the nuclear industry have little leeway in exercising this balance and safety is their top priority. In other industries such as aerospace, transportation, healthcare, and manufacturing, the risk is slightly lower, and it may be viable to decrease the number of network IEDs and still attain a proper safety level. In the utility industry the design of the network should be analyzed to determine how many customers are affected should a failure occur. Areas of high exposure should represent those areas of high investment.

[1] Out of control: Why control systems go wrong and how to prevent failure - Health & Safety Executive – UK 2003

Scenarios for both the protection function and the control function should be evaluated in order to determine where the risks are greatest. The distinction between these two intelligent electrical network sub-processes needs to be well understood.[2]

Protection functions

Protection functions allow for the quick isolation of the section of the electrical network that is in default. This limits the consequences of an incident. These protection functions are performed by a series of IEDs. For example, each IED may be programmed in a specialized manner which allows it to focus on a particular aspect of the electrical distribution process such as current arrival, current departure, line status, voltage transformation, or motor operation.

In order to better understand the concept of protection functions, consider the example of an arc flash incident. The main role of arc protection is to detect an arc flash and to cut off the current path feeding the arc. The arc is detected by an arc sensor and confirmed by a phase or an earth-fault overcurrent. Depending upon where the sensor is located, the confirmation by overcurrent is done locally or remotely and the tripping occurs locally or remotely (see **Figure 1**). The consequence of a non-eliminated default represents risk to people, loss of production, and damage to expensive physical infrastructure. The consequence of the tripping function executed without demand from the electrical process represents non-distributed energy costs and even safety risks in the applications where the loss of power supply is critical (for example to maintain lighting and / or air circulation in a tunnel in case a problem occurs). This is why IED protection functions need to be properly configured and designed.

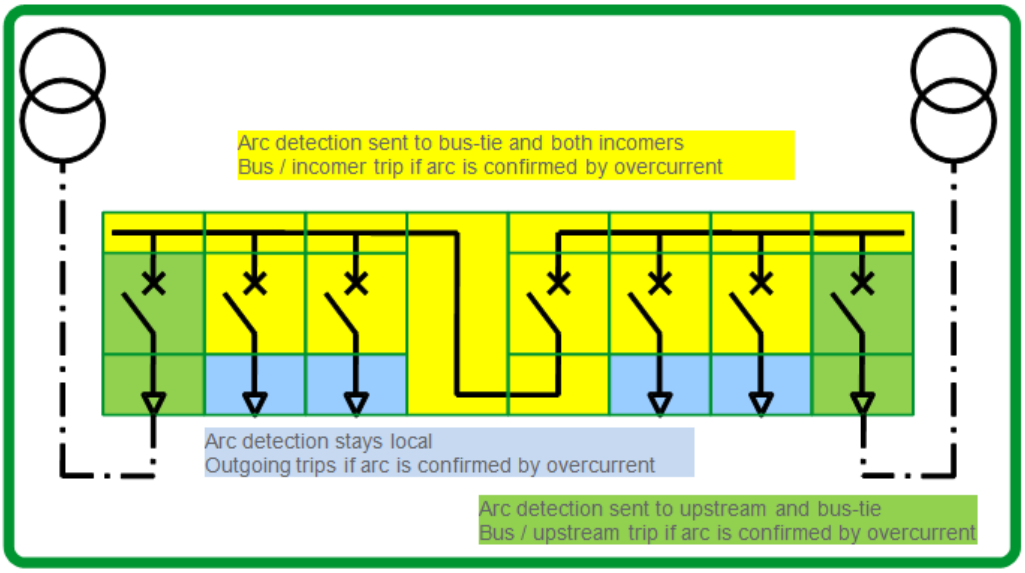


Figure 1
Arc flash protection is enabled by the IED's integrated in the network

Control functions

Control functions relieve the burden on operators by automatically executing some pre-defined actions that must be executed in a very short time. These functions diminish the risk of human error in circumstances where quick responses are required. Control functions are frequently performed by IEDs.

[2] Mémento De La Sûreté Du Système Electrique Edition 2004, RTE

One example of a common challenge is how to modify the electrical network scheme with switching devices without breaking capacity. In order to accommodate such a scenario, IEDs involved in the control function need to be configured and designed according to the following rules:

- Avoid opening or closing a switch, where changing the position of a switch will establish or cut off a current circuit
- Avoid opening or closing a circuit breaker where the new position of the circuit breaker will connect a live circuit to the earth or will establish a current circuit through a switch in movement

In this example, if key rules are not configured and designed within the IED for proper control or automatic sequence, the consequences could result in injury and damage to the equipment.

The level of safety integrity and availability of intelligent electrical networks can be adjusted or enhanced based on requirements. **Appendix A,** located at the end of this paper**,** illustrates several designs that alter the level of safety, integrity, and availability.

Step 2: Application of standards

The IEC 61508 standard defines a methodology for engineering safety functions that *allows all the relevant factors, associated with a product or application, to be fully taken into account and thereby meet the specific needs of users of the product and the application sector*[3]. This standard is widely used by electronic device manufacturers and suppliers when any part of the safety function contains an electrical, electronic, or programmable electronic component and where application sector international standards do not exist.

The IEC 61508 standard specifies the risk assessment and the measures to be taken in the design of safety functions for the avoidance and control of faults. In fact, IEC 61508 provides a complete safety life cycle that accounts for possible risk of physical injury and damage to the environment. Acceptable levels of risk are determined and procedures for residual risk management over time are established (see **Figure 2**).

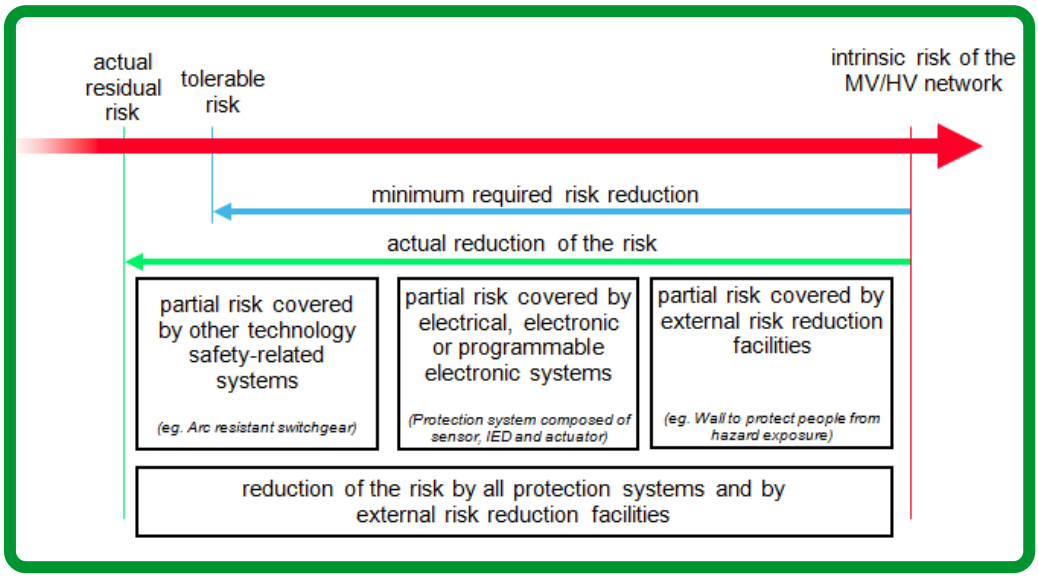


Figure 2
Functional safety and risk reduction

[3] IEC, Edition 2.0 2010-04, IEC 61508 parts 1 to 7: *Functional safety of electrical / electronic / programmable electronic safety-related systems*

The standard also requires that hardware be designed to tolerate a certain level of random hardware faults, and to demonstrate safe operation in harsh environments. It also calculates the probability of failure of each safety function.

In order to achieve the necessary Safety Integrity Level (SIL), the standard requires a proof of residual risk, which is based on the probability of dangerous failure (see **Table 2**). The calculation is based on the equipment components that influence the entire safety loop (sensor, IED, actuator). The failure probabilities of each component are considered together so that the safety level of the holistic architecture can be determined.

Table 2
Safety integrity level (SIL) estimates the probability of failure

Safety integrity level (SIL)	Target average probability of failure per year	Target 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

The standard is quite comprehensive and addresses hardware failures, software failures, systematic failures, and environmental and operational failures. The standard recommends a set of techniques and measures for controlling these failures.

Some examples of the type of guidance provided in the hardware domain include:

- Verification of measured signals through analogue signal monitoring by comparative reading between the current / voltage phases
- Verification of the processing unit by a second processing unit through the reciprocal exchange of data and by detecting differences
- Verification of the output by coil monitoring of the relays

"A third party can ensure that the quality level is achieved without requiring each utility stakeholder to become an expert in functional safety."

Recommendations to achieve the required safety integrity on the software side include:

- Implementation of self tests to monitor electronics at start up, during IED operation, and to monitor program execution and data integrity
- Use of static and dynamic analysis tools
- Use of automated verification tools
- Use certified tools for code generation

The standard also provides requirements regarding development methods, competence of the project team, project management, change management, tracking of requirements, and documentation.

Safety integrity level, the company experience, and the complexity and uniqueness of the design all impact the correct implementation of the standards. Since assessments that evaluate system reliability are relatively new in the domain of power systems, the recommended practice is to utilize an accredited independent organization to perform the assessment.

When interpreting IEC 61508 standards, assessment by an external body ensures that appropriate techniques and measures have been selected and applied. A third party can ensure that the quality level is achieved without requiring each utility stakeholder to become an expert in functional safety.

Step 3: Maintenance plan

As illustrated in **Table 1**, 35% of process control system related downtime is due to maintenance and modifications work. The IEC 61508 standard also addresses recommended approaches to maintenance.

The purpose of maintenance is to detect and repair faulty systems and anticipate potential failures (preventive maintenance). To ensure a level of system integrity that conforms to the IEC 61508 standard, an efficient diagnostic and maintenance plan must be implemented.

In order to execute this step, proper hardware and software data must be gathered. The following actions are recommended:

- Identify the failure probabilities per device as per the defined Safety Integrity (SIL) levels (see **Table 2**). Products that are more reliable will require less maintenance.
- Implement IED software self-tests for all sensitive electronic components (e.g., CPU, memory). In case of failure, the failure is detected instantly and the test resets the IED to a safe state. The self testing function helps to significantly reduce the amount of maintenance that needs to be performed (see **Figure 3**).
- Simplify spare parts logistics. Since manufacturers of products publish the failure rates of their designs, it is possible to size the spare parts inventory with more precision and this helps to reduce logistics costs.

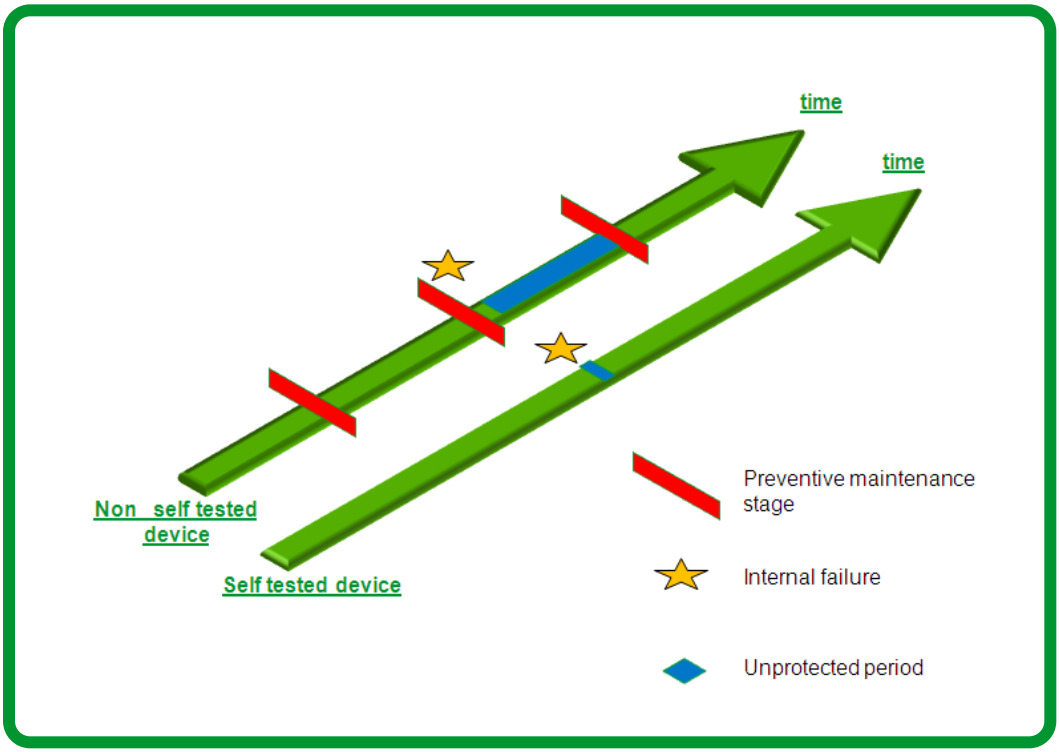


Figure 3
Advantages of devices which are capable of the self-test function

Standard maintenance will still be required for components that are not checked by self-tests. These elements have a probability of failure that increases over time. It is necessary to

perform scheduled maintenance (such as examining torque connections) in order to maintain uptime.

The IEC 61508 standard specifies the following aspects of completing a maintenance plan:

- Implementation of procedures
- Maintenance scheduling
- Documentation practices
- Execution of functional safety audits
- Documentation of modifications that have been made to the safety-related systems

Since many IEDs are modular in design, they are swappable which means that they can be tested off of the network. This helps to reduce both maintenance and planned downtime. **Figure 4** summarizes the benefits of implementing a maintenance plan based on IEC 61508 standard guidelines.

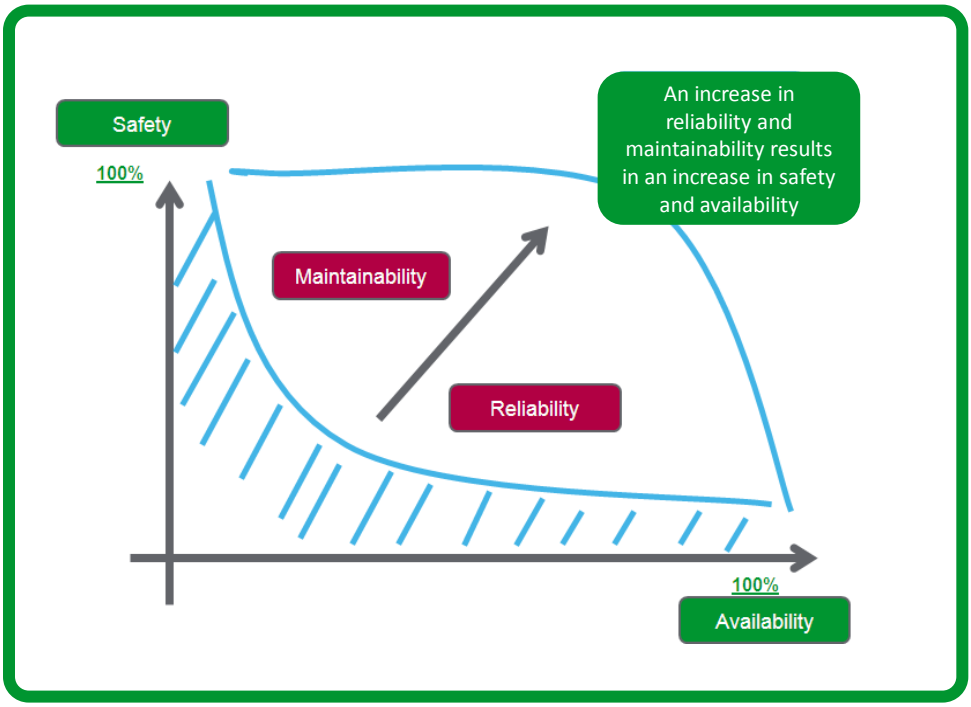


Figure 4
How a solid maintenance program increases both availability and safety

Regarding modifications, the IEC 61508 standard requires that an analysis be carried out to assess the impact of the proposed modification on safety (see **Appendix B** for detailed chart of this process).

Additional standards

The role of software continues to grow in importance as intelligent electrical networks continue to proliferate. This paper has primarily focused on the IEC 61508 standard, but other standards such as UL 1998, IEC 60880, and IEC 61508-3 also focus on software within electrical networks (see **Appendix C** for a more detailed explanation of these standards).

The standards all share a similar objective. The shared goal is to produce reliable, robust firmware with pre-defined behaviors in the event of a hardware or firmware failure. The

UL standards provide very general recommendations while the IEC standards publish detailed requirements. IEC standards provide techniques to reach the objectives while UL standards highlight objectives but do not specify techniques. The IEC 60880 standard, on the other hand, focuses more on cyber security. **Figure 5** provides an overlay map of the major similarities and differences of the various standards.

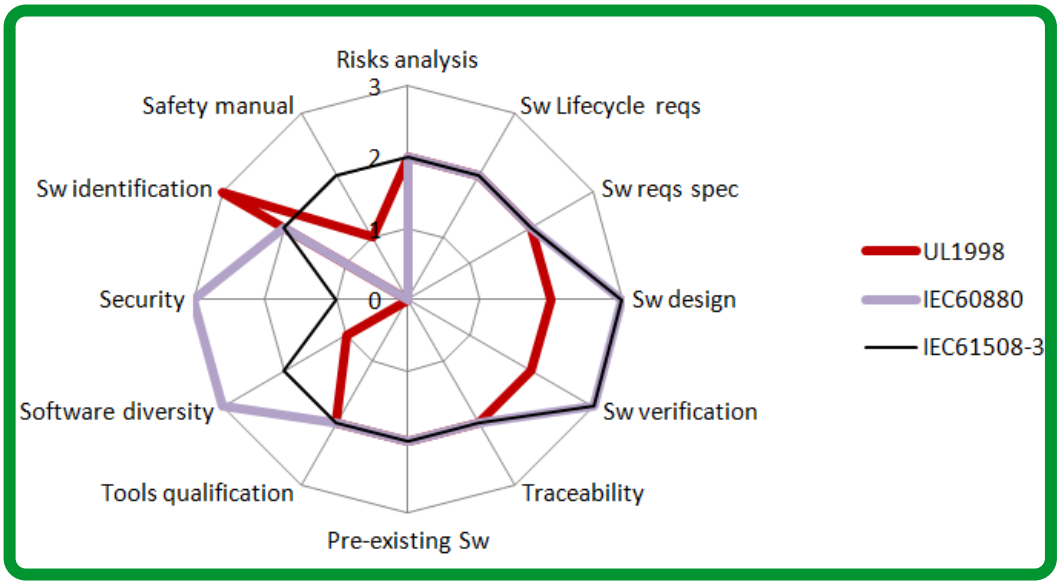


Figure 5
Comparison and positioning of reliability related software standards

Conclusion

The rapid growth of Intelligent Electronic Devices (IED's) within electric networks is allowing utilities to manage increased demand from users across the globe. However, the new technologies demand that safety standards be updated and modernized. Industry standards such as IED 61508 provide a roadmap for organizations that wish to deploy and support the new technologies. However many utilities do not have the time to invest in becoming functional safety experts. Implementation of the new technologies dictates that knowledgeable individuals help to design and support these new networks. Involvement of qualified third parties can ensure proper training, can assist in hazard and risk analysis, can help in the determination of safety integrity levels (SILs), and can specify the safety functions.

About the authors

Jean-Baptiste Samuel is responsible for protection relay automation within Schneider Electric's Energy Division. He has 10 years of project development experience with specialization in protection relays and electrical networks. He holds a graduate degree in software engineering from the University of Bordeaux, France.

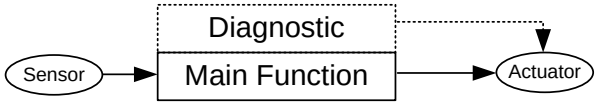
Maximilien Laforge is responsible for software dependability within Schneider Electric's Projects & Engineering Center (Energy Division). Since 2007 he has worked to improve software integrity and assists software development teams to attain safety certifications (e.g., IEC 61508, UL1998). He holds a Master degree from CNAM, France.

Michel Bonnet is responsible for functional safety management within Schneider Electric's energy automation department (Energy Division). Since 2008 he has driven quality assurance and functional safety management development projects in the domain of protection relays. He is an experienced application engineer and has worked on safety and substation Automation Digital Control System projects. He holds an engineering degree from ESIGELEC, in Rouen, France.

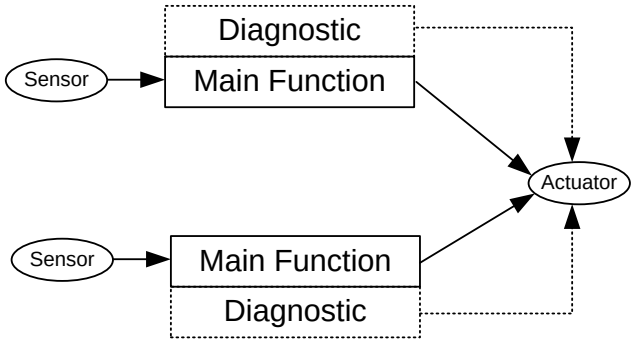
Appendix A
Safety Integrity and Availability Designs

It is possible to deploy multiple types of architectures to increase the safety integrity (lower probability of failure) and / or the availability (higher hardware fault tolerance). Below are some examples of common architectures:

Basic "1 out of 1 (1oo1)" architecture
Here a single channel performs the safety function. Detected faults lead to shutdown.
For example, in a protection function using an undervoltage trip coil, an electrical network defect or a severe internal failure of the IED will activate a circuit breaker trip.

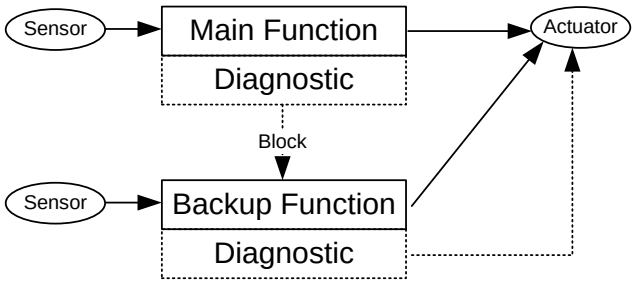


1 out of 2 (1oo2) architecture for higher safety integrity
Here, 2 channels can perform the safety function. Detected faults lead to shutdown.



1oo1 with backup for higher availability
For higher availability, a single channel can perform the safety function. Detected faults in the main channel lead to time limited single-channel operation of the backup function.

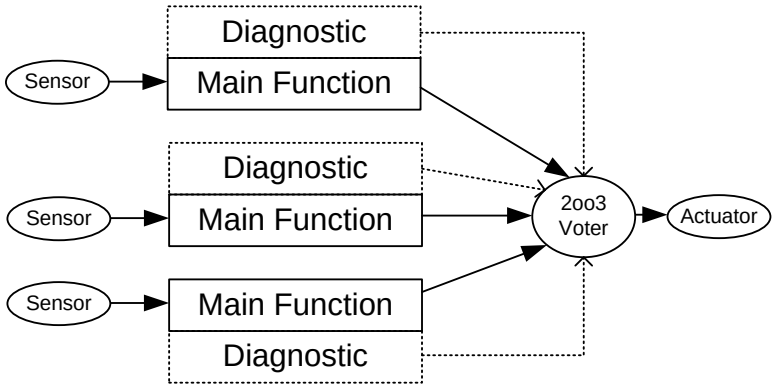
For example, in a protection function using a shunt trip coil, an electrical network defect will activate a circuit breaker trip order while a severe internal failure of the IED will transfer the protection function to a backup protection.



Appendix A (continued)

2oo3 for higher safety integrity and higher availability.

Here, 2 channels can perform the safety function (2oo3). Detected faults in one channel lead to 1oo2 operation.

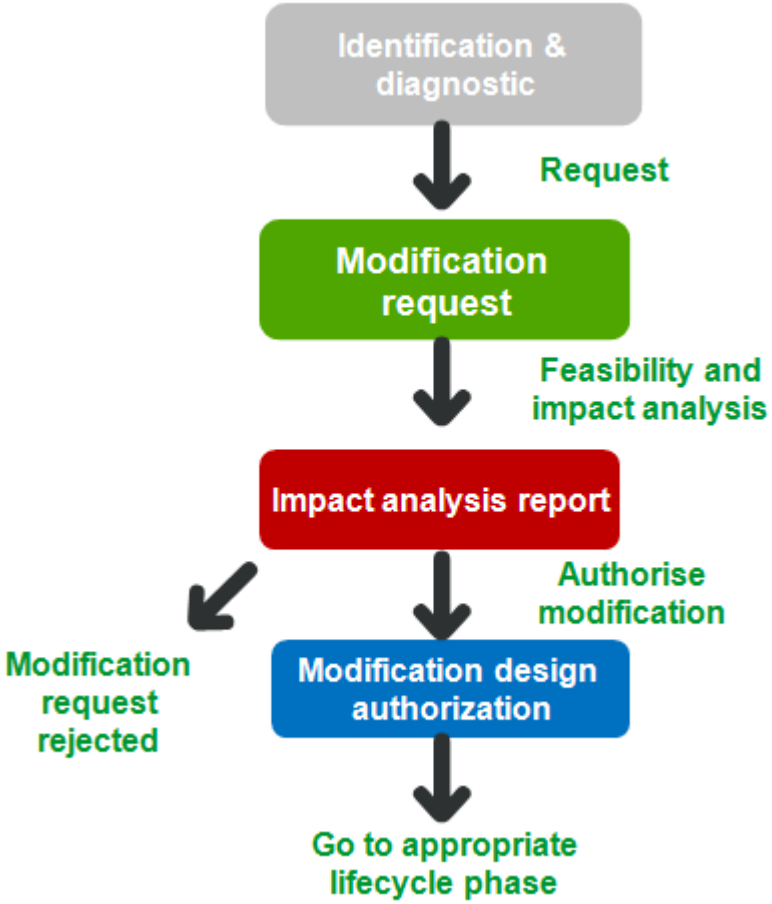


As demonstrated it is possible to adjust safety integrity and availability levels of programmable electronic systems and networks. However, a complete Safety Integrity Level (SIL) assessment report needs to first be conducted to determine probability of failure risks.

Such a report should include:

- A functional safety manual that defines the architecture safety and availability goals and how to operate the system
- Certified data for all safety parameters
- Evidence that failure avoidance and control measures have been executed during the project
- Assessment of the functional safety management system used by the manufacturer (including processes used, and competence of the project team)

Appendix B
IEC 61508 Modification Procedure Model[4]



[4] IEC, Edition 2.0 2010-04, IEC 61508 *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: general requirements* - Figure 9: Example of modification procedure model

Appendix C
Additional Standards

UL 1998 – Software in programmable components[5]

UL 1998 is an umbrella standard that addresses application-specific embedded software residing in programmable components. Application-specific means that the software is limited to a designated application. This allows effective evaluation of the hazards and risks associated with the software. The requirements in UL 1998 are applicable to embedded microprocessor software whose failure is capable of resulting in a risk of fire, electric shock, or injury of persons. The requirements in UL 1998 are intended to supplement applicable product or component standards and requirements. These requirements are intended to address risks that occur in the software or in the process used to develop and maintain the software.

IEC 61508-3 – Functional safety of electrical/electronic / programmable electronic safety-related systems – Part 3: Software requirements

IEC 61508 is an umbrella standard concerning basic functional safety issues across many industries. Part 3 covers the software requirements of electrical / electronic / programmable electronic safety-related systems. The requirements apply to any software forming part of a safety-related system or used to develop a safety-related system. The requirements cover all software lifecycle activities from specification to design and validation and up through maintenance.

IEC 60880 – Nuclear power plants: Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions[6]

IEC 60880 is an application specific standard. It addresses the software of computer-based instrumentation and control (I&C) systems of nuclear power plants performing functions of safety category A as defined by IEC 61226. Category A denotes the functions that play a principal role in the achievement or maintenance of nuclear power plant safety to prevent a design basis event from leading to unacceptable consequences. Category A also denotes functions whose failure could directly lead to accident conditions which may cause unacceptable consequences if not mitigated by other category A functions. This standard provides requirements for achieving highly reliable software. It addresses each stage of software generation and documentation, including requirements specification, design, implementation, verification, validation and operation. The IEC 60880 standard is the interpretation of IEC 61508-3 for the nuclear industry.

Functional safety and cyber security standards

The following is a list of common safety and cyber security related standards:

- IEC 62351-10: Security architecture for TC 57 systems
- IEC 62351-7: Network and system management
- IEC 62351-8 RBAC: Power system management
- IEEE 1686 Standard for Substation Intelligent Electronic Devices Cyber Security Capabilities. (2007, 12).
- NERC CIP 007: Systems Security Management - Ed. 4. (2011, 01 24)

[5] UL 1998 - Software in programmable components 10/2008

[6] IEC 60880 – Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions 05/2006