Challenges implementing AS61508 on infrastructure projects

P. Kroon
Kroon Technology, Adelaide, Australia

ABSTRACT: Functional safety, as defined in AS61508 [1], provides a robust framework for the delivery of safety related systems. It has been a common requirement in infrastructure projects for over 2 decades. The objectives for its inclusion, and thus how it has been specified, have varied between projects. This has created confusion over what a compliant process may be. In all cases though, the core objective has been to deliver safer and more reliable systems.

In this paper the author aims to identify many of the common challenges encountered in projects in delivering safety related systems intended to be compliant with AS61508 [1] in infrastructure projects. Looking at some common challenges in delivering AS61508 [1] across the lifecycle from identification of hazards, selecting appropriate Safety Integrity Levels (SILs), delivering compliant solutions, and maintaining their performance in an operational context.

1 INTRODUCTION

Infrastructure projects are increasingly relying on complex control systems to enhance safety and efficiency resulting in more value from the investment. Whilst complex control systems can provide tangible benefits in these areas, they can also be a source of new risks and inefficiencies if not implemented effectively. As a result, it has become common practice to include reference to AS61508 [1] in infrastructure projects to support the development of complex control systems. AS61508 [1] provides guidance on functional safety of electrical, electronic and programmable electronic safety related systems. It covers the entire lifecycle for a system from concept through to decommissioning.

Whilst AS61508 [1] is routinely specified in infrastructure projects, the scope of its application varies between projects creating confusion in industry on how to achieve compliance. In many cases, the focus is on software development with the hardware aspects of AS61508 [1] disregarded to the detriment of the level of safety achieved. An understanding of some key hardware concepts considered in AS61508 [1] including Systematic Capability (SC), energise to trip, proof testing, and useful life, can benefit not only functional safety but good control system engineering.

2 SYSTEMATIC CAPABILITY

A logical consideration in the selection of components for safety applications is having confidence the component will work reliably when required. Whilst there is typically lot of focus on quantifying the effect of random hardware failures, commonly referred to as calculating the PFD (probability of dangerous failure on demand), little consideration is given to systematic failures. Components that form part of a safety function need to be selected with the goal of minimising systematic faults. AS61508.2 [3] sets out two options for demonstrating the appropriate selection of components based on hardware, Route 1_S and Route 2_S.

2.1 Route 1_S

Route 1_S, relies on a component being engineered in accordance with the relevant techniques and measure to ensure the likelihood of systematic faults being present is sufficiently low. AS61508.2 [3] includes several requirements and tables detailing techniques and measures to be used in the engineering of a component. The level effort and effectiveness in the implementation of these techniques and measures is also specified with the aim being to achieve a level of rigour commensurate with the target Safety Integrity Level (SIL).

It is impractical for integrators and end users to determine whether a device has been engineered in accordance with the relevant techniques and measures set out in AS61508.2 [3].

Therefore, in practice, Route 1_S relies on the concept of independent certification, where a third party attests that a claim of compliance with the relevant parts of AS61508 [1] made by the manufacturer is true based on the provision of objective evidence.

There are four levels of Systematic Capability SC1, SC2, SC3, and SC4. The required SC is aligned with the target SIL, for example a minimum of SC1 is required for a SIL1 application. Another example, a component that certified as SC3 is suitable for use in safety functions allocated SIL1, SIL2, or SIL3. In practice, integrators and end users can select a certified component with the appropriate SC, confident that the component is sufficiently free from systematic faults relative to the SIL for the safety function they are implementing.

This is the simplest approach to demonstrating systematic capability, but it may not be practical for some specialist components, or where a well proven component is preferred rather than using a new certified component that is untried in an application.

2.2 Route 2_S

AS61508 [1] does not require the use of certified components. It is an option but is not mandatory. If a component can be demonstrated to work effectively in a given application with a suitably low failure rate, then it may prove to be a better option over an untested certified component. This is known as proven in use.

AS61508.2 [3][2] route 2_S includes the requirements to be satisfied in order to demonstrate a proven in use argument to justify using a device in a given application.

Using the proven in use approach, there must be objective evidence available that demonstrates the component has worked reliably in similar applications, thus proving through operational experience that the component is sufficiently free from systematic faults to be trusted for use in a safety application.

3 ENERGISE TO TRIP

In many industries, it is typical practice to design safety functions so they remove energy to achieve a safe state, commonly referred to as a deenergise to trip function. In infrastructure projects, it is typical for safety function to need energy to perform their function. This could be to power jet fans or pumps to achieve or maintain a safe state. For these types of applications a loss of power would present a dangerous failure, as no power would compromise the safety function. These types of safety functions are typically referred to as energise to trip, as they require energy when there is a demand on the safety function. Energise to trip functions present a few challenges, in particular:

- Most safety PLCs are only suitable for deenergise to trip; and
- The energy source must be considered in the quantification of random hardware failures.

3.1 Safety PLC limitation

Most safety PLCs are only certified for deenergise to trip functions. Safety PLCs have very high levels of diagnostics and are designed to revert to a safe state when a fault is detected. The safe state for safety PLCs designed for deenergise to trip functions is to turn off its outputs.

In a deenergise to trip function, this would be the equivalent to the safety function activating and thus revert the system to a safe state. However, this behaviour would prevent an energise to trip safety function from operating and thus compromise the ability for the safety function to respond when there is a demand.

Careful consideration needs to be given to whether a safety function is energise to trip and if the control system is suitable for use for energise to trip functions.

As an example a popular architecture for infrastructure projects is to use Rockwell ControlLogix PLCs which Rockwell Automation state are suitable for SIL1 or SIL2 applications. Rockwell Automation provides a reference manual for the use of ControlLogix for SIL 2 applications [6]. In the manual it states, "*If the application cannot tolerate an output that fails open (de-energized), then an external means such as a manual override or output must be wired in parallel*". The manual goes on to provide an example architecture, that is shown in Figure 1, along with a method of operation.

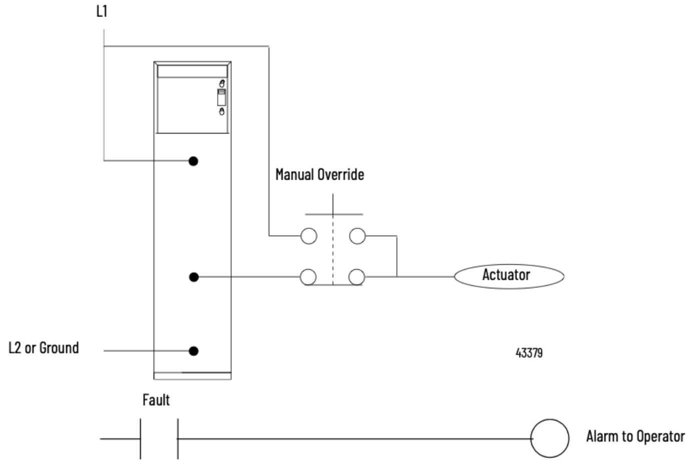

Figure 1. Example provided in Rockwell publication for energise to trip function

The proposed method indicates that in the event that a fault is detected by the PLC, an alarm should be provided to the operator who then uses a manual override to achieve the safety function, essentially manually turning on the device. In practice, for infrastructure projects manual overrides to compensate for PLC degradation would be impractical to implement as they are remotely operated and have the potential to exacerbate a hazardous event with incorrect or uncoordinated operations.

PLCs designed for energise to trip functions such as the HIMA HiMax [7], will continue to function in a degraded state, enabling safety functions to be preserved in the presence of a fault. Another popular PLC for infrastructure is the Siemens S7 1500 series PLC, as noted in associated functional safety certification [9] "*on condition that the "0 state" (closed-circuit principle) is defined as the safe state for the binary inputs and outputs*". This indicates that the PLC platform is only suitable for deenergise to trip applications.

3.2 Consideration of energy source in PFD calculations

For energise to trip functions to operate, they need energy/power. Therefore, in accordance with AS61508.2 [3], consideration of the energy/power source must be made in the PFD calculations, as a loss of power would result in the safety function failing to operate if there were a demand. Failure to consider the reliability of the energy/power source would completely negate the PFD calculations.

4 PROOF TESTING

It is typical to design safety functions so that they place or maintain a system in a safe state if certain conditions are present, or when initiated by an operator as opposed to continuous control. These types of functions are defined as demand mode safety functions, as they are safety functions that only perform on demand. If a safety function fails when there is a demand, it is reasonable to conclude, one or more components implementing the function must have:

- Failed in a manner that compromised its operation, as it did not operate when required.
- The presence of the failure was unknown, otherwise appropriate actions would have been taken to remedy the failure.

These types of failures are defined in AS61508 [1] as dangerous undetected failures. Other common terms include, dangerous dormant failures, dangerous hidden failures; and unrevealed failures.These failures present the biggest risk to safe operation, as they prevent a safety function operating on demand. As a consequence, AS61508 [1] requires proof testing to be undertaken to reveal dangerous undetected failures. AS61508.4 [4] clause 3.8.5 defines a proof test as a "*periodic test performed to detect dangerous hidden failures in a safety-related system so that, if necessary, a repair can restore the system to an "as new" condition or as close as practical to this condition*". Various issues have been observed in relation to proof testing in the infrastructure sector, including:

- impractical proof testing intervals;
- assuming perfect proof test coverage;
- failure to define appropriate proof tests;
- failure to undertake suitable proof tests at the specified interval

Each of these issues compromise any safety argument, either through creating an overly optimistic predicted of random failure rate (e.g. PFD) or adversely affecting the capacity to reveal dangerous undetected failures in practice.

4.1 Impractical proof testing intervals

The proof test interval has a direct effect on predicting the random failure rate of a safety function which is required by AS61508.2 [3] clause 7.4.5. The average probability of dangerous failure on demand (PFD_{avg}) of a single component can be calculated by the following equation based on the PDS Method Handbook [8].

$$PFD_{avg1oo1} = \frac{\lambda_{DU}\, TI}{2}$$

Where λ_{DU} = rate of dangerous undetected failures; TI = proof test interval.

As shown by this equation, the proof test interval is directly proportional to the PFD_{avg}. As observed on one project, the PFD_{avg} was reduced from 1 year (8760 hours) to 8 hours for jet fan proof testing. This had the effect of reducing the PFD_{avg} by 3 orders of magnitude or approximately 1000 times lower having a profound effect on the PFD_{avg}. However, it was impractical to implement and Imposes significant obligations on the operators and maintainers.

As a proof test for a component is intended to reveal all dangerous undetected failures, it typically requires a visual inspection and function testing, which is not practical every 8 hours. Further, it is unlikely that the contribution of a single jet fan to the tunnel air velocity can be effectively evaluated with the instrumentation installed in the tunnel, thus the proof test coverage (PTC) would be in question, the impact of which is discussed later.

It is critical that specified proof test intervals are achievable. Preferably minimum proof test intervals based on access and maintenance resource levels are specified in the contract documents.

4.2 Assuming perfect proof test coverage

Many PFD calculations encountered for infrastructure projects assume 100% PTC, that is, they assume all dangerous undetected failures will be revealed. In practice, this is very unlikely to be achieved. To be compliant with AS61508 [1], manufacturers are required to supply a safety manual that includes a proof test procedure and the associated PTC. Typically the PTC for transmitters is around 90 to 95% for devices intended for safety applications.

Figure 2 highlights the impact of imperfect proof testing, it is based on AS61508.6 [5] Table B.9. It shows that a reduction from 100% to 90% PTC doubles the PFD. This example highlights that failure to consider PTC in calculating the PFD results in overly optimist results.

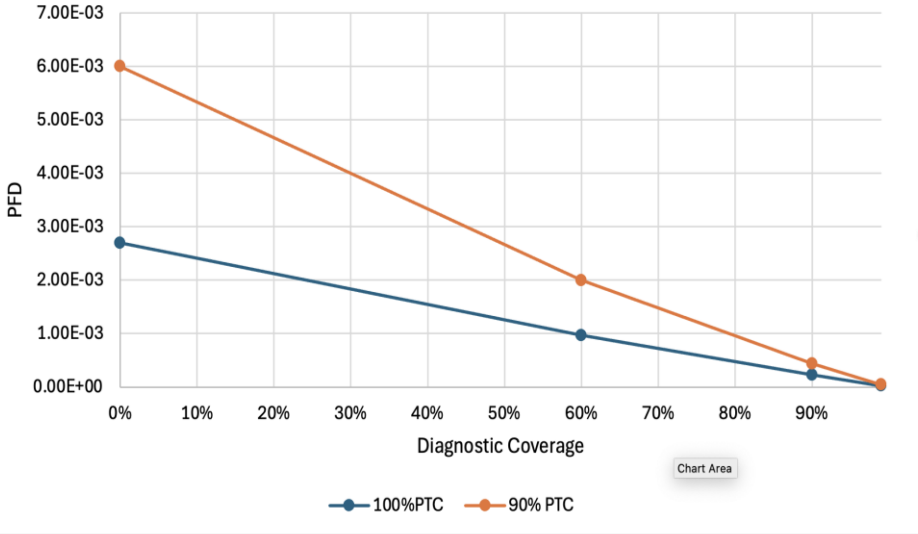

Figure 2. Impact of non-perfect proof test

4.3 *Failure to define appropriate proof tests*

It is typical to review operation and maintenance manuals, only to find no or very generic information in relation to proof test procedures. Proof test procedures must be developed and provided that provide clear guidance on how to inspect and test a device with the aim of revealing all dangerous undetected faults. The procedure should be step by step and repeatable by any technician, ensuring a consistent repeatable activity. Failure to provide this critical information or failure by operators and maintainers to follow the proof test procedures will compromise the integrity of the safety function.

4.4 *Failure to undertake suitable proof tests at the specified interval*

As noted in section 4.1, the PTI has a direct effect on the PFD. As unreliability is the complement of reliability it can be concluded that over time the likelihood of the device failing increases. This concept is shown in Figure 3, which shows the probability of failure increases over time in line with a natural decay curve.

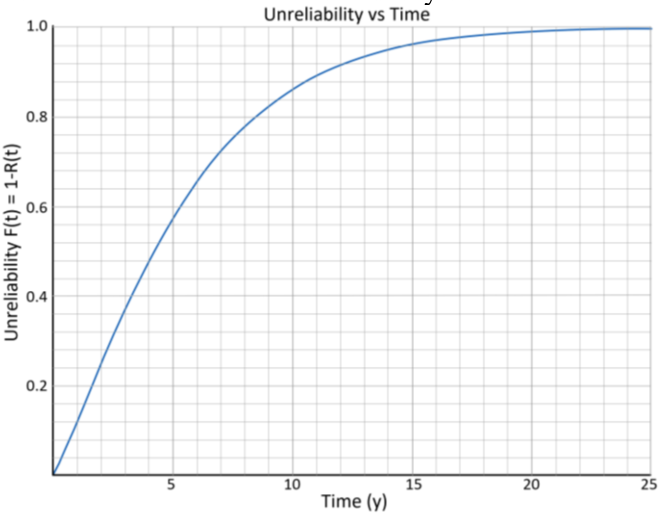

Figure 3. Unreliability versus time

If after a defined period, a device is proof tested following a procedure with a 100% PTC and any faults present fixed, restoring the device to as new condition, then the likelihood of a dangerous undetected fault being present reverts back to zero. The average of this period can then be derived. If the proof test interval is consistent then the average for one period is the average for the useful life of the device. This is shown in Figure 4.

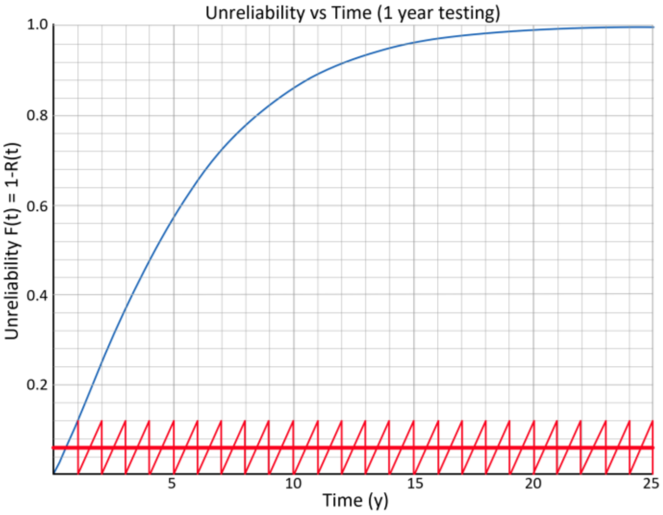

Figure 4. PFD instantaneous and PFD average, 1 year proof test interval

If the proof test interval is extended to 5 yearly for operational reasons, then the PFD average will increase proportionally, as shown in Figure 5.

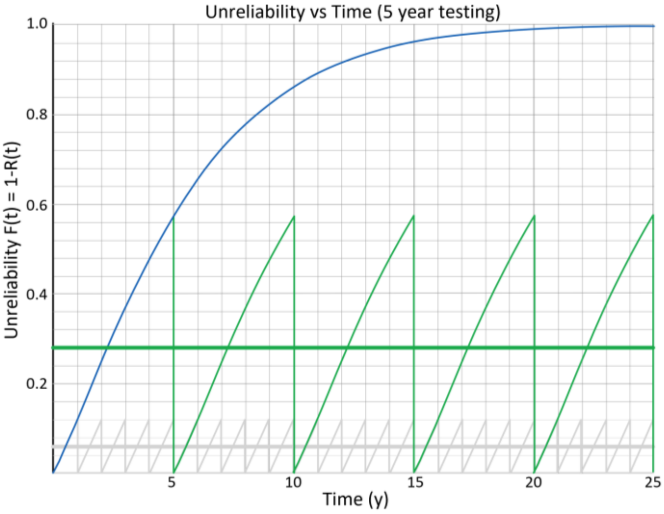

Figure 5. PFD instantaneous and PFD average, 5-year proof test interval

Where proof testing either is not undertaken at all or the proof testing is delayed to align with other operational considerations then the PFD increases. In practical terms, this means a safety function is more likely to fail due to a random hardware failure when it is called upon.

In the design phase it is important to ensure the proof test intervals used in the PFD calculations are practical and the testing can be completed at the nominated interval. In the operational phase it is critical suitable proof tests are undertaken within the intervals used in the PFD calculations.

5 USEFUL LIFE

A key assumption for the PFD calculations to be valid, is that components have a consistent failure rate. To achieve this, components forming part of a safety function must be replaced prior to the device reaching the end of its useful life.

A classic concept in reliability theory is the bathtub curve. The bathtub curve suggests there are three distinct phases, wear in, useful life, wear out. During wear in there is a higher failure rate which rapidly diminishes. This is also commonly referred to as burn in. There is then a period with a constant failure rate which is considered to be the useful life. Then there will be a rapid rise in the failure rate as the component moves into the wear out phase. This concept is illustrated in Figure 6. In Figure 6, the x axis is time, however the useful life of a component could be determined as a function of time, hours of operation, or number of cycles.

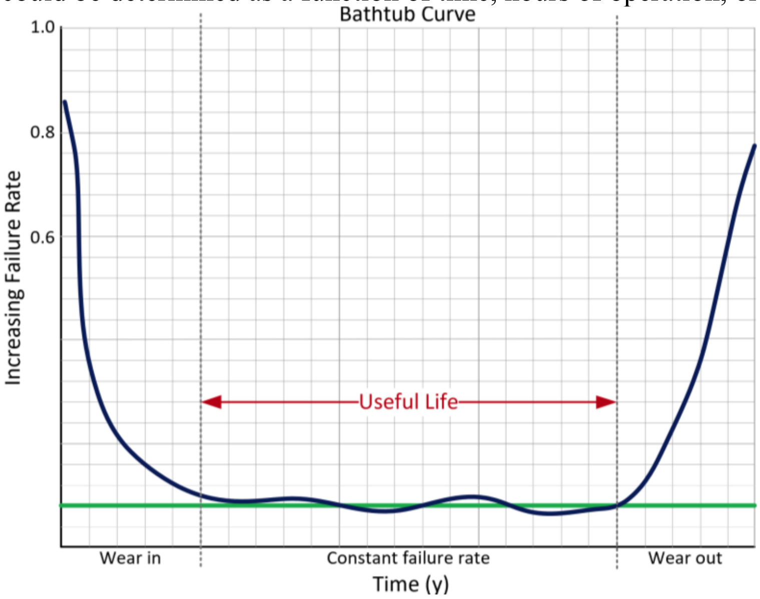

Figure 6. Reliability bathtub curve

If components are left in service until failure, then the likelihood of a component being in a failed state when there is a demand on the safety function becomes almost inevitable. It simply becomes a case of a failure being revealed through a failure of a safety function during a demand or periodic testing.

Even if components are being replaced periodically, if they are left in service after reaching the wear out phase then the likelihood of failure starts increasing exponentially and thus the likelihood of a failure of the safety function also increases rapidly, negating the PFD calculations and the integrity of the safety function. In practice, for every component used in a safety function:

- the useful life must be specified in an appropriate manner, i.e. time in service, hours run, or number of cycles;
- the current life of each component must be tracked;
- Components need to be replaced prior to reaching wear out;
- Component failure data collected; and
- Useful life assumptions periodically verified.

6 CONCLUSION

There are a number of concepts defined in AS61508 [1] that are crucial for ensuring the integrity of control system. Failure to address any of the key hardware concepts discussed, increases the likelihood of a safety function not working when there is a demand with potentially tragic consequences.

These same concepts can be used for other control systems to enhance their integrity improving the performance of the systems they support.

Whilst some projects have utilised AS61508 [1] to provide a framework for the delivery of robust software, without a systems thinking approach and suitable hardware the potential benefit offered by adopting AS61508 [1] will not be realised.

The guidance provided in AS61508 [1] represents good engineering practice, providing a framework for implementing an engineering process with rigour. Experience in other industries has shown that once the concepts are understood for deploying safety related systems, the knowledge permeates into the development of other control systems. This results in an improvement in the performance of those control systems and thus an improvement in the performance and safety of the systems of interest they are intended to control and monitor.

7 REFERENCES

[1] AS61508 2011. *Functional safety of electrical/electronic/programmable electronic safety-related systems Parts 1 to 7.* Standards Australia

[2] AS61508.1 2011. *Functional safety of electrical/electronic/programmable electronic safety-related systems Part 1: General requirements.* Standards Australia

[3] AS61508.2 2011. *Functional safety of electrical/electronic/programmable electronic safety-related systems Part 1: Requirements for electrical/electronic/programmable electronic safety-related systems.* Standards Australia

[4] AS61508.4 2011. *Functional safety of electrical/electronic/programmable electronic safety-related systems Part 4: Definitions and abbreviations.* Standards Australia

[5] AS61508.6 2011. *Functional safety of electrical/electronic/programmable electronic safety-related systems Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*. Standards Australia

[6] 1756-RM001U-EN-P-March2025. *ControlLogix SIL 2 Applications.* Rockwell Automation Publications

[7] HI 801 001 E Rev. 3.00 (0944). *HIMax System Manual*. HIMA Paul Hildebrandt GmbH +Co KG

[8] PDS method handbook. 2010 *Reliability prediction method for safety instrumented systems*. SINTEF

[9] Z10 067803 0020 Rev.00. *Report to certificate Safety-related Programmable System Simatic Safety System.* TÜV SÜD Product Service