Architectural constraints and 'proven-in-use'

Question:

This question often gets asked:

> **How can manufacturers apply route 2_H, given they cannot easily obtain proven-in-use reliability data for the exact same version of the devices?**

The brief answer:

It is a good question, but it confuses two different requirements.

IEC 61508 route 2_H is a method of determining **architectural constraints**. Route 2_H requires the failure rates to be estimated with a statistical confidence level of 90%. The failure rates must be measured during actual operation of a specific make, model and version of a device – but this is **distinctly different from being 'proven-in-use'**.

The term **'proven-in-use'** is specifically related to requirements for **systematic capability.**

Systematic capability is not directly connected to the measurement of failure rates. It has nothing to do with architectural constraints.

Systematic capability is a measure of the **systematic safety integrity of an element** that is applied in a safety function. Systematic safety integrity is achieved by eliminating, avoiding or controlling preventable failures.

IEC 61508 describes three different methods that may be used to establish systematic capability. The methods are designated route 1_S, 2_S and 3_S.

Route 2_S allows systematic capability to be established through a device or element having been proven-in use. The other two methods (routes 1_S and 3_S) are based on the application of techniques to prevent, control or avoid systematic faults.

Outline:

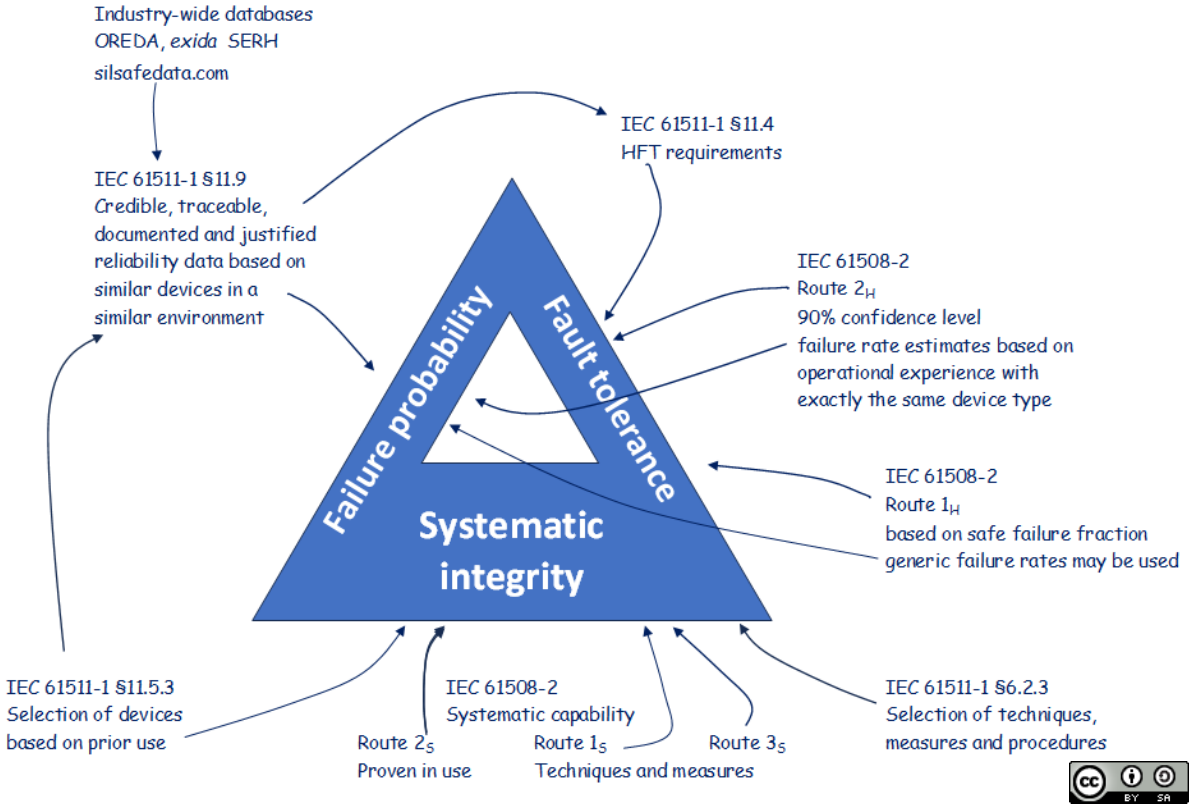
The objective of this paper is to explain that functional safety relies on **three separate sets of constraints** that must all be satisfied:

1. **Systematic integrity (prevention of preventable failure)**
2. **Estimated probability of failure (for failures that are not readily preventable)**
3. **Architectural constraints (minimum levels of fault tolerance for higher SIL)**

Introduction

Systematic integrity relies on a deliberate selection and application of quality management procedures, techniques and measures. Systematic integrity of devices may be demonstrated to some extent through the prior use of the same equipment in a similar environment.

Prior use (IEC 61511), proven in use (IEC 61508 route 2_S), and avoidance and control of faults through techniques and measures (IEC 61508 route 1_S and 3_S) all relate to demonstration of systematic integrity.



Probability of failure estimates depend on the assumption that failure rates can be maintained at reasonably constant values.

The failure rates that can be achieved in operation always depend on the environment in which equipment is operated and maintained. Variation in failure rates always spans at least a whole order of magnitude.

The objective of **architectural constraints** is to compensate for uncertainty in failure rate estimates and for the assumptions made in the design of safety functions (refer to IEC 61511-2 Ed 2 §11.4.1 Note 2). IEC 61508-2 §7.4.4.1.1 notes that the objective is to achieve a safety system architecture that is sufficiently robust to achieve the required integrity level given the complexity of the systems.

Architectural constraints are expressed in terms of the **minimum levels of hardware fault tolerance** required to achieve a specified safety integrity level.

IEC 61508 provides two options for architectural constraints: **Route 1_H and 2_H**

Discussion

Systematic integrity

Functional safety depends primarily on **systematic integrity.**

At least 95% of faults and failures in safety systems are preventable. This assertion is based on the observation that lowest reported failure rates for any type of equipment are at least 50 times lower than the highest reported failure rates (refer to OREDA).

Systematic integrity is achieved by preventing preventable faults and failures. Systematic integrity depends on a conscious, deliberate, and methodical application of quality management procedures and techniques. All functional safety standards apply quality management frameworks that are consistent with ISO 9001.

IEC 61508 was developed specifically to provide guidance on avoiding faults and failures in electronic and programmable electronic safety devices. It includes detailed guidance on the selection and application of procedures, techniques and measures for the design and development of hardware and software applied in safety-related systems.

The IEC functional safety standards all begin with requirements for formal management systems in functional safety engineering. Technical activities in functional safety systems cannot be expected to be effective without rigorous management frameworks.

According to IEC 61508, **project management** and **documentation** (i.e. information management) are the two core techniques that are mandatory for safety integrity. They need to be applied throughout the design and development of any safety systems. The level of effectiveness needs to be increased for higher levels of safety integrity. More complicated systems also need higher levels of effectiveness.

Higher effectiveness is achieved by applying:

- Increased levels of detail and additional techniques in design, inspection and testing
- Increased levels of independence in review, analysis, inspection, testing, audit and assessment.

IEC 61511-1 §6 requires the selection of procedures, techniques and measures during the planning of activities in all safety lifecycle phases. The selection needs to be appropriate for the required safety integrity. IEC 61511-1 leaves the selection open, though some limited guidance is provided in IEC 61511-2. Reference is made to IEC 61508-3 for techniques and measures related to the application program.

IEC 62061 provides detailed requirements for procedures, techniques and measures depending on the level of complexity and on the required integrity level.

ISO 13849 specifies detailed procedures and techniques. Additional requirements are specified for the higher performance levels d and e.

Systematic capability

IEC 61508 uses the term **systematic capability** as a '*measure of* […] *the confidence that the systematic safety integrity of* ***an element*** *meets the requirements of the specified SIL*'.

The term is limited to hardware and software in devices and systems that are built to comply with IEC 61508.

The primary method of establishing systematic capability is designated **route 1_S**. Procedures, techniques and measures are selected to avoid or control systematic faults. The level of effectiveness is increased for higher SIL. The functional safety assessor reviews the selection and application of the procedures, techniques and measures. The assessor makes a subjective judgement as to the level of safety integrity achieved.

IEC 61508 includes the option of 2 other methods for assessing systematic capability for **pre-existing** systems. These 2 methods were intended to be applied to systems that had been developed before the second edition of IEC 61508 was released in 2010.

Route 2_S depends on evidence that equipment has been **proven in use.** There needs to be sufficient operating experience to show that the probability of systematic faults remaining in the system is low enough to meet the specified SIL. For example, a system that has been shown to have a probability of (systematic) failure on demand of less than 10^{-3} would meet SIL 2. The demonstration would need to have shown that the system performed successfully with the full range of parameter combinations and across the full range of specified environmental limits. Alternatively, it might be demonstrated that the system has operated for an aggregated total of more than 10^7 device-hours (about 1,000 device years) without systematic failure.

Route 3_S depends on a retrospective analysis of the quality procedures, techniques and measures applied for equipment that was designed before 2010.

Selection of devices in IEC 61511

IEC 61511-1§11.5 specifies requirements for the selection of devices to be used in a safety instrumented system. There are only two choices:

1. Devices can be selected that comply with IEC 61508-2 and IEC 61508-3, and these devices '*can be applied in accordance with the requirements for systematic capability in IEC 61508-2*'
2. Evidence of suitability through **'prior use'** of similar devices.

In addition: '*all devices shall be suitable for the operating environment*'.

IEC 61511-1 §11.5 specifies the evidence required to establish prior use. It clarifies that: '*the main intent of the prior use evaluation is to gather evidence that the dangerous systematic faults have been reduced to a sufficiently low level compared to the required safety integrity'.*

Evidence of prior use is useful for demonstrating device failure rates that can be achieved in a particular application. For example: A total of 200 to 300 device-years of experience over at least 2 calendar years could be sufficient. That would be enough to support the claim that a failure rate is in the order of 0.01 pa if fewer than 2 or 3 failures of that type were recorded over that time.

Failure probability

The engineering process is never perfect. Some faults cannot be prevented.

SIL targets are defined in terms of targets for failure rate or probability of failure on demand. The standards specify that calculations are necessary to demonstrate that targets can be achieved.

Mathematical models can be used to estimate the **probability of unpreventable dangerous failure.** The models are based on the simplifying assumption that the faults which cannot be prevented are mostly random and occur at reasonably constant rates.

In practice all failure rates vary widely due to human factors, systematic factors and environmental factors. Reasonably constant and predictable failure rates can be achieved and maintained only by controlling those factors.

Probability of **unpreventable dangerous failure** is **minimised by design.** Equipment is designed and selected to be suitable for its application and environment. Equipment failure rates are maintained at reasonably constant levels through condition monitoring and **preventive maintenance.**

A study published by *exida* in 2016 concludes that failure rates can be expected to be at least 3 times higher than normal if maintenance activities are not completed promptly and effectively (Bukowski and Stewart, 'Assessing Safety Culture via the Site Safety Index'). The OREDA datasets indicate that failure rates can be expected to vary by a factor of at least 30 between different users.

Reliability centred maintenance techniques are applied to achieve a balance between cost of maintenance and cost of failure. Reliability centred maintenance can be applied to reduce equipment failure rates by at least a factor of 3, and possibly by more than a factor of 10. That level of improvement is only feasible if the equipment is readily accessible for maintenance, and adequate resources are available.

Probability of **unpreventable dangerous failure** may be reduced by **continuous automatic diagnostic functions and fault reactions.**

Some dangerous failures cannot be detected reliably by diagnostic functions. The probability of ***undetected* dangerous failure** may be reduced if faults which might lead to failure can be revealed through periodic (e.g. annual) testing and inspection.

Higher integrity levels or performance levels are achieved by using **fault tolerant designs**. Safety functions can be designed so that they continue to meet their performance targets even though some of their component elements have failed.

Fault tolerance

The IEC standards specify constraints on the selection of safety function architectures. These architectural constraints depend on the target SIL. Essentially the architectural constraints define the minimum level of fault tolerance that is acceptable for a safety function.

Fault tolerant architectures are not usually necessary to achieve SIL 1 performance. Fault tolerant architectures are usually unavoidable in achieving SIL 3 performance.

Estimates of failure rate and probability of failure on demand are based on assumptions about how systematic failures will be avoided and how equipment performance will be maintained.

Designers may make optimistic assumptions in their calculations to justify using a cheaper design.

For example, a single channel architecture could be claimed to achieve SIL 3 performance if the designer assumes unrealistically low failure rates in the calculations.

Architectural constraints provide a safeguard to compensate for the wide uncertainty in calculations and for the unavoidable variability in failure performance.

IEC 61508 architectural constraints

IEC 61508-1 allows a choice of two methods for evaluating architectural constraints. These two methods are primarily intended for use by manufacturers of E/E/PE safety-related systems. They may also be applied by designers of safety functions that apply safety-related systems.

IEC 61508 categorises safety-related devices as either Type A or Type B.

Devices can be classified Type A when they have:

- Well defined failure modes
- Deterministic behaviour
- Sufficient dependable failure rate data

Other devices are classified Type B.

The following information is required for both Type A and Type B devices regardless of whether route 1_H or route 2_H is applied:

- Comprehensive data and documentation
- Quality management
- Configuration management
- Assessment of systematic capability
- Safety manuals to demonstrate compliance with IEC 61508

Architectural constraints can only be evaluated and satisfied if this information is available.

IEC 61508 route 1_H

The first edition of IEC 61508 provided only one method of evaluating architectural constraints. That original method is designated route 1_H in the current edition of the standard.

Route 1_H sets the maximum SIL that can be claimed for a sub-system based on the safe failure fraction (SFF) and the hardware fault tolerance (HFT) for that sub-system.

The safe failure fraction is estimated on the basis that failures can be classified as either safe or dangerous. Failures can either be detected by continuous (or at least frequent) diagnostic functions, or they remain undetected. The safe failure fraction is the fraction of the failures that are either safe or dangerous but can be detected. The analysis assumes that corrective action or compensating measures are applied promptly when dangerous failures are detected.

IEC 61508 route 1_H is useful for applications in which diagnostic functions can be implemented, or where devices can be designed to reduce the proportion of failures that are dangerous.

The basic route 1_H table is for devices designated as ‘Type A’.

IEC 61508 Route 1_H - Maximum SIL claimable for sub-systems with Type A devices

SFF	HFT		
	0	1	2
SFF < 60%	SIL 1	SIL 2	SIL 3
60% ≤ SFF < 90%	SIL 2	SIL 3	SIL 4
90% ≤ SFF < 99%	SIL 3	SIL 4	SIL 4
SFF ≥ 99%	SIL 3	SIL 4	SIL 4

The maximum SIL that can be claimed is reduced by one level for 'Type B' devices. These are complex devices with complex failure behaviour and/or uncertain failure rate data. Devices that rely on software would generally be classed as Type B.

IEC 61508 Route 1_H - Maximum SIL claimable for sub-systems with Type B devices

SFF	HFT		
	0	1	2
SFF < 60%	Not allowed	SIL 1	SIL 2
60% ≤ SFF < 90%	SIL 1	SIL 2	SIL 3
90% ≤ SFF < 99%	SIL 2	SIL 3	SIL 4
SFF ≥ 99%	SIL 3	SIL 4	SIL 4

Safe failures are defined as those failures increase the probability of spurious operation of a safety function.

The thinking at that time was that spurious failures would generally result in a safe condition.

That rationale would usually be valid in machine safety applications. Most machines are safer when stopped. This is not valid in most process sector applications because spurious failures may increase the risk of hazards occurring.

Machinery applications

The architectural constraint requirements in IEC 62061 are based on route 1_H, but only the Type B table is used. Type B is applied because complex devices are typically used. The table is modified to relax the constraints when 'well-tried components' are used in a single channel architecture (i.e. with no fault tolerance). SIL 1 is allowed with HFT = 0 and SFF < 60% with well-tried components because they would usually be classified as Type A.

High levels of SFF can be achieved for safety functions in machinery applications because diagnostic coverage is readily achieved and 'well-tried principles' can be applied to reduce the proportion of failures that are dangerous. Refer to ISO 13849 for explanation of 'well-tried components' and 'well-tried principles'.

Diagnostics can be implemented because the safety function devices operate with relatively short cycles. Each device in the function is exercised through its complete range of sensing or action at least several times each week or each day. Unexpected device states can be detected within each cycle. The machine can be stopped if a fault is detected in a safety function.

Process sector applications

Route 1_H was difficult to apply in process sector because final elements can usually only be exercised infrequently, typically once or twice per year. It is not possible to achieve any diagnostic coverage if the elements cannot be exercised through their complete range of action at daily (or at least weekly) intervals.

Another concern with route 1_H is that spurious safety function activation is not usually safe in process sector applications. Processes are safer in steady state operation. Process shut down and start-up cycles involve increased risk of hazards. There is a clear benefit in applying diagnostic coverage to detect dangerous failures. There is no clear benefit in increasing the rate of spurious trips. It would be better to base route 1_H on levels of diagnostic coverage instead of safe failure fraction.

IEC 61508 route 2_H

Route 2_H was introduced as an alternative in IEC 61508 edition 2. It is a simpler method:

- HFT is not required for SIL 1 or for SIL 2 low demand
- HFT = 1 is required for SIL 2 high demand and for all SIL 3
- HFT = 2 is required for SIL 4
- Type B devices must have diagnostic coverage > 60%

IEC 61508 route 2_H depends on the reducing the uncertainty in component failure rate estimates.

Route 2_H requires that the failure rates used in calculation must be selected to have a **confidence level of 90%.** The failure rates need to be measured for the exact same type of components in actual operation and in a similar environment.

Route 1_H allows failure rates at a 70% confidence level, and generic failure rate data may be used (data recorded for similar devices of different makes and models).

IEC 61508-4 does not include a formal definition of confidence levels. Reference may be made to ISO 14224. A statistical confidence level relates to the uncertainty in the estimate of a parameter that has a true value that can be measured. There is a 90% chance that the true value of the parameter is between estimates at the 5% and 95% levels.

Theoretically, there is a 10% chance that the true value of a failure rate will be worse than an estimate at the 90 % confidence level.

Statistical confidence levels can only be applied for components that have a single true value of failure rate that can be measured. The route 2_H method is only useful for electronic components because truly constant failure rates only occur in electronic components (refer to ISO/TR 12489 for an explanation of this).

Statistical confidence levels can be determined using the chi-squared function. The differences between estimates at varying confidence levels depend only on the number of failures that have been counted:

	Number of failures counted			
	1	**2**	**3**	**10**
$\lambda_{90\%} / \lambda_{AVG}$	3.9	2.7	2.2	1.5
$\lambda_{70\%} / \lambda_{AVG}$	2.4	1.8	1.6	1.2
$\lambda_{90\%} / \lambda_{70\%}$	1.6	1.5	1.4	1.2

For example:

If 1 out of 100 devices failed after 1 year of service, then the simple average rate is $\lambda_{AVG} \approx 0.01$ pa. An estimate at the 90% confidence level would be $\lambda_{90\%} \approx 0.039$ pa, and an estimate at the 70% confidence level would be $\lambda_{70\%} \approx 0.024$ pa

There is no significant difference between $\lambda_{90\%}$, $\lambda_{70\%}$ and λ_{AVG} if more than 10 failures have been counted.

The chi-squared function may also be applied to estimate a failure rate with any given confidence level from the total recorded time in service, even though no failures have yet been recorded. With zero failures in *T* hours, $\lambda_{70\%} \approx 1.2/T$.

IEC 61508 applies the concept of confidence level in failure rate measurements presumably because it is intended to apply to electronic devices comprised of electronic components. Electronic components can be expected to have reasonably constant failure rates, but only in controlled environments. IEC 61709 provides stress models which may be used to estimate the extent of variation in failure rates.

Strictly speaking, statistical confidence levels only apply to electronic components. Composite devices and sub-systems do not have one true value of failure rate that can be measured.

Confidence levels cannot be applied to the measurement of any failures that have variable rates.

Confidence levels might arguably be applied to failure rates of electronic logic solver hardware or of sensor electronic circuits. They could not be applied to sensor mechanisms, process interfaces or to cabling systems.

Certifying bodies such as *exida* apply route 2_H through FMEA. The overall failure rate of a composite device is estimated by summing the failure rates of the individual components. The component failure rates can be based on previous experience in similar applications with the exact same make, type and version of those individual *components*.

Correction factors may be applied for variation in environmental stress factors. The 90% confidence level requirement is applied **at the component level**. In this way route 2_H may be applied even without operational experience with the composite device. A large volume of operational experience is already available for components, though of course different versions of similar integrated circuit chips will have different failure rates.

IEC 61511 hardware fault tolerance requirements

The process sector standard IEC 61511-1 specifies requirements for hardware fault tolerance in §11.4. The requirements are summarised in Table 6. IEC 61511-1 allows the option of applying either IEC 61508-2 route 1_H or 2_H as an alternative to Table 6.

The method summarised in IEC 61511-1 Table 6 is derived from IEC 61508 route 2_H. The method relaxes the requirements for statistical confidence levels:

The requirements are derived from IEC 61508 route 2_H but require 'credible and traceable reliability data' instead of 90% confidence levels. The reliability data may be from 'prior use' or may be drawn from industry-wide databases. The data must be for similar devices in similar operating environments. Prior use with the exact same type is not necessary. And again, 'prior use' in this context is distinctly different from 'proven-in-use'.

IEC 61511-1 Reliability data requirements

IEC 61511-1 defines requirements for reliability data in §11.9, separately from the requirements for fault tolerance in §11.4.

IEC 61511-1 §11.9.3 requires the use of reliability data that are *'credible, traceable, documented, justified and based on field feedback from similar devices used in a similar operating environment'*. This requirement is mandatory, regardless of the source(s) of data, and regardless of how hardware fault tolerance requirements are assessed.

The source of data is left open. §11.9.3 NOTE 1 clarifies that the reliability data may include '*data from general field feedback reliability databases*'. Reliability data could presumably be drawn from prior use or from industry-wide databases such as OREDA and silsafedata.com. Either way, safety function designers need to justify their assumptions and provide documentation supporting the feasibility of achieving the assumed failure rates in operation.

IEC 61511-1 §11.9.4 states that '*reliability data uncertainties shall be assessed and taken into account when calculating the failure measure*'.

IEC 61511-1 §11.4.9 and §11.9.4 requires reliability data with 70% confidence levels, but that needs to be clarified in the standard. Statistical confidence levels cannot be applied to sensor sub-systems or to final element sub-systems.

Strictly speaking, '*certainty'* levels should be applied instead of confidence levels for devices other than electronic components. **The intent of IEC 61511 seems to be that users should select failure rates so that there is less than a 30% chance of exceeding the selected failure rate in operation**.

IEC 61511-1 Requirements for selection of devices

There is no explicit link between the hardware fault tolerance requirements in IEC 61511-1 Table 6 and requirements for prior use. Prior use is explicitly related to requirements for systematic integrity rather than to requirements for faut tolerance.

Requirements for prior use are described in the separate section §11.5, under the heading 'Requirements for the selection of devices'. Devices may either be selected on the basis of prior use or on the basis of compliance with IEC 61508-2 and IEC 61508-3. Systematic capability should be considered for devices that comply with IEC 61508.

IEC 61511-1 §11.5.2.2 states that devices shall be suitable for the operating environment, regardless of whether IEC 61508 compliance or prior use is applied. A note is included to explain that failure rates depend on the operating environment and mode of operation, and that failure rates should be expected to vary.

The requirements in §11.9.3 for credible and traceable reliability data always apply.

It can be concluded that the hardware fault tolerance requirements in IEC 61511-1 Table 6 depend on credible and traceable reliability data. The data may be from prior use or may be drawn from industry-wide databases.

Creative Commons Licence