

COMPONENT ASSESSMENT FOR IEC 61508 – A WORKED EXAMPLE

P R Smith

Moore Industries – Europe
United Kingdom
Contact – prsmith@mooreind.com

Keywords: Random failures, Safe Failure Fraction

Abstract

A 3-wire RTD is used to illustrate the methodology involved with assessing a component for use in a Safety Instrumented Loop.

1. Introduction

1.1 Background

IEC 61508 has now been a fact for over three years. Part 1 was approved for publication at first edition as long ago as December 1998; the first edition of Part 2 (which is the subject of this paper) was published a little later at the end of May 2000.

Despite the increasing age of IEC 61508 it appears to be a still very much maligned and misunderstood document. Most people are probably aware that the standard covers Functional Safety, is particularly applicable to electrical and electronic systems and uses a risk based approach. It is considered 'good' practice, by our friends in the legal field. Should your plant be the one unfortunate enough to suffer a serious accident then litigation may well follow against persons and Companies who see fit to ignore it. It is not and cannot be perfect but I, like many others, believe that it is a very good attempt to provide a consistent design methodology for safety systems. So, let us criticise it only if we are able and our intention is to improve it.

The requirements of Part 2 are not 'rocket science' and do not take a great deal of understanding for any engineer with a reasonable grounding in mathematics and in particular probability theory and statistics. It is quite reasonable to expect that anyone who is designing or integrating equipment on which lives might depend should be competent to deal with the issues that the standard raises.

My objective here is to discuss the hardware assessment process from the perspective of the individual loop component. Note that I do not wish to neglect the crucial issue of software assessment (IEC 61508-3) which is necessary for any instrument whose operation involves the use of software in some way. The issues involved merit a separate article so they must of necessity be left for a future article.

1.2 Supplier Understanding

Recent surveys of instrumentation suppliers indicate that few Companies understand that they have a duty of care when providing equipment into safety applications. This is of great concern as section 6.0 of the Health & Safety at Work Act is quite clear :

The duties placed on designers, manufacturers, importers and suppliers of articles for use at work are to:

- a. Ensure articles are designed and constructed to be safe and without risks to health when being set, used, cleaned or maintained by a person at work
- b. arrange for testing and examination to ensure safe design and construction
- c. provide persons supplied with articles with adequate information about:
 - i. use of the article;
 - ii. Any conditions necessary to ensure safety during setting, using, cleaning, maintaining, dismantling or disposing of the article;
- d. provide persons already supplied with new information as it becomes available.

There is an additional duty on designers and manufacturers to arrange for research to discover and hence eliminate or minimize risks. The Health & Safety at Work Act also places heavy responsibility on software engineers to ensure the integrity of their designs.

I understand that the HSE has applied section 6 of the Health & Safety at Work Act in at least one case concerning instruments intended for use in safety systems and I consequently believe that the onus is upon instrumentation manufacturers to comply with IEC 61508 be they simple sensor or smart instrument suppliers.

1.3 Sub-Component SIL

I have attended many events arranged by bodies such as the DTI, The Safety Critical Systems Club, CASS etc and considerable discussion has considered the issue of individual component SIL. Many engineers believe that an individual loop component cannot have a Safety Integrity Level. This is a technically correct but misleading interpretation and I believe accounts, to some extent, for the apparent neglect of certification so far.

The allocation of a Hardware safety integrity **limit** to an individual loop component is fundamental to IEC 61508 part 2. This allocation is the basis for further safety use of the loop component and is dependent on the availability of a sufficient dossier of evidence to meet the requirements of a specific SIL.

If the conclusion is SIL 2 then that component may ONLY be used to support safety functions upto SIL 2. In practice this means it may be used in safety loops required to provide a risk reduction equal to SIL2 (or lower). A separate assessment will determine whether the loop in its entirety achieves SIL2 but each loop sub-component **MUST** be capable of supporting a safety function upto SIL 2.

IEC 61508 Part 2 requires the provision of certain information, at least:

The fault tolerance that may be assumed for the loop component

The safe failure fraction of all potential failures

The predicted undetected dangerous failure rate – theoretical

The predicted safe failure rate – theoretical

The relationship of failure rate to environmental conditions such as temperature, vibration, emc, humidity etc.

The recommended highest Hardware safety integrity limit

Restrictions in use report including measures and techniques for the avoidance of systematic failures.

1.4 Objectives

Few Companies are supplying this information and many are denying the necessity. This leaves the loop designer with a problem because somehow it is necessary to comply with the standard and provide evidence that the proposed safety loop has been assessed and the predicted risk reduction is reliable.

It is the object of this paper to propose an approach to assessing an instrument using the ‘simple’ example of a 3 Wire Resistance Temperature Detector (RTD). Before I do this let us take a quick look at the two hardware assessments that must be made (not forgetting that if the subject contained software then it would be necessary make a further assessment against the requirements of IEC 61508 part 3) :

- a. Qualitative
- b. Quantitative

Each one of these two assessments produces a Hardware safety integrity limit but it is the lowest estimate of the two that must apply! If assessment a. concludes a capability of SIL1 and estimate b. a Hardware safety integrity limit of SIL3 then the applicable capability is limited to SIL1.

2.0 IEC 61508 SIL Assessment requirements

2.1 Quantitative Assessment – Random Hardware failures

Part 6 of IEC 61508 provides the methodology required to calculate the Probability of Failure to Danger (PFD) that is required to enable a quantitative SIL to be assessed. The IEC 61508 calculation uses fail to danger rates combined with a mean down time assessment to derive a figure for the PFD_{sys} (Average Probability of Failure on demand of a safety function for the E/E/PES safety related system).

A dangerous failure rate and a safe failure rate must be obtained or judged, for each sub-system involved in the safety loop. The calculations of Part 6 actually require the typical failure rate, ($\cong 1/MTBF$) of a device to be resolved into four components:

- λ_{SD} - Detected safe failure rate (per hour)
- λ_{SU} - Undetected safe failure rate (per hour)
- λ_{DD} - Detected Dangerous failure rate (per hour)
- λ_{DU} - Undetected dangerous failure rate (per hour)

Using the guidance provided in Part 6 a Probability of Failure on Demand figure may be calculated and consequently a Safety Integrity Level.

2.2 Qualitative Assessment – Safe Failure Fraction

The standard requires each component in the loop (called a sub-system) to be assessed against the IEC 61508 requirements for Safety Integrity (IEC 61508 Part 2, para 7.4.3).

Each loop component means the field sensor and its installation, all interfacing equipment, any logic modules and all field output devices including final process valves, actuators, positioners, solenoid valves and whatever else may be required to implement the safety function.

The requirement is to determine that each component is suitable for its intended function and this includes the application of existing standards such as EMC. Forgive me if I neglect these and focus on the requirements of the standard itself, suffice it to say that any such complementary standard must be considered and complied with.

The standard identifies two parameters, ‘Hardware Fault Tolerance’ and ‘Safe Failure Fraction’. Two tables within the standard (part 2, para 7.4.3.1.4) are applicable.

For Hardware Fault Tolerance, two cases are considered:

Type A – Effectively simple devices which may or may not include software.

Type B – Effectively complex devices which often do include software.

Simply, we are required to decide whether we have intimate understanding of the device concerned:

Failure Modes of all constituent components?

Behaviour under fault conditions?

Extensive, Reliable Field failure data in support of claimed failure rates?

If the decisions are ‘No’ then the device would be ‘type B’.

If ‘Yes’ then the device would be ‘type A’.

These tables limit the Hardware safety integrity limit that can be claimed for any ‘safety function’ based on its architecture alone and irrespective of how good the quantitative assessment of SIL may be.

Simplified Representation of IEC 61508 Type A (IEC 61508-2 Table 2)

Simplified Representation of IEC 61508

Safe Failure Fraction	Hardware fault tolerance		
	0	1	2
<60%	SIL1	SIL2	SIL3
60% - <90%	SIL2	SIL3	SIL4
90% - <99%	SIL3	SIL4	SIL4
>=99%	SIL3	SIL4	SIL4

Type B (IEC 61508-2 Table 3)

Safe Failure Fraction	Hardware fault tolerance		
	0	1	2
<60%	Not allowed	SIL1	SIL2
60% - <90%	SIL1	SIL2	SIL3
90% - <99%	SIL2	SIL3	SIL4
>=99%	SIL3	SIL4	SIL4

Note:

A Hardware Fault tolerance of 'N' means that 'N+1' faults could cause a loss of the safety function.

The 'safe failure fraction' of a sub-system is defined as the ratio of the average rate of safe failures plus dangerous detected failures of the sub-system to the total average failure rate of the sub-system.

Mathematically:

$$\frac{I_{SD} + I_{SU} + I_{DD}}{I_{SD} + I_{SU} + I_{DD} + I_{DU}}$$

If an assessment has to be made in the absence of manufacturers support then it must be worst case, based on good engineering judgment and with a documented rationale supporting the conclusion. In all but the simplest case the inevitable conclusion must be 'type B'. To achieve even the lowest level of Safety Integrity with a normal commercial 'electronic' instrument it will be necessary to provide a reasoned judgement that 60 – 90% of all predicted failures will be 'safe'. This may be tricky for an analogue instrument but almost impossible for a complex digital instrument containing embedded software.

Remember that this is just part of the assessment and it has to be done for 'each' loop sub-system! Fortunately the design of safety electronics has progressed so far that you will not have a problem obtaining the correct data from such suppliers. Several informed manufacturers of loop components are also actively complying with the standard. So, if the designer chooses wisely then the problem should reduce to just two or three sub-systems.

3.0 Assessment of a 'Simple' sub-system

3.1 Competency

Before proceeding further you will need to assess your own competency to proceed with the assessment. If you are not experienced in instrumentation or at least comfortable with electronics then you should not proceed but obtain the services of a suitably qualified colleague. If you consider yourself to be capable then it will be necessary to begin your safety loop documentation with a brief resumé of your own competence and capability to carry out the assessment.

3.2 Qualitative

i. Fault Tolerance

Few instruments are redundant by design hence it is a safe assumption that a Fault Tolerance of '0' applies (Ref IEC 61508-2 Tables 2 and 3).

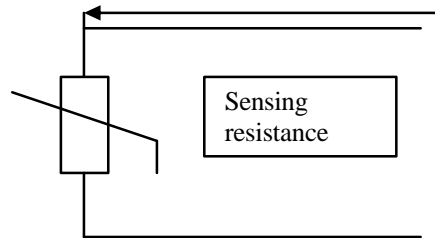
In the case of our 3 Wire RTD we can be certain by inspection that only one fault will result in loss of the measurement.

ii. Safe Failure Fraction

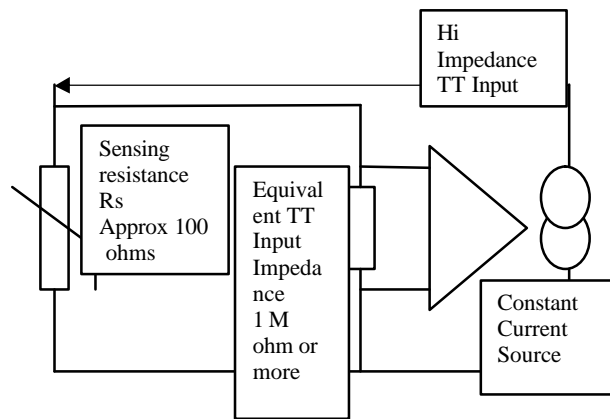
Refer to section 2.2 of this paper for a definition. It is not possible to estimate SFF without some knowledge of the device and its potential failure mechanism.

Fortunately the 3 Wire RTD is a simple device and its failure modes are relatively easy to define:

- a. Equivalent Circuit of the RTD alone, neglecting terminal and interconnecting wiring resistances.



- b. With External sensing and current supply added.



We must consider failure modes with reference to the application as, what is a dangerous failure for a process high trip application may not be dangerous for a process low trip application.

Hence, Failure modes are:

1. Constant Current source connection broken or source failed 'low' prior to sensing amplifier connection.
2. Constant Current source 'drifts' with a consequent impact on the apparent resistance.
3. RTD sensing resistance failed 'open' circuit.
4. Common return line open circuit.

5. RTD sensing resistance, positive terminal open circuit.
6. Input to sensing amplifier 'open' circuit.
7. RTD sensing resistance 'drifts'.

We may now construct a table of failures for the two possible

T5	Low Trip Application		High Trip Application	
	safe	dangerous	safe	dangerous
Failure Mode 1	✓			✓
Failure Mode 2	50%	50%	50%	50%
Failure Mode 3		✓	✓	
Failure Mode 4		✓	✓	
Failure Mode 5		✓	✓	
Failure Mode 6	✓			✓
Failure Mode 7	50%	50%	50%	50%

applications:

We must make an assumption that no one failure mode is more likely than another. In the absence of definitive data this is the only practical course. Note that failure modes 2 & 7 have no bias either way so we must score them 50% to dangerous and 50% to safe.

Hence, for Low trip applications the Safe Failure Fraction may be estimated as 3.0 out of 7, or 43%. For High trip applications the Safe Failure Fraction is estimated as 4.0 out of 7, or 57%.

iii. Conclusion

Using table A of IEC 61508-2 we may conclude that the SIL of any safety function that relies on the RTD in a non redundant configuration is limited to SIL 1 for either case.

Using table B neither are allowed.

Which table should we use?

The Standard requires,

A subsystem can be regarded as type A if, for the components required to achieve the safety function,

- a) *the failure modes of all constituent components are well defined; and*
- b) *the behaviour of the subsystem under fault conditions can be completely determined; and*
- c) *there is sufficient dependable failure data from field experience to show that the claimed rates of failure for detected and undetected dangerous failures are met.*

Fortunately, our investigation of failure modes is thorough and it is therefore reasonable to claim a), *'the failure modes of all constituent components are well defined'*.

It is also reasonable to claim b) because the RTD is a simple device and the effects of external environmental influence can be pretty well predicted.

This leaves c). The word 'sufficient' helps us here because although we would prefer to see the Manufacturers declaration and experience summarised in some degree of self certification, in reality this is not available. We have, however, researched the available published generic data and obtained several different sources so we are confident that the data is dependable and just to be sure we will use the worst case in the calculation of PFD in the Quantitative assessment. Until manufacturers recognise their responsibility and take the necessary steps by publishing adequate data then I believe that this is the best that can be done to both follow the standard, provide reasonable 'evidence' and establish a practical assessment method.

3.3 Quantitative

i. IEC 61508 Certified Equipment.

In the case of sub-systems which have been independently assessed by bodies such as BASEEFA (2001) Ltd or TUV then certification will state λ_{DU} , λ_{DD} , and Safe Failure Fraction from which λ_{SU} and λ_{SD} may be inferred.

ii. Non IEC 61508 Certified Equipment

Generally, manufacturers of non-certified components are not prepared to publish the required data for assessing SIL or propose a self assessment. However, obtaining a written statement to this effect is an essential part of this assessment by an individual working to achieve a 'good' practise solution to the problem of compliance. If the manufacturer will provide a measure of data then you have a starting point, if not then the approach using 'generic' data is justifiable in the absence of acceptable certified components.

iii. Data

There are many useful publications that contain more or less detailed data and it is always a good idea to compare several such data sets. Even when the data is the manufacturers own it is a good idea to calibrate it by comparison with that from generic databases.

Such data is usually given in terms of MTBF, (mean time between failures), the inverse of which approximates to total failure rate per hour for a mature device. Of course, such data is derived from various sources and must consequently be used with care. It is by definition statistically based and the accuracy of statistical information is usually expressed as a confidence level, which is in turn related to the number of samples available. Clearly a failure rate based on a total sample of one will not be quite as convincing or have as great a confidence level as that based on a sample of several hundred.

It is important to have some knowledge of the application conditions under which the data was determined and apply an appropriate factor to account for any differences that may apply to the case being considered. Some typical factors to apply to failure rates based on benign conditions are :

(Ref. D.J.Smith, 'Reliability, Maintainability and Risk')

Quality

- Normal Commercial procurement x 2
- Procured to a specification and quality system x 1
- Subject to 100% burn in x 0.4

Environment

- Dormant with little or no electrical/mechanical stress x 0.1
- Benign x 0.5
- Fixed Ground with no adverse vibration or temp cycling x 1
- Portable or vehicle mounted x 4

iv. Estimation for 3 Wire RTD

For the purpose of this illustration we will use three sets of data applicable to the RTD.

Source One is included in a publication by a well known expert in the field of Reliability

Item	Failure rate in failures per year		
	lowest	-	Highest
Temperature Instrument Sensor	0.00175	-	0.0876

Source Two compiled by a large Petrol Refinery

Item	Failure rate to danger (FTD) per Year		
	Clean Service	Moderate Service	Dirty Service
RTD / PRT	0.01	0.02	0.03

Source Three compiled by a large US Instrumentation Manufacturer

Item	Total Failure rate in failures per year		
	lowest	-	highest
Temperature Instruments RTD	0.0175	-	0.07

v. Which to use?

The three sets of data are reasonably consistent, at the low end a factor of 10 between sources is not too surprising. We don't know anything about sample size and failures of components in identical conditions of use will always exhibit some spread.

Our application may be viewed as 'clean' service but to ensure we err on the pessimistic and hopefully safe side we will use the 'worst' data presented by the Petrol Refinery and check it using our estimate of Safe Failure Fraction and Source three.

vi. PFD Calculation

Note that PFD's are applicable only where the demand rate is low in relation to the proof test interval. Where the demand rate is higher then these formulas will be increasingly in error in the dangerous direction, ie the PFD will be under estimated. IEC 61508 Part 6 Para B.3.2. provides formula applicable to the High demand or continuous mode.

IEC 61508 Part 6 provides the procedure and equations required. Our application will be in an architecture of '1oo1' to trip, i.e. only one sensor will be used and should this result in a measurement that exceeds the defined safety setting of the safety loop then the safety trip will be initiated.

Part 6 para B.2.2.1 gives an equation (applicable to 'low demand mode' only) for a '1oo1' architecture, the average probability of failure on demand is:

$$PFD_G = (I_{DU} + I_{DD}) \cdot t_{CE} \quad (1)$$

Where:

Key to terms:

- T₁ = Proof Test Interval
- MTTR = Mean Time to Repair
- DC = Diagnostic Coverage
- λ = Total Failure Rate per hour
- SFF = Safe Failure Fraction

Channel equivalent mean down time,

$$t_{CE} = \lambda_{DU} / \lambda_D [(T_1/2) + MTTR] + (\lambda_{DD} / \lambda_D) MTTR \quad (2)$$

$$\lambda_{DU} = \lambda / 2 \cdot (1 - DC); \lambda_{DD} = \lambda / 2 \cdot DC \quad (3)$$

In the case of a simple device such as the RTD and in the absence of any external diagnostics, Diagnostic Coverage (DC) = 0

So,

$$\lambda_{DU} = \lambda / 2; \lambda_{DD} = 0 \quad (4)$$

and we may infer that, consequently,

$$\lambda_{SU} + \lambda_{SD} = \lambda / 2 \quad (5)$$

However, we have performed a basic failure mode effect analysis in our qualitative assessment above and this gave us two distinct SFF's dependent upon whether the application relied on a high or a low trip to protect the process.

For the Low trip application SFF = 43%, for the High trip SFF = 57%

Now according to Annex C of IEC 61508-6:

$$SFF = \frac{\lambda_{SD} + \lambda_{SU} + \lambda_{DD}}{\lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU}} \quad (6)$$

As λ_{DD} = 0 and λ_{SD} + λ_{SU} = λ_S then we may simplify the equation to

$$\frac{\lambda_S}{\lambda_{Total}} \quad (7)$$

and hence, **For a Low trip application** we may estimate that $\lambda_S = 0.41 \times \lambda_{Total}$

and by implication,

$$\lambda_{DU} = (1 - 0.41) \times \lambda_{Total} \dots\dots\dots (8)$$

Similarly, for the High Trip application

$$\lambda_S = 0.58 \times \lambda_{Total} \dots\dots\dots (9)$$

And

$$\lambda_{DU} = (1 - 0.58) \times \lambda_{Total} \dots\dots\dots (10)$$

By Calculation :

$$t_{CE} = 1 \times [(T_1/2)+MTTR] + 0.MTTR = (T_1/2)+MTTR$$

For a Proof test interval of one year (8760 hours) and a MTTR (Mean Time To Repair) of 8 hours then

$$t_{CE} = 4388.$$

And

$$PFD_G = (\lambda_{DU}).4388$$

Using the worst case figure of Source 2 (above) this gives

$$PFD_G = (0.03 /8760) \times 4388 = 0.01503, \text{ or } 1.5 \times 10^{-2}$$

Remember that 0.03 is quoted as a dangerous failure hence it is not necessary to use the equations of (8) or (10).

Compare this with the table 2 of IEC 61508-1 and it is clear that this result is acceptably within the range of SIL1. Though it should be noted that the application associated with the failure to danger is not described and hence we cannot differentiate between a high or a low trip.

Repeating the calculation but using the data from source three which is a 'Total' failure rate and using (1) and (2) above we get the results

$$\text{Low Trip } PFD_G = ((0.07 \times (1-0.41))/8760) \times 4388 = 0.0207, \text{ or } 2.07 \times 10^{-2}$$

And

$$\text{High Trip } PFD_G = ((0.07 \times (1-0.58))/8760) \times 4388 = 0.0147, \text{ or } 1.47 \times 10^{-2}$$

Both are comfortably within the range of SIL 1.

4. CONCLUSION

4.1 A 'safe' estimate of the limiting Safety Integrity capability of any safety function that relies on a non redundant 3 Wire RTD in either Low or High Trip applications and with no external diagnostics, is SIL 1.

4.2 To achieve a higher SIL it is either necessary to introduce a more complex architecture, OR improve

the diagnostic levels by using a transmitter that will detect both 'open' and 'short' circuit failures of the 3 Wire RTD and hence remove the failure to danger probability completely. Of course it will then be necessary to demonstrate that the PFD of the Transmitter is adequate for the intended use.

4.3 This paper has proposed an acceptable method for demonstrating the limiting safety integrity of a non certified 'simple' device but it is clear that the difficulties of repeating the task with a more complex instrument, particularly if it makes use of embedded software, will be considerable.

4.4 Manufacturers take note. Instrument Sales in the future are likely to go predominantly to the Companies who have are able to provide a sufficient dossier of evidence to allow the end users to easily carry out their system assessment for the complete loop and to support certification where this might be required.

5.0 DISCUSSION

Reasons for using accredited suppliers or equipment:

1. Evidence is provided by the supplier in the form of either an accredited certificate or a formal report which documents the failure performance of the device. Hence, the task of the end user is minimised.
2. Typically, an assessment of a single sub-system (of the loop) will take 16-24 hours in the absence of supplier co-operation and this work will need documenting as evidence and the result may not be optimum or minimal risk.
3. Project costs and timescales are consequently significantly reduced.
4. Safety is optimised because subjectivity is removed.
5. Compliance with IEC 61508 is assured
6. Regulator concerns are minimised.

Note that this paper is intended to provide guidance only and is necessarily brief. None of the figures quoted here by example should be referenced without corroboration.

Finally, many thanks to all my colleagues both internal and external who have been patient enough to read and comment on the draft copies of this document.