



FUNCTIONAL SAFETY 2014

A Two Day Conference

Organised by

The Institute of Measurement & Control





Functional Safety 2014

DAY 1

1. Welcome & Keynote Speech – Alan Jones
2. Hybrid Applications of IEC 61511, Paper – Laurie Blackmore
3. Hybrid Applications of IEC 61511, Presentation – Laurie Blackmore
4. Managing Functional Safety Standards, Presentation – Audrey Canning
5. Standards Activity – Process Sector Functional Safety, Presentation – Gerry Creech
6. Machinery Sector Functional Safety Standards, Presentation – Stewart Robinson
7. Machinery Standard Cross Reference, Presentation – Stewart Robinson
8. Railway Functional Safety Standards, Presentation – Roger Short
9. Development of a SIL 2 Wireless IR Gas Detector, Presentation – Jorgen Svare
10. Development of a SIL 2 Wireless IR Gas Detector, Paper – Jorgen Svare
11. A Practical view of Risk Reduction Management, Paper – Luis Duran
12. A Practical view of Risk Reduction Management, Presentation – Luis Duran
13. Trip Setting Nomination and Process Safety Time, Paper – Harvey T Dearden
14. Minimising Systematic Failure in Safety Instrumented System Design, Paper – Cenbee Bullock
15. Minimising Systematic Failure in Safety Instrumented System Design, Presentation – Cenbee Bullock
16. Pragmatic Compliance Requirements, Paper – Samuel Rajkuma Vincent
17. Pragmatic Compliance Requirements, Presentation – Samuel Rajkuma Vincent
18. Proof Testing, Presentation – Dil Wetherill

DAY 2

1. Functional Safety – Team of Individuals or Individual Team, Paper – Rob Nicol
2. Functional Safety – Team of Individuals or Individual Team, Presentation – Rob Nicol
3. Application Software integrity, Paper – Neil Wakeling
4. Application Software integrity, Presentation – Neil Wakeling
5. Proof testing Presentation, Stuart Main
6. Annex A of IEC 61508-2 and its effect in SIL Determination, Presentation Dr Hassan El-Sayed
7. Cybersecurity Safety and Security, Presentation O Luis Duran
8. Legacy SIS: When to Maintain or Evolve? Presentation – Rob Pashby & John Walkington
9. Application of IEC61131-6 Programmable Controllers, Presentation – Guido Neumann
10. Managing Functional Safety Competence, Presentation – Paul Reeve

Do we feel safe yet?



Institute of Measurement and Control

4 November 2014

Alan Jones BEng CEng FIET

BG Group Automation Engineering Manager and Functional Safety GTA



Hasdrubal processing plant
Tunisia

BG Group at a Glance



We are an international exploration and production and LNG company.

Facility Types

On and offshore production, LNG liquefaction, Coal Seam Gas ...



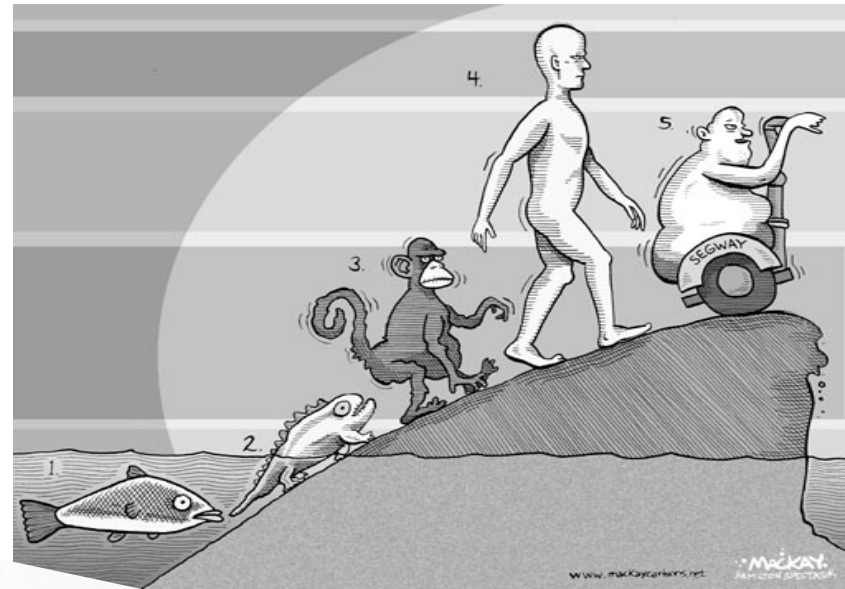
Engineering Support & GTAs

- **Asset Centric Operations**
 - Asset Technical Authorities
- **Central Engineering Resource**
 - **LEAD - SERVE – ASSURE**
 - Discipline Leaders
 - Group Technical Authorities



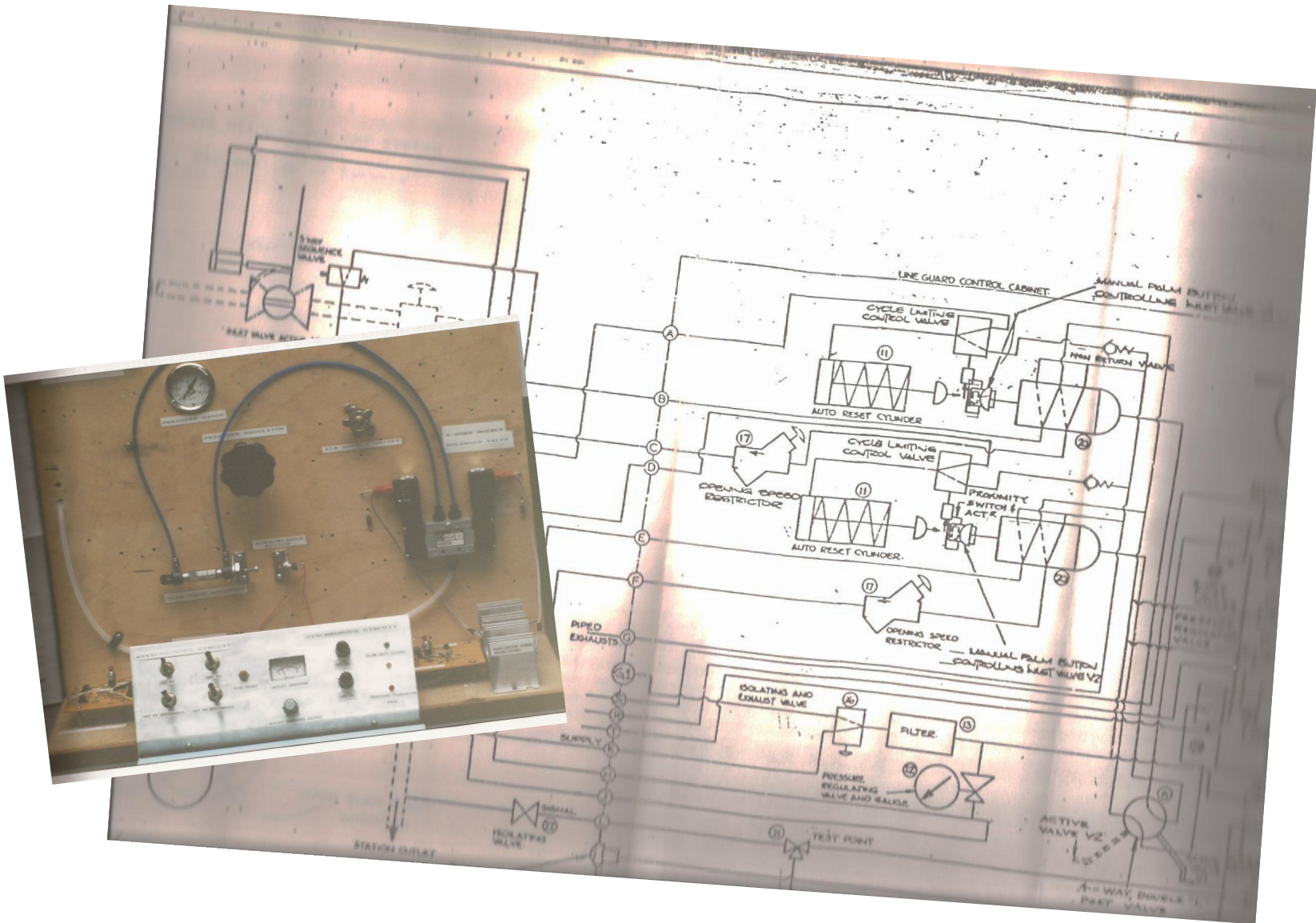
Do we feel safe yet?

- Has the established and practiced approach to *Specifying and Achieving Functional Safety* reached both:
 - Adequate Maturity?
 - Sufficient Application?



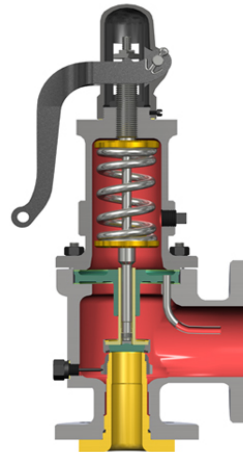
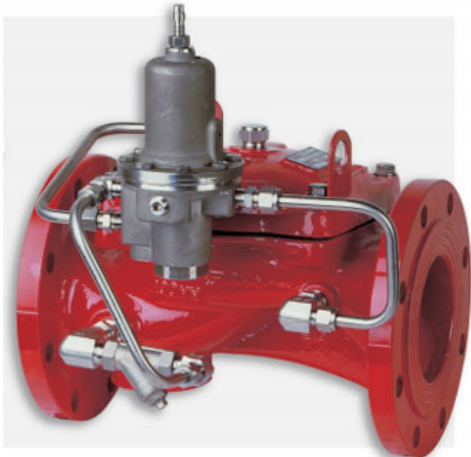
History

Back to the Start - The Uni' Project



Looking back – 25 years ago ...

- *“Functional hmm”*
- Reliability = hardware failure rates
 - λ , MTBF, Fault Trees, RBDs, Markov models
- Safety Systems
 - Mechanical
 - Non-programmable



A Quiet Revolution ...

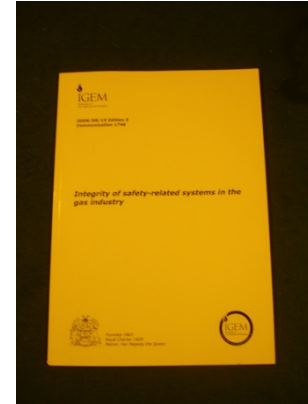
- Programmable systems
 - Well established for Control
 - Honeywell TDC 2000 1975
- *BUT SAFETY??*



How could they be
TRUSTED?

Industry Guidance Develops ...

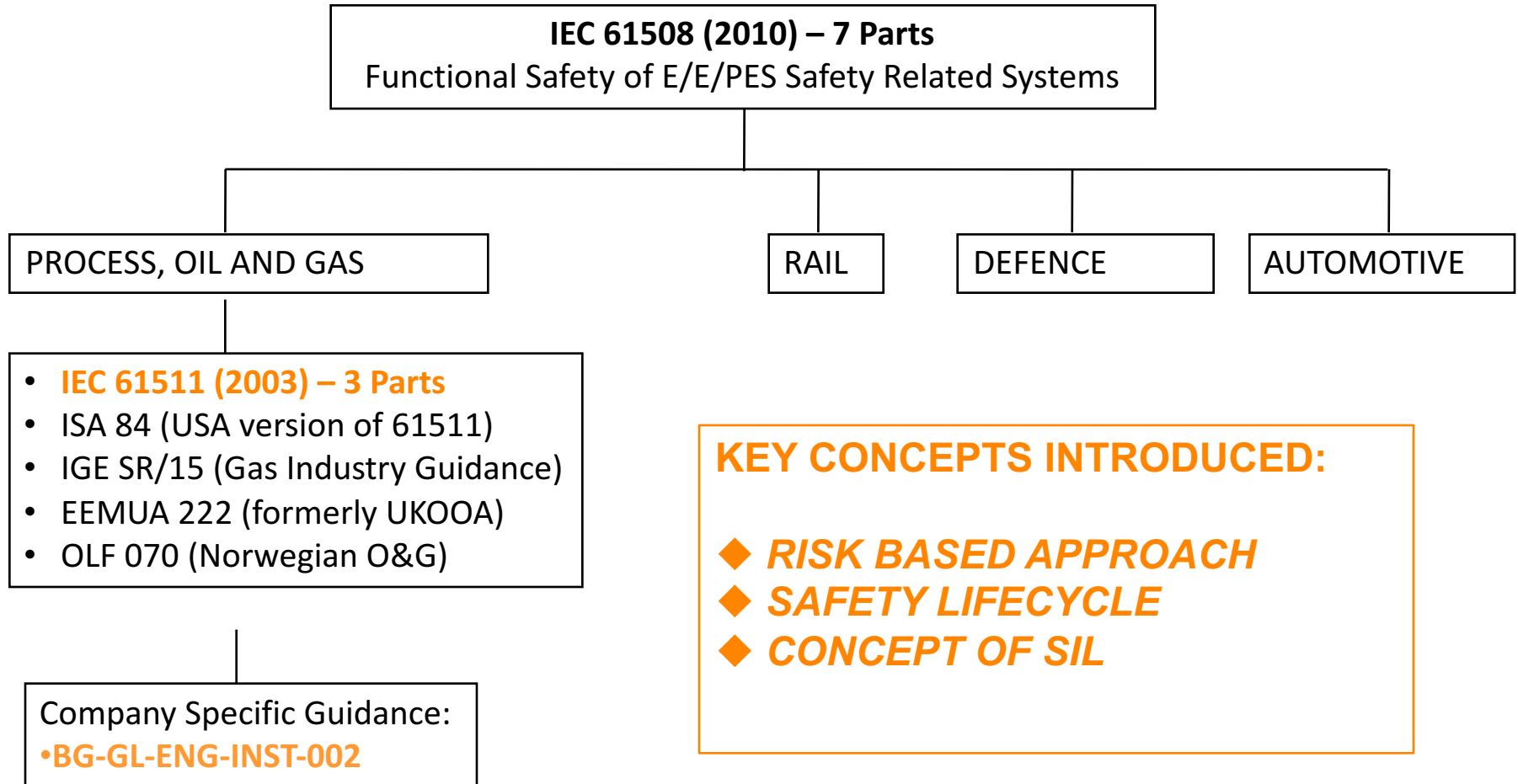
- UK PES 1987
- IGE/SR/15



- IEC

- Guidance to developers in demonstrating systems safe for intended use
- Two studies – one Systems, the other Software
- Combined in 1995 as IEC 1508
- ***IEC 61508 published 2000***

... and Matures



Living with 61508

You don't really know how good it is until you try to use it ...

- 3 years in Trinidad, got married, had a son - how bad can it be?



This bad.

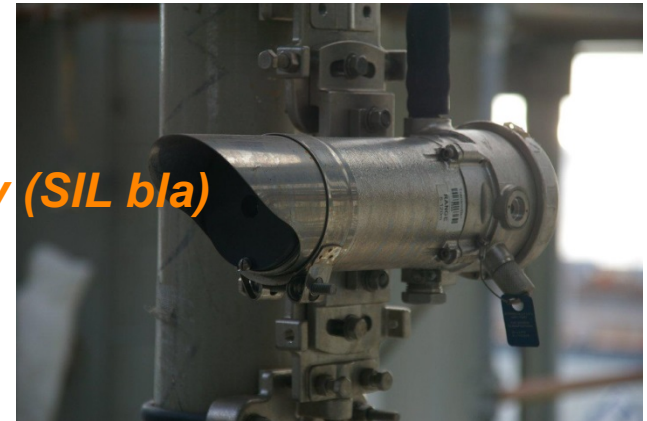
- Application of BG FS Guideline to Offshore platform project
- Many shortcomings, inconsistencies.
- *Total rewrite needed*
- Republished 2010

Living with 61508 – the fire and gas problem

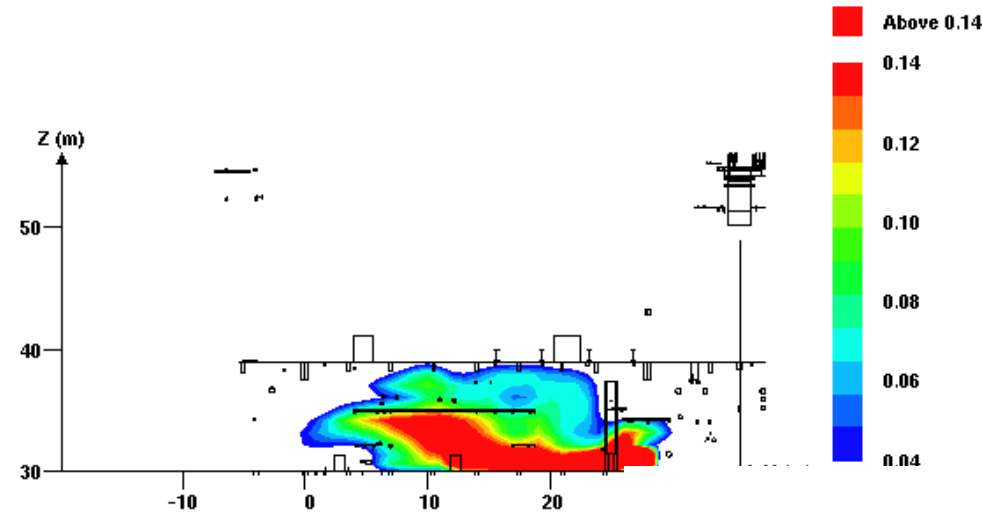
Difficulties with Fire and Gas

- How to apply the risk based approach post event?
 - LOPA, Risk Graph, even quantified approaches do not help
 - UK HSE Hydrocarbon release database:
 - “60% of HC releases detected in open modules”
 - **F&G Detector placement >> detector integrity (SIL bla)**

- One to many relationship ...
 - Achieving even SIL 1 near impossible
 - But just how many final elements actually need to operate?
 - We can't know, but it's not all of them ...
 - Depends where the event (e.g. leak) occurs



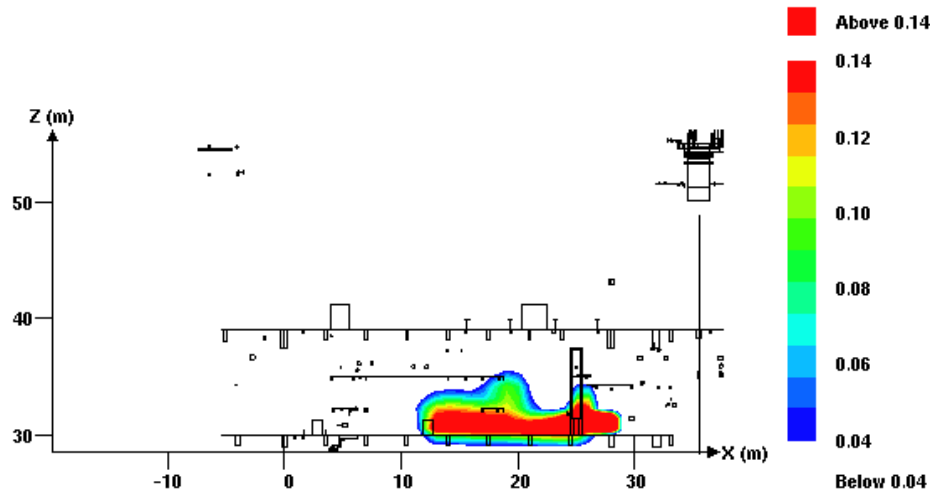
Detector Placement Effect



Gas Detectors Original Configuration

Job=200017. Var=FMOLE (m3/m3). Time= 6.000 (s).
XZ plane, Y=48.5 m

Gas Detectors Revised Configuration



Job=200017. Var=FMOLE (m3/m3). Time= 1.997 (s).
XZ plane, Y=48.5 m

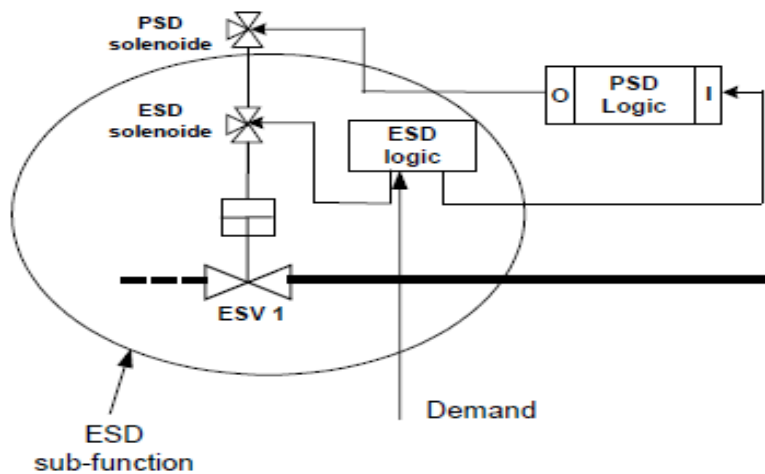
Norway to the Rescue!

- OLF-070 Guideline
- “Unconventional” IEC61508 tertiary guidance
 - Semi prescriptive approach
 - Standard SIFs identified, SILs allocated
 - SIL allocated per what should be *achievable*
 - Implement per SIF architecture
 - Achieve PFD
 - Assumes ISO 10418 / API 14C
 - Non standard SIFs per 61511
- SIL targeting process reduces



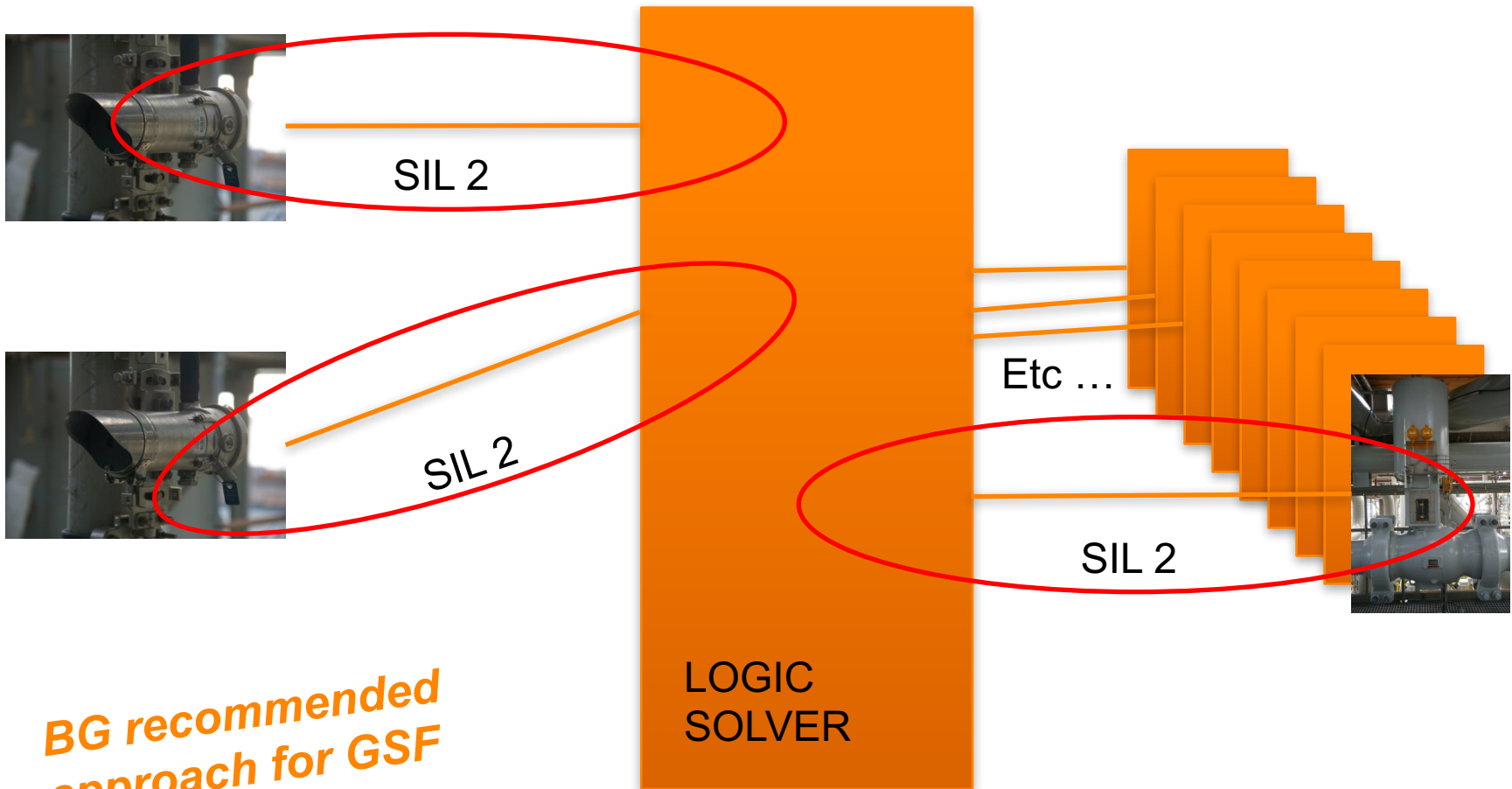
OLF-070 Approach to F&G

- Global SIFs: “functions which typically provide protection for one or several fire cells”
 - Divide into *initiator* and *final element* **SUB FUNCTIONS**
 - E.g. F&G detector sub function target - SIL 2 at 6 month proof test



BG recommended approach for F&G
BUT – Detector placement emphasised

One to Many Relationship ...

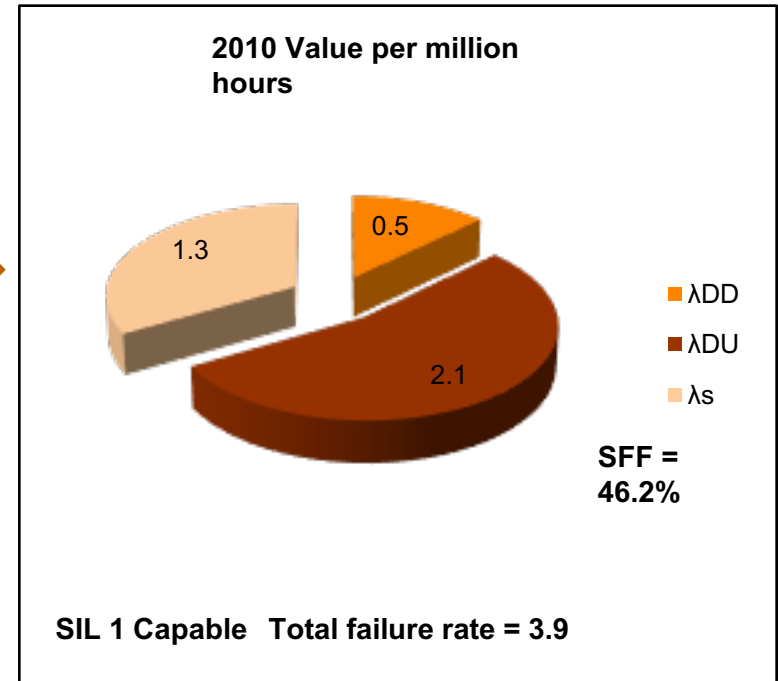
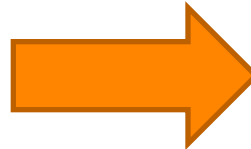
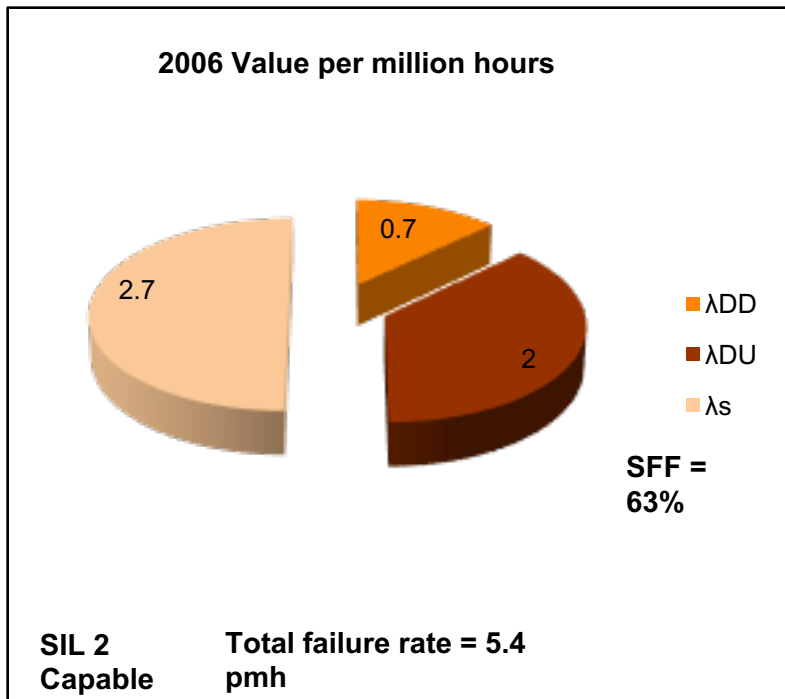


BG recommended approach for GSF

Living with 61508 - Safe Fail fraction

SFF Anomaly

SFF and HWFT - prescriptive elements of risk based standard



The device is better, yet SIL capability has reduced

Living with 61508 - Consistency

Common Mistakes

- *Failing to develop the Consequence*
- *Independence (not)*
 - *Protection Layer selection*
- *Application of Conditional modifiers*
- *Use of multiple alarms*
- *Human Error as a cause*
- *Optimistic data*
- *CCF*



Many differing interpretations of similar situations and base data

Addressing Consistency

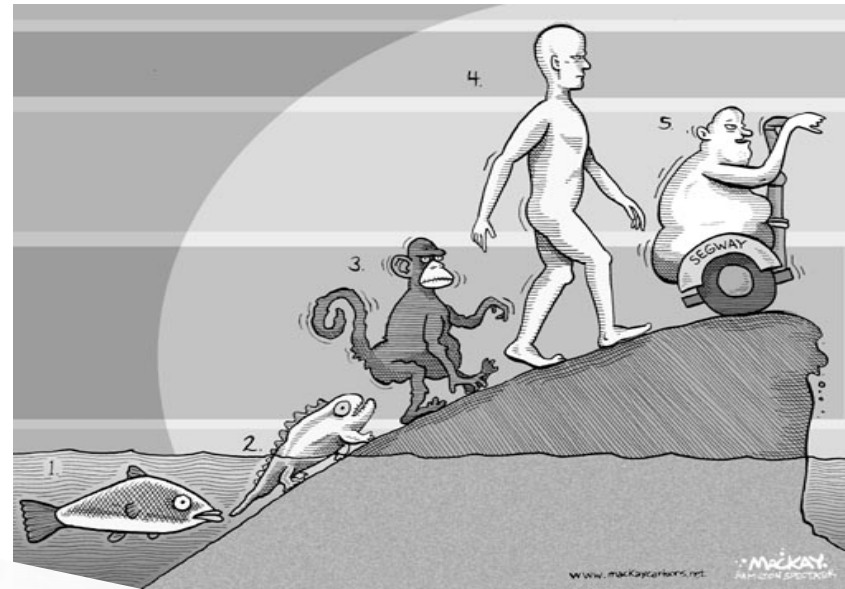
- Integrity review Chairs approved by Functional Safety GTA
- Standard Ignition probabilities table
 - Ignition = Explosion (no POI x POE)
 - Draws from OGP Ignition probabilities paper
- Standard Human Error Rates (HEART / TESEO based)
- Reliability data for common items

LOCATION	RELEASE RATE (kg/s) ¹		
	<0.5	0.5-20	>20
	(Minor)	(Major)	(Massive)
PIPELINE (not Piping)			
Liquid Industrial	0.005	0.03	0.07
Liquid Rural	0.004	0.006	0.007
Gas ⁴ / LPG Industrial	0.006	0.05	0.6
Gas ⁴ / LPG Rural	0.001	0.004	0.05
SMALL ONSHORE PLANT²			
Liquid	0.003	0.03	0.1
Gas ⁴ / LPG	0.003	0.06	0.6

So do we feel safe yet?

Do we feel safe yet?

- Has the established and practiced approach to *Specifying and Achieving Functional Safety* reached both:
 - Adequate Maturity?
 - Sufficient Application?



Do we feel safe yet?

- Industry guidance (IEC 61508 and 61511) is well developed and understood.
 - Risk based approach well accepted
 - Some shortfalls, but we understand them and can work with them.
- Methodologies well established
 - Integrity determination and verification
 - Safety Lifecycle
- Application is widespread within the process industries
 - Some pockets of ignorance
- Functional Safety is well established as a discipline
 - Providing confidence that we are managing risk to industry accepted levels of tolerability
- BUT: New Threats – Process control systems security
 - E.g. Stuxnet, Night Dragon

Complacency is the Enemy



- *We are the weak link*
 - *Maintain Competency*
 - *Address Consistency*
 - *Drive standards improvement*
 - *Be awake to new threats*
- *Be “Healthily Pessimistic”*

HYBRID APPLICATIONS OF IEC61511 WHEN OTHER STANDARDS ARE THE REGULATORY OR CONTRACT REQUIREMENTS

INTRODUCTION:

In many parts of the world such as the USA, Brazil and Africa the regulatory basis for the design of process industry instrumented safety systems is not usually IEC61511 but other standards such as API RP14C or ISO10418. These proscriptive approaches have significant limitations when compared to IEC61508/61511. Typical shortcomings include a lack of a performance specification, no lifecycle requirements and a failure to address systematic or software issues.

To try to address some of these concerns operators are increasingly specifying IEC61511 in addition to any other company or local regulatory requirements. This results in a hybrid design. The extent of the IEC61511 lifecycle that is applied in these hybrid projects varies from part lifecycle such as SIL assessment and SIL validation only, to full lifecycle. This can lead to confusion over the design basis in areas where the standards contradict each other, as well as potential contractual conflict between operator and design contractor over equipment scope and responsibilities. Further complications can arise if the requirement includes asset protection as well as safety and environmental.

The author has been involved in several such projects and will present real examples including:

- Full lifecycle implementation but with retention of all API protection
- API design but with SIL assessment and validation only
- API design but with pre-defined integrity level requirements plus validation

The challenges, benefits, shortcomings and results of these various approaches will be discussed, as will be the general issue of including asset protection in what should be a safety system.

TYPICAL DESIGN BASED ON API RP14C

I will use API RP14C as an example of a proscriptive regulatory design basis since it (and its sister standard ISO10418) are those with which I am most familiar. It is the one extensively used in the offshore industry as the design basis for safety instrumented systems (SIS).

Equipment is categorised by type such as pressure vessels, pumps, heat exchangers etc. and for each category the requirement for instrumented trips is pre-defined. Similarly, requirements for mechanical protection such as relief valves are also defined. These standard designs are not related to the level of safety risk that the equipment presents. Providing the design includes these trips then it is API-compliant. No performance requirements are specified, the mere presence of the trip regardless of the quality of the equipment is sufficient to comply. Similarly, software and systematic fault concerns are not considered. By contrast, and maybe to compensate for potential quality shortcomings, quite onerous test intervals are specified. SIS transmitters must be tested every 3

months and shutdown valves (SDV) every year. These frequent test intervals can in themselves lead to increased risk since testing often involves the placing of people in the hazard zone, or shutting down sections of the plant which then requires a start-up which is a hazard phase of operation. Such concerns over standards such as API were a major element that drove the introduction of risk-based lifecycle approaches such as IEC61508/61511.

For a typical offshore production facility with separation, gas compression, injection etc., there might typically be 200 to 300 SIS “trips”, based on the API approach. When an IEC61511 SIL analysis is carried out there may be as few as 50 safety instrumented functions (SIF) rated at SIL1 or above for personnel safety. (This is often due to the low personnel exposure factors). Similarly, there will be a very few SIFs that require more equipment than would be provided by the API design due to the level of risk they present. As one can see the designs and therefore the equipment to be supplied for these two approaches can be quite different.

WHY HYBRIDS AND HOW MUCH OF IEC61511 ?

Where IEC61511 is not a regulatory requirement for the SIS certification, rather than simply staying with the older proscriptive design it is increasingly common to see contracts placed with both the proscriptive standard and IEC61508/IEC61511 specified in the contract. This could be for a number of reasons including:

- 1)** The person writing the specification for the operator has no idea what they are doing, nor its implications. They have simply been standard-picking without knowledge. (BAD)
- 2)** The operator has made a conscious decision to implement IEC61508/61511 as part of their safety management policy regardless of any regulatory requirements, either across their organisation or for a specific project, because of the benefits it delivers. (GOOD)

Either way, one ends up with a hybrid specification. What then needs to be established is how much of the IEC61511 lifecycle is to be applied. Since IEC61511 is not a regulatory requirement this scope is defined by the operator and must be made fully clear to the designer, usually an EPC contractor, and to avoid later disputes it should either be fully clear in the main specification or clarified by the EPC contractor prior to tendering and contract award. Since the lifecycle could include requirements for competency this could affect the EPC team personnel and the main relevant subcontractors such as the ICSS supplier and major package suppliers. It is essential to establish as a minimum:

- The regulatory design basis. This is the base and minimum requirement
- The scope of the 61511 lifecycle to be implemented
- If it is for personnel safety only or if it includes asset/environmental, reputation

I have been involved with a number of hybrid projects and some examples will follow.

- Full lifecycle implementation but with retention of all API protection
- API design but with SIL assessment and validation
- API design but with pre-defined integrity level requirements plus validation

SCHEME 1 - FULL LIFECYCLE IMPLEMENTATION BUT WITH RETENTION OF ALL API PROTECTION

This approach is in many ways the easiest to understand although it involves the most work. The project was executed just as if it is a regulatory IEC61511 project. This included the development of a lifecycle implementation plan, competency assessments, lifecycle verification, SIS validation and functional safety assessments. The IL assessment and validation was carried out for safety, environment and asset but for this project only safety SIF's were considered for further elements of the lifecycle such as safety requirements specification (SRS), software code reviews and functional safety assessment (FSA).

Because the regulatory basis was the proscriptive standard, all functions related to compliance with that standard were retained in the SIS even though many could have been removed completely or transferred to the DCS on the basis of the SIL assessment. There may even be a little more equipment for any cases where the SIL assessment showed a need for a high SIL design. Similarly, test intervals must remain compliant with the API standard even though in all cases they could have been increased (sometimes significantly) under IEC61511. It could be thought that his design results in an ultra-safe installation, but in my view this is incorrect. The SIS is some three or four times larger than it would need to be under IEC61511 and so results in complexity that in itself can result in increased risk in areas such as testing and spurious trips. Additionally, the high test frequency will further increase the chance of spurious trips and place people in the hazard zone more often than needed. However, at least the equipment quality needed to meet performance standards and (very importantly), systematic issues were addressed for safety functions.

Assuming that SIF loop components will need to comply with IEC61511 related to their SIL rating, this needs to be considered when specifying equipment at the early stages of the project, rather than simply purchasing on a lowest-cost basis.

Since the full lifecycle is implemented, competency requirements for the project team and major package suppliers will need to be enforced.

The addition of the full lifecycle requirements will add man-hours to the project scope and the formal testing and validation related to the later stages could impact schedule. In particular, these schedule implications must be considered from the beginning and understood by project management.

SCHEME 2 - API DESIGN BUT WITH SIL ASSESSMENT AND VALIDATION

This is the most common form of hybrid. The extent of IEC61511 lifecycle implementation ends at SIL validation (and maybe with the production of an SRS).

There are two main benefits resulting from carrying out the SIL assessment and validation. Firstly, for SIL-rated SIF's a performance requirement is specified for the equipment, which is of course a good thing, and assuming the design must meet the architectural requirements of IEC61511 then fault tolerance is provided where needed for high-SIL SIF's.

This design, as with the Scheme 1 approach, results in a "full size" SIS, just as would be required for the base regulatory design. The more onerous testing frequency and its associated potential to

increase risk is also retained. None of the later stage benefits related to software and systematic issues, formal validation, FSA etc., are considered. However, the impact on schedule is minimised. Maybe this is why this hybrid compromise is the most popular!

SCHEME 3 - API DESIGN BUT WITH PRE-DEFINED INTEGRITY LEVEL REQUIREMENTS PLUS VALIDATION

As an example of this approach, I have seen specifications that state that all safety functions must meet SIL2 and then also often identify one or two additional named functions for SIL3 (eg flare drums, HIPPS). This really is the least beneficial type of hybrid, since it rejects the risk-based concept of IEC61511 completely as well as missing out the critically important later stages related to software and systematic faults. Further, these specifications rarely go on to define what is meant by safety functions. A typical SIS will contain a large number of functions (maybe 50% of the SIS functionality) that are not safety related at all. They are “housekeeping” trips consequential to a safety trip, which are placed in the SIS for convenience. This must be clarified at an early stage to avoid confusion and dispute over the SIS design.

This approach will at least have the benefit of specifying performance standards for the equipment via the SIL.

What will result from this type of hybrid is a SIS that is even larger and more complex than the base regulatory design and this approach should be avoided whenever possible. If it is required to implement any content of IEC61511 it should as a minimum include the hazard identification and risk assessment phases.

POTENTIAL BENEFITS FROM HYBRID SCHEMES 1 & 2

Although the design that results from a hybrid is not the optimum that should result from a regulatory IEC61511 approach, schemes 1 and 2 do bring benefits, some of which have already been discussed. These include:

- Understanding of high risk plant areas and maybe even reconsideration of process/mechanical design to reduce risk (inherently safer design)
- Performance standards specified for equipment
- Fault tolerance in design for high risk SIF's
- Attention to systematic faults (scheme 1)
- Competency is considered (certainly for scheme 1 and to a lesser degree for scheme 2)

Further, it may be possible to open dialogue with the regulatory authority with regard to testing frequency. This is certainly feasible for scheme 1 (full lifecycle) although the argument diminishes as the extent of the applied lifecycle is reduced. For instance, it is hard to argue for reduced testing if software and systematic faults have not been addressed.

POTENTIAL BENEFITS FROM HYBRID SCHEME 3

The only benefit is the specification of performance requirements for the equipment via the SIL, but this is probably outweighed by the significantly increased complexity of the overall SIS and its associated testing load.

For all of these approaches it is important to realise that, because the functions required by API RP14C are implemented the SIS is much larger and more complex than it would be if based on IEC61511 for safety SIF's at SIL1 or above. This may well be by a factor of 3 or more. It is also fundamental to remember that since IEC61511 is not a regulatory requirement deviations from the standard can be agreed between the operator and designer. This can include reduction in achieved SIL compared to assessed SIL, less rigorously enforced validation, special consideration for packages, etc.

ASSET PROTECTION AND ITS EFFECT ON SIS SIZE FOR IEC61511 PROJECTS

The implementation of asset protection in the SIS is also a form of hybrid design when the regulatory design basis is IEC61511 (most asset protection is inherently provided in an API RP14C design so asset protection does not have a significant impact if the design basis is API). Asset protection is not generally part of the regulatory basis for a plant since it is a user cost/benefit exercise. However, its implementation is often part of a contract requirement for IEC61511 projects and its implementation methodology is usually addressed via a reference to IEC61511. Understanding the implementation basis in relation to IEC61511 is important in order to fully define the asset protection scope and responsibilities. Its implementation can significantly affect the design and size of the SIS and result in uncertainty about the SIS implementation. There are two main issues addressed here - the basis of asset integrity level assessment, and separation of safety and asset functions into different systems.

The first stage is to define and understand the assessment basis for asset protection. As with personnel safety, the assessment basis must reflect a defined and demonstrated level of tolerable risk. Too often this is ignored when deciding the basis for asset integrity level assessment and an almost arbitrary risk graph is used without true understanding of its implications. If we are to keep a link to the principles of 61511, an approach based on orders of magnitude risk reduction rather than a true cost/benefit analysis, then we need to start by defining the equivalent to tolerable safety risk. This would be the tolerable financial loss per hazard per year. One way to start this off is to look at the (typical) cost per year of the protection function (CAPEX and OPEX), if it were to be implemented. Clearly, the annual loss one is protecting against must be greater than this. Since at the assessment phase we do not know what integrity level is required, and given that the cost of the protection function is quite variable, this number needs to be some average generic cost. We could for instance start with something like \$10k pa, to cover the CAPEX of the protection loop equipment discounted for the project life, plus the annual costs of testing, maintenance etc. The annual loss we are protecting against must be greater than this. The graph or LOPA can then be calibrated to deliver this tolerable financial risk. If this more analytical approach is taken to defining and

calibrating the graph or LOPA then it is likely that the number of asset based SIF's would reduce (because they are not financially justified) and so lessen the overall impact on SIS size.

IEC61511 includes the statement in section 1 (scope) "may be applied in non-safety applications such as asset protection". The intent of this statement is not clear but, since the standard is titled "Functional **Safety** - **Safety** Instrumented Systems for the Process Industry Sector", one could conclude that the suggestion is that the **methodology** could be appropriate to determining performance requirements for instrumented systems for financial protection. It does not follow that the intent was that such functions should be implemented in the SIS. This point is relevant since it is common that instrumented functions to protect against financial loss outnumber those protecting against loss of life by a factor of 2:1. If all these functions are implemented in the SIS then it is perhaps three times larger and more complex than it needs to be for safety protection alone, and so consideration needs to be given to separating these functions into a dedicated SIS and (say) a process shutdown system. Any such requirement needs to be defined and understood by all parties.

Hybrid applications of IEC61511 – Laurie Blackmore

Lawrence Blackmore C Eng, FIET, F Inst MC, TUV FSExp

Gulfstream Engineering

Hybrid applications of IEC61511 – Laurie Blackmore

My background:

- Involved in IEC61508/61511 applications since 1995
- 2001 - 2013, responsible for IEC61511 implementation for a major offshore designer/operator of leased FPSO's
- Projects in West Africa, Brazil, Canada, USA, Norway, Malaysia, Australia, UK
- Various Clients – Petrobras, Petronas, Shell, BP, Exxon, ENI, Talisman, Encana
- Various regulatory authorities
- Projects range from no 61511 content to full lifecycle

Hybrid applications of IEC61511 – Laurie Blackmore



Hybrid applications of IEC61511 – Laurie Blackmore

Regulators eg:

- UK HSE
- USA BSEE
- Canada CNSOPB

SIS Design codes eg:

- IEC61511 (process)
- API RP14C (oil and gas offshore)
- ISO10418 (oil and gas offshore)
- NFPA (boilers)
- IAEA 1116 (nuclear)

CA's eg:

- Det Norske Veritas (DNV)
- Lloyds
- American Bureau of Shipping (ABS)

Regulators, Certifying Authorities and Design Codes

Hybrid applications of IEC61511 – Laurie Blackmore



In many parts of the world IEC61511 is NOT the accepted primary SIS design code for the regulator and/or operator, but is often added to the primary code in the contract either:

- 1) Deliberately by the operator to benefit from 61511 elements or**
- 2) In error by “standard-picking” when compiling the specification**

The designs are different and this leads to HYBRID designs and potential confusion. Scope must be clarified.

Why are there Hybrids?

Hybrid applications of IEC61511 – Laurie Blackmore

Equipment is categorised by type such as pressure vessels, pumps, heat exchangers etc

For each category the requirement for instrumented trips is pre-defined regardless of level of risk

Requirements for mechanical protection such as relief valves are also defined

No performance requirements are specified

Software and systematic fault concerns are not explicitly considered

Onerous test intervals are specified. SIS transmitters every 3 months and SDV's annually

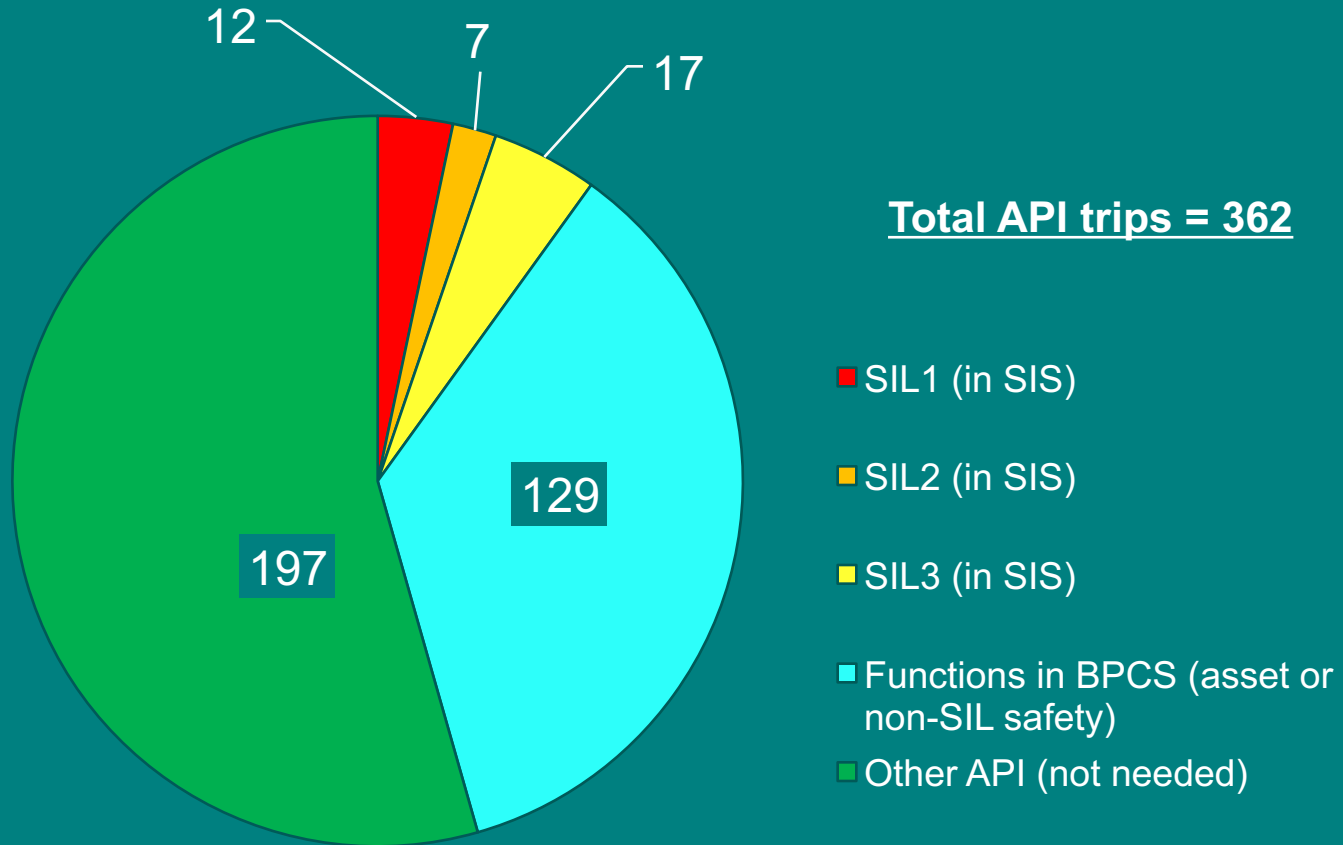
API Design Basis

Hybrid applications of IEC61511 – Laurie Blackmore

- For a typical offshore production facility with separation, gas compression, injection etc. there might typically be 300 to 400 SIS “trips” based on API leading to a SIS with maybe 1000 I/O
- When an IEC61511 SIL analysis is carried out there may be as few as 40 safety instrumented functions (SIF) rated at SIL1 or above for personnel safety or environment leading to a SIS with maybe 100 I/O
- This leads to simpler SIS directed at the high risk functions, with less exposure to systematic failures and more focused testing
- There is a big difference here so a hybrid contract needs clear definition

API SIS compared to IEC61511 SIS

Hybrid applications of IEC61511 – Laurie Blackmore



Example of API and IEC61511 for an offshore installation

Hybrid applications of IEC61511 – Laurie Blackmore

The author has been involved in several such projects with API RP14C as the regulatory design basis and will present real examples including:

- Full lifecycle implementation but with retention of all API protection
- API design but with SIL assessment and validation only
- API design but with pre-defined integrity level requirements, plus validation

The benefits, shortcomings and results of these various approaches will be discussed

Hybrid applications of IEC61511 – Laurie Blackmore

API RP14C is the regulatory design basis BUT the Operator wants to benefit from IEC61511 full lifecycle advantages for areas where API is lacking. Benefits include:

- Establish level of risk for each hazard
- Specify performance requirements related to level of risk
- Design is based on SIL requirements
- Fault tolerance where needed
- Personnel competencies
- Address software issues
- Address systematic issues
- More formalised validation
- Prioritise testing resources

Full lifecycle implementation but with retention of all API protection

Hybrid applications of IEC61511 – Laurie Blackmore

Disadvantages include:

- SIS is as big or even bigger than the non-61511 (API) design leading to increased complexity of operation, maintenance. This increases the risk of systematic faults - the primary cause of major incidents
- Testing frequency is still based on API RP14C (3 months transmitters, 1 year SDV's) rather than (longer) IEC61511 intervals. This reduces ability to focus on the high-risk functions.
- The engineering cost and potential schedule increase associated with IEC61511 is incurred without the benefit of equipment rationalisation or reduced testing costs

Lifecycle/contract issues:

- Make sure it is clear in the contract if IEC61511 applies to only safety or includes asset etc
- Only apply 61511 lifecycle requirements for stages after SIL assessment for safety SIF's at SIL 1 or above? (Clarify in the contract since it has an impact on engineering hours and potentially equipment)

Full lifecycle implementation but with retention of all API protection

Hybrid applications of IEC61511 – Laurie Blackmore

API RP14C is the regulatory design basis BUT the Operator wants to benefit from SIL assessment and design validation. Benefits include:

- Establish level of risk for each hazard
- Specify performance requirements related to level of risk
- Design is based on SIL requirements
- Fault tolerance where needed
- ~~▪ Personnel competencies~~
- ~~▪ Address software issues~~
- ~~▪ Address systematic issues~~
- ~~▪ More formalised validation~~
- Prioritise testing resources

API design but with SIL assessment and validation

Hybrid applications of IEC61511 – Laurie Blackmore

Disadvantages include:

- SIS is as big or even bigger than the non-61511 (API) design leading to increased complexity of operation, maintenance. This increases the risk of systematic faults - the primary cause of major incidents
- Testing frequency is still based on API RP14C (3 months transmitters, 1 year SDV's) rather than (longer) IEC61511 intervals. This reduces ability to focus on the high-risk functions
- The engineering cost and potential schedule increase associated with the elements of IEC61511 is incurred without the benefit of equipment rationalisation or reduced testing costs. **These increases are considerably less than in the previous case.**

Lifecycle/contract issues:

- Make sure it is clear in the contract if IEC61511 applies to only safety or includes asset etc. This affects engineering hours.

This is the most common form of hybrid

API design but with SIL assessment and validation

Hybrid applications of IEC61511 – Laurie Blackmore

API RP14C is the regulatory design basis BUT the Operator has decided to pre-specify integrity levels without SIL assessment. Benefits include:

- ~~Establish level of risk for each hazard~~
- Specify performance requirements ~~related to level of risk~~
- ~~Design is based on SIL requirements~~
- Fault tolerance ~~where needed~~
- ~~Personnel competencies~~
- ~~Address software issues~~
- ~~Address systematic issues~~
- ~~More formalised validation~~
- ~~Prioritise testing resources~~
- The manhours and potential schedule implications are reduced since only SIL validation is required

API design but with pre-specified integrity levels for safety functions

Hybrid applications of IEC61511 – Laurie Blackmore

Disadvantages include:

- SIS is **much** bigger than the non-61511 (API) design leading to increased complexity of operation, maintenance. This increases the risk of systematic faults - the primary cause of major incidents
- Testing frequency is still based on API RP14C (3 months transmitters, 1 year SDV's) rather than (longer) IEC61511 intervals. This reduces ability to focus on the high-risk functions
- ~~The engineering cost and potential schedule increase associated with IEC61511 is incurred without the benefit of equipment rationalisation or reduced testing costs.~~
These increases are considerably less than in the previous case.

Lifecycle/contract issues:

- Since there is no SIL assessment make sure it is clear in the contract to what functions these pre-defined SIL's apply. What is **Safety**? This can have big impact on engineering hours and equipment costs.

AVOID THIS DESIGN BASIS WHEREVER POSSIBLE

API design but with pre-specified integrity levels for safety functions

Hybrid applications of IEC61511 – Laurie Blackmore

A common feature of all these hybrid schemes:

SIS is larger and more complex than an IEC61511 design based on SIF's at SIL1+

For a typical offshore production facility:

Scheme 1 & 2 – Maybe 10% bigger than just API and maybe 3 to 4 times bigger than IEC61511

Scheme 3 – Maybe 30% bigger than just API and maybe 4 to 5 times bigger than IEC61511

Size and Complexity

Hybrid applications of IEC61511 – Laurie Blackmore

A common feature of all these hybrid schemes:

SIS is larger and more complex than an IEC61511 design based on SIF's at SIL1+

For a typical offshore production facility:

Scheme 1 & 2 – Maybe 10% bigger than just API and maybe 3 to 4 times bigger than IEC61511

Scheme 3 – Maybe 30% bigger than just API and maybe 4 to 5 times bigger than IEC61511

There is a similar effect on an IEC61511 implementation if asset protection is included in the SIS – it becomes a hybrid

Size and Complexity

Hybrid applications of IEC61511 – Laurie Blackmore

- **For API RP14C projects**, inclusion of asset protection does not have a significant impact on the SIS since it is generally inherently covered by the API design
- **For IEC61511 projects**, inclusion of asset protection in the SIS can increase the size and complexity of the SIS by factors of 3 or more
 - ❖ Assessment methodology needs to be considered in a logical way
 - ❖ Where any asset functions are to be implemented (in SIS or other system) needs careful consideration

Asset Issues

Hybrid applications of IEC61511 – Laurie Blackmore

Assessment methods:

(1) True cost benefit analysis - Need to know cost of SIL

- Cost of SIL1 can vary by a factor of more than 100 !
- Cost increase of SIL1 to SIL2 could be minimal (not x 10)
- Cost increase of SIL1 to SIL3 could be only a factor of 2 (not x 100)
- **IEC OOM approach not suitable – use alternative analysis for true cost/benefit**

Asset Assessment Issues

Hybrid applications of IEC61511 – Laurie Blackmore

Assessment methods:

(2) Use 61511 OOM approach (not really cost/benefit for reasons above)

- Need to define tolerable \$ risk per year as starting point for graph calibration or LOPA TMEL
- Implementing an asset SIF costs money (CAPEX and OPEX) so tolerable risk must be $>$ that cost, say $\times 10$ to result in an IL1 function
- BUT implementation cost is variable (as above) so maybe take a generic figure?

Most asset assessments result in more protection than is justified

Asset Assessment Issues

Hybrid applications of IEC61511 – Laurie Blackmore

Implementation location:

- Asset protection functions are often more numerous than safety protection functions
- Is it correct to increase the size and complexity of the SIS by including these asset functions?
- IEC61511 says “may be applied in non-safety applications such as asset protection”
- Is this referring only to the methodology? There is no specific detail about system location
- Proposal is to locate asset-only functions (and “housekeeping” functions) in a separate system (PCS, PSD etc). This keeps the SIS for safety and there is no confusion regarding where IEC61511 applies.

Asset Implementation Issues

Thank You

Laurie Blackmore
Gulfstream Engineering
www.gulfstream-engineering.com

Hybrid applications of IEC61511 – Laurie Blackmore

Managing Functional Safety Standards

Audrey Canning
Virkonnen Ltd.

November 2014

Introduction

- Background
- International Standards Organisations & BSI Governance
- Standards Development Process
- What can go Wrong?
- How you can get Involved (without waiting 25 years)

Background

- Late 1980s – informal advice to BSI GEL65/1
- Early 1990s – appointed to GEL65/1, nominated by IET
- Mid 1990s – appointed UK Expert to IEC 61511 WG NP
- Late 1990s – appointed UK Expert to IEC 61508/3 Ed2 WG
- Mid 2012 – appointed Convener IEC 61508/3 WG
- April 2013 – convened ad hoc WG that developed NP31
- Jan 2014 – appointed Chairman BSI GEL65/1
- April 2014 – attended IEC65 Convention in capacity of IEC 61508/3 WG Chair + UK delegation leader
- May 2014 – appointed member NP31
- Mid 2014 – convened IEC 61508/3 preparation WG
- Sept 2014 – attended training!

Virkonnen

Background

- ACOS: Advisory Committee on Safety
- CD : Committee Draft
- CDV : Committee Draft for Vote
- FDIS : Final Draft International Standard
- IEC : International Electro-technical Commission
- NC : National Committee
- NO : Nominating Organisation
- NP : New Work Item Proposal
- RV : Report of Voting
- SPSC : Standards Policy and Strategy Committee
- TC : Technical Committee
- WG : Working Group

International Governance

- IEC : not-for-profit, non-governmental
- Membership : 83 National Committees
- ISO/IEC Directives Part 1 : Basic procedures for development of international standards and other publications
- ISO/IEC Directives Part 2 : Rules for the structure and drafting of international standards (CEN/CENELEC & BSI have similar guidance)
- Appoints Technical Committees (TCs)

International Governance

- NC requirements :
 - representative of country's interests
 - decision making processes influenced by all stakeholders
 - provide open access and balanced representation
- NCs responsibility : Appoint experts and delegates to IEC TCs and WGs

BSI Governance

- UK's National Standards Body under MOU with HMG
- Royal Charter 1929 The British Engineering Standards Association
- Funded by HMG for “ring fenced” activities 2013 :£4.32M
- Required to:
 - publish standards in accordance with BS 0
 - satisfy HMG's obligations under EU Directive 98/34
 - represent UK in International Standards organisations
 - consider “public policy interest” as agreed with HMG

BSI Governance

- 2 membership categories
 - c10,000 Committee Members (no voting rights)
 - c15,000 subscribing members (AGM vote + discounts)
- Governing Body : Board of Directors elected at AGM
- Board appoints Standards Policy and Strategy Committee – includes external members
- SPSC creates BSI (shadow) TCs & appoints chairman

BSI Governance

- GEL65/1 Scope
 - UK input to IEC SC65A : generic aspects of systems used in industrial-process measurement and control
 - operational conditions (including EMC)
 - assessment methodologies
 - functional safety
 - operation of systems as a whole
 - compatibility of main elements of the systems
- TCs identify UK Nominating Organisations (NOs)
- NOs appoint TC members
- TC chairman leads deliberations to establish consensus

BSI Governance

- Requirements on NOs : (BS 0 \$ 7.3)
 - formally constituted, appropriate TORs
 - open and non-discriminatory membership
 - authoritative voice for defined interest(s)
 - committed voluntary active support for consensus-based standards
- Gel65/1 NOs
BCS, EEMUA, GAMBICA Inst MC, Energy Institute, Lloyds Register, MIRA, SaRS, , Oil and Gas UK, HSE, The Conformity Assessment of Safety-related Systems, Energy Networks Association, Inst. of Gas Engineers and Managers, The 61508 Association, The Institute of Ergonomics and Human Factor, Secretary - IEC/SC 65
+7 Individual Capacity Experts appointed to IEC TCs/WGs

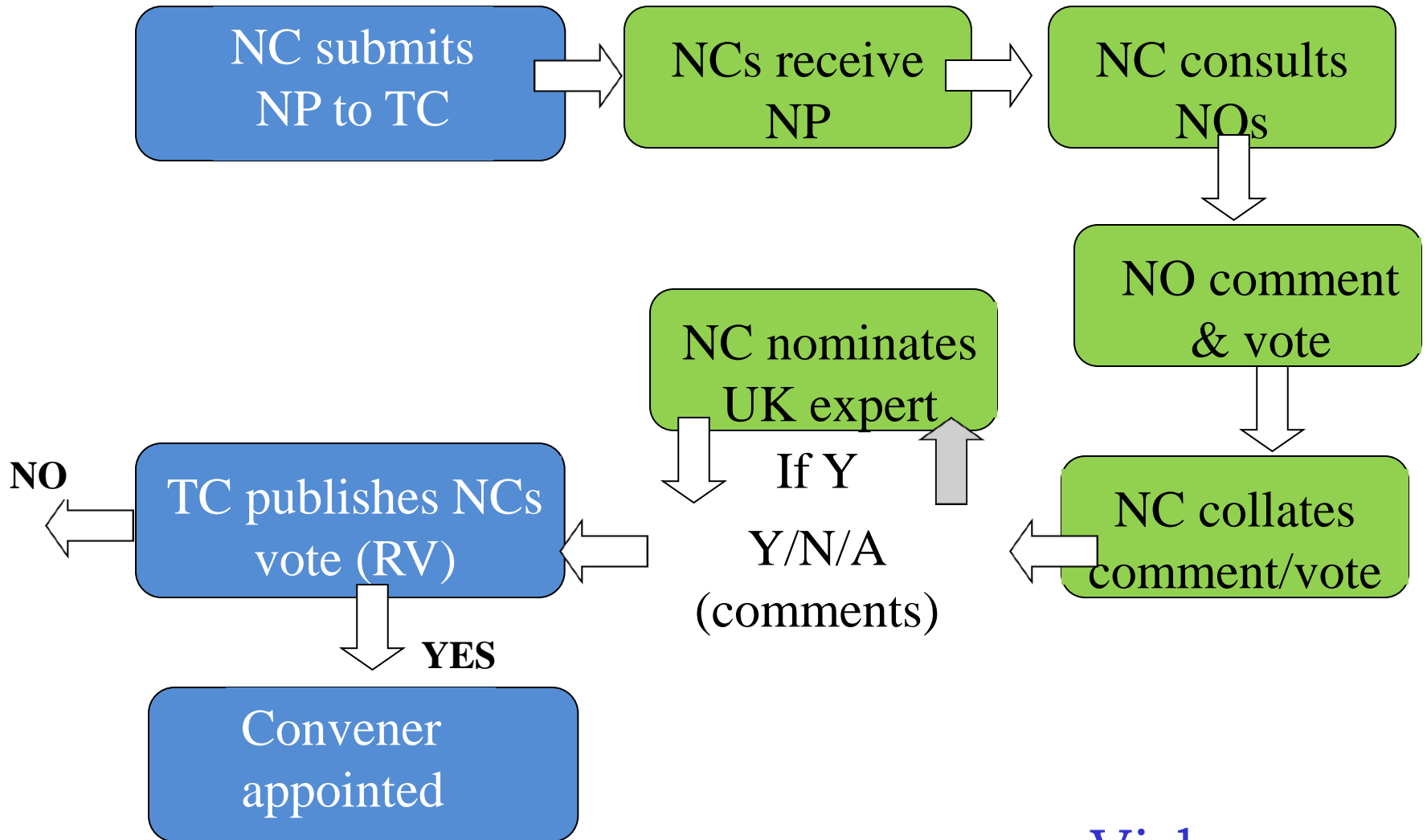
BSI Governance

- Requirements on Chairmen
 - establish UK view in Int'l and EU standards
 - alert BSI to imbalance in membership
 - act impartially (put aside particular org or interest)
 - ensure all views heard
 - compliance with BS 0
 - have suitable technical expertise, but not-pre-eminent
 - understand application of standards for which TC responsible

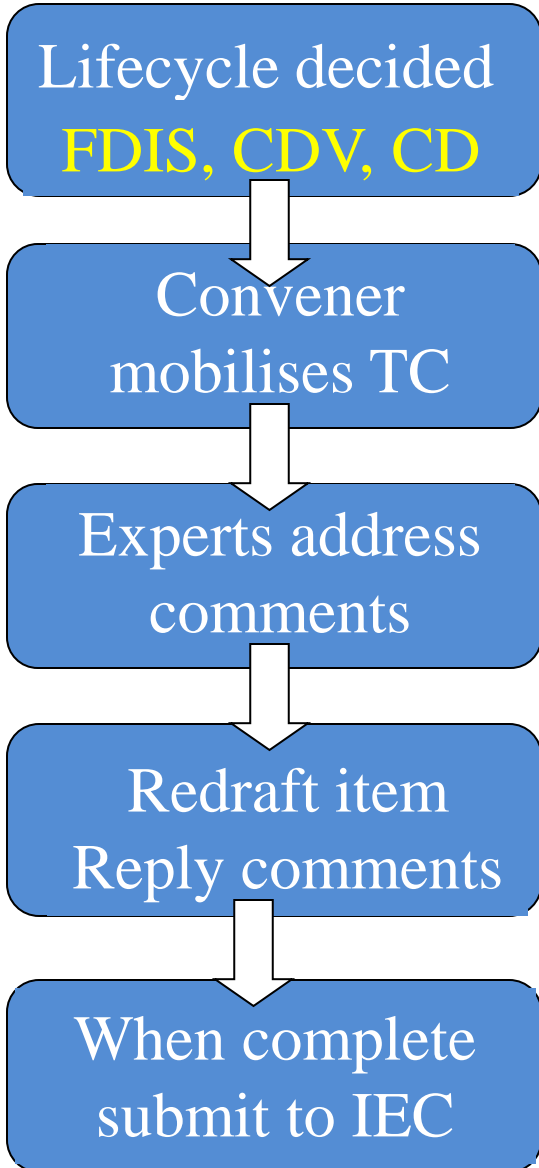
BSI Governance

- Requirements on TC Members
 - comply with BS 0
 - contribute own expertise and represent the interests of their nominating organisations
 - act in good faith with due diligence and vigilance
 - ensure standard technically sound, free from commercial bias & consistent with BS 0
 - follow BS0 IP policy
 - formally declare any potential conflict of interest

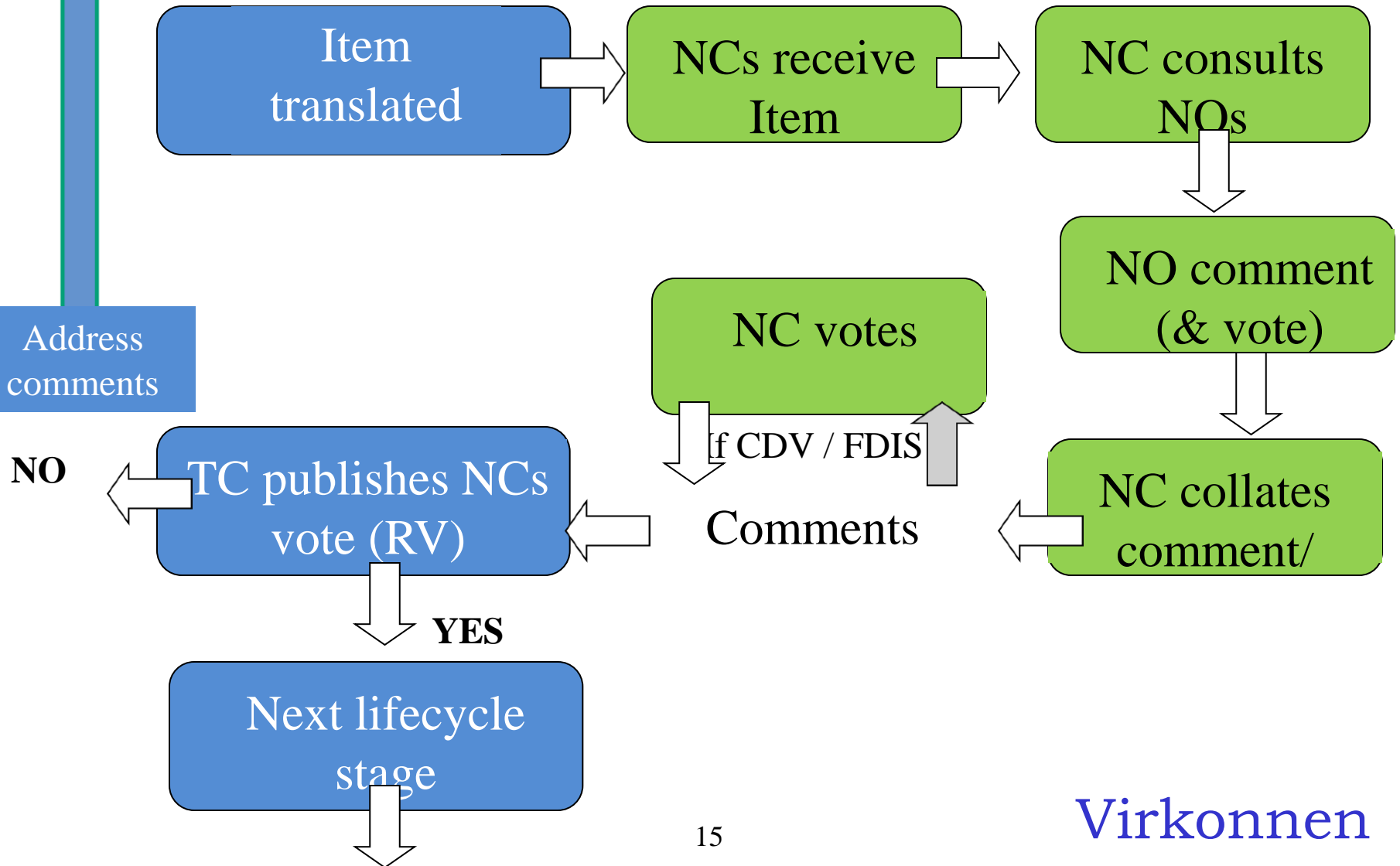
Standards Development Process



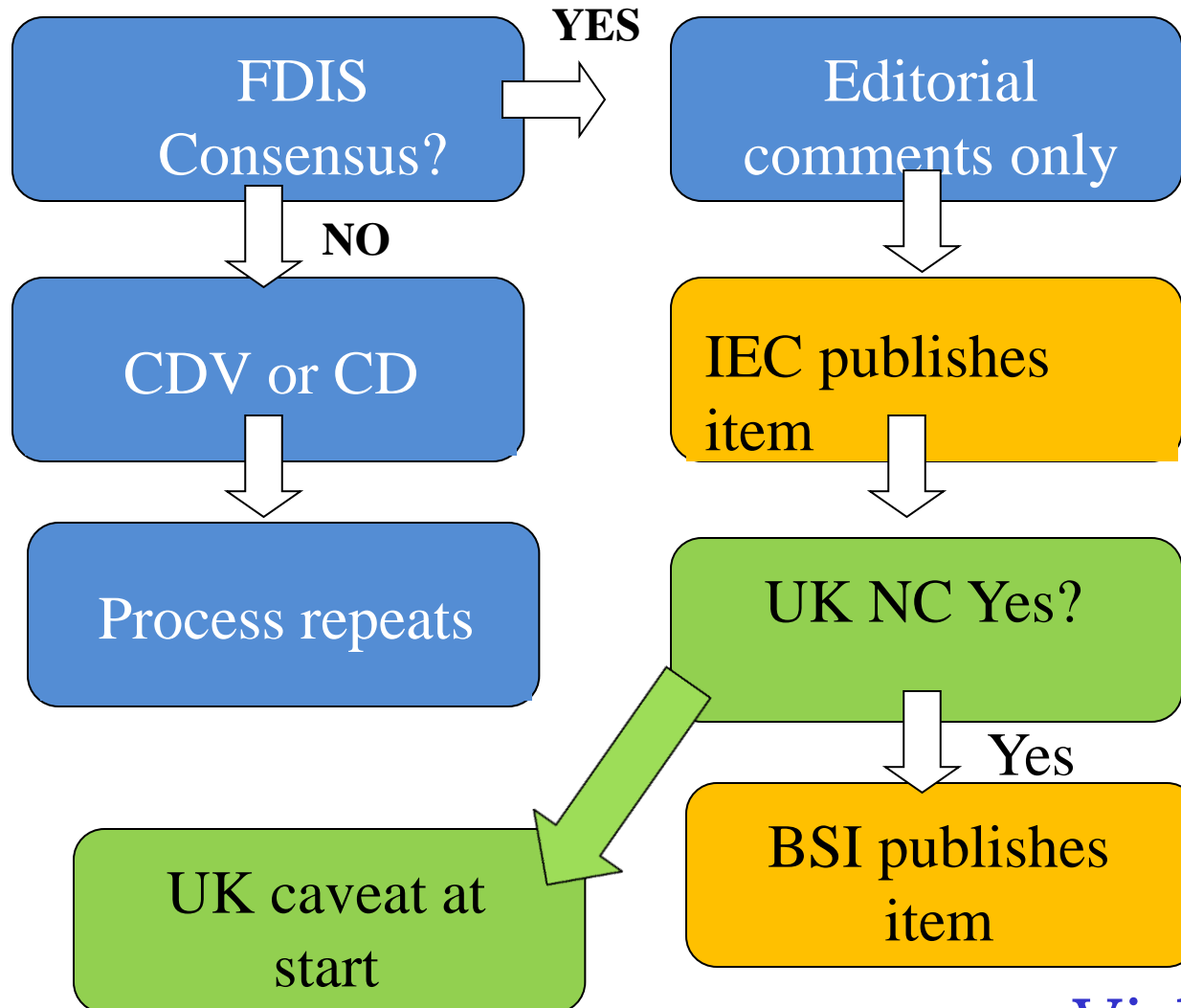
Standards Development Process



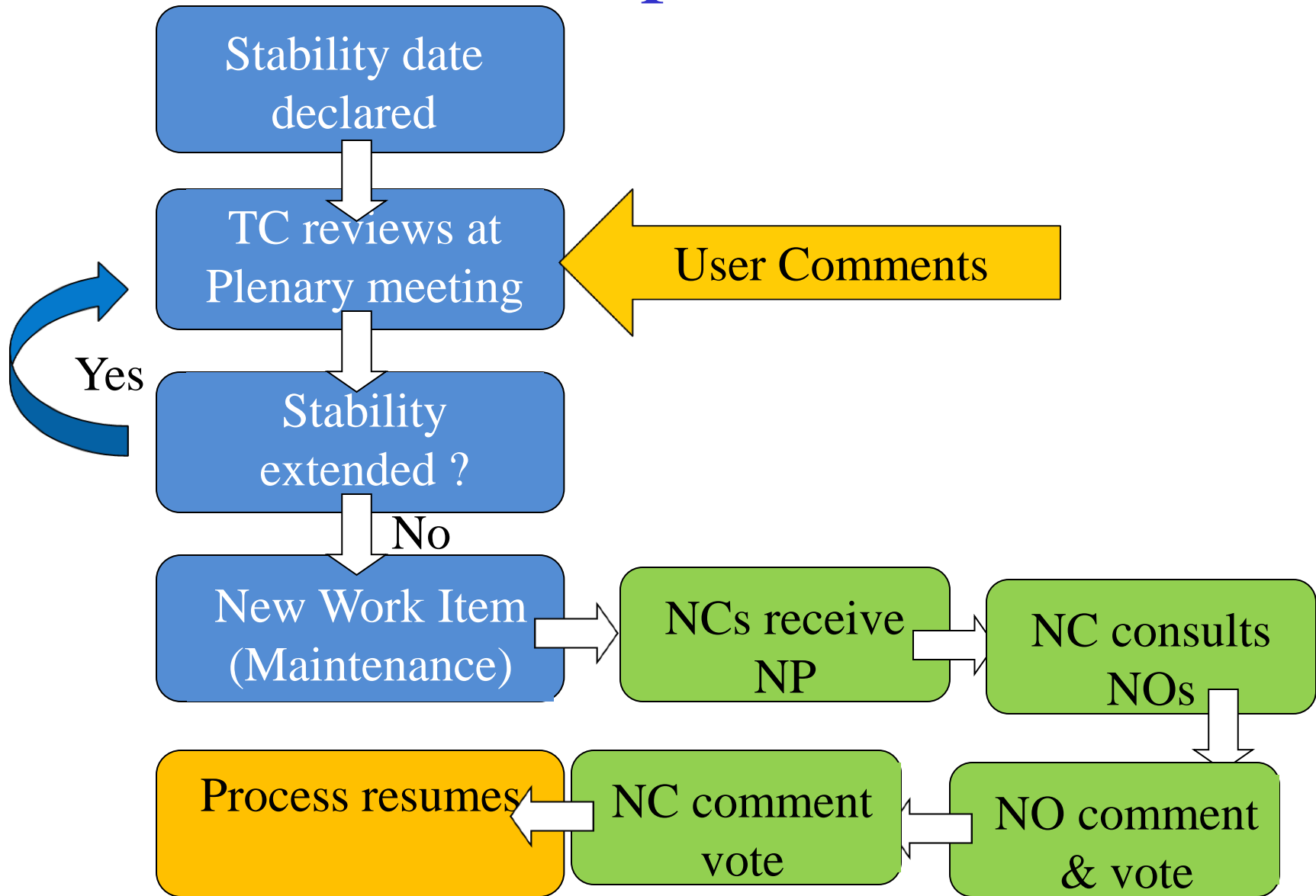
Standards Development Process



Standards Development Process



Standards Development Process



Standards Development Process

- Reasons to maintain:
 - outstanding technical comments from FDIS
 - ad-hoc comments on usability received
 - new knowledge and processes since published
- Reasons to NOT maintain:
 - change imposes cost on standards users
 - costly in volunteer time & effort
 - new input requires new consensus forming

What Can Go Wrong?

- Multiple Languages
- Too much haste in carrying point
- Richness of the English language
(Side benefit of the French translation!)
- Divided by a common language
(Essential standards tool – OED)

What Can Go Wrong?

- Regulatory and assessment differences
- Everything which is not allowed is forbidden
- Everything which is not forbidden is allowed
- Everything is allowed even if it is forbidden

What Can Go Wrong?

- Sector & application differences
(e.g. level of control)
- Codes of Practice /Sector norms
(e.g. Industry/Medicine/Defence)
- Application characteristics
(e.g. Response time
Process safety time
Existence of a safe state)

What Can Go Wrong?

- Timing of technology intercepts
- Length of time to develop consensus
- Complexity of the subject matter
(ideal vs. realism e.g. lifecycle
immediate vs. influencing e.g. tools
application vs. product e.g. notations)
- Emergence of new methods – OO, Agile

What Can Go Wrong?

- Perceived role of Standards
 - Level playing field
 - Leading the field
- Diverse backgrounds of participants
 - Participants motivation
 - The IP issue

What Can Go Wrong?

- Upshot
 - extrapolate to generic agreement
 - erosion of “onerous” requirements
 - progressive divergence
 - multiple conflicting standards for same applications
 - barriers to trade/competence

(Containing) What Can Go Wrong?

- We need a “gold standard” – otherwise all standards are liable to sacrifice
- It will of necessity be generic – to gain consensus and survive technology change
- It will be a compromise – too onerous for some, too lax for others
- And if it aims to cover cradle to grave E/E/PES engineering it will NOT be short !

(Containing) What Can Go Wrong?

- ACOS : coordinates work across TCs to ensure consistency in IEC safety standards
- ISO/IEC Guide 51 - inclusion of safety aspects
- IEC Guide 104 - preparation & use of Basic Safety / Group Safety publications. Relationship between Group Safety Functions and product TCs (+ other application specific Guides)

How can you get involved?

- Identify your NO (or potential NO) & get nominated to relevant NC – we have both attending and corresponding members
- Identify your NOs rep and intercept his circulation (you will benefit from sight of CD, CDV & FDIS drafts)
- Respond to (any) NOs call for comments – for UK every comment is addressed, initially by NC, then by TC
- Ask to see the responses

Virkonnen

Conclusions

- International standards bodies and BSI have extensive governance procedures - which are applied
- In the UK the role of the NO is critical to enable their members to influence standards
- To avoid erosion affecting all - we need a reference standard for functional safety - for all the criticism of its faults I haven't found a better one than IEC 61508!

Process Sector Functional Safety

GERRY CREECH

A solid blue horizontal bar at the bottom of the slide.

IEC 61511 Ed 2 Timeline

Committee Draft For Vote (CDV)

- Released for vote early 2014
- National committee comments now in.
- Approx. 310 comments from 11 of the 28 countries that voted.
- 26 of the countries voted in favour of the standard and 2 against.
- Most comments are editorial, about 90 are technical with many duplicates.
- Some countries have stated that IEC61511 needs to be modified to bring it more in line with IEC 61508 requirements (included in the 90 technical), which is a requirement of IEC Guide 104.
- Maintenance committee due to meet in Cologne on 8th – 11th December.
- Adjustments need to be made ready for release of FDIS for vote during 2015.

Some key changes in edition 2

Terms, definitions and abbreviations

- More closely aligned with IEC 61508

Edition 2 is Based on IEC 61508 route 2H

- Hardware fault tolerance defined by table 6 (no Safe Failure Fraction)
- Route 1H can be used by going to IEC 61508

Systematic Capability

- Largely built into requirements.
- Components / elements assessed in accordance with IEC 61508 must be used in accordance with IEC 61508 Systematic Capability requirements.

BPCS as a protection layer

- Clarification has been added regarding the number of BPCS independent protection layers that can be used for a given hazard.

Software

- Some parts of edition 1 section 12 have been distributed to the appropriate lifecycle clauses.

Security

- Clauses for security have been added.
- This a specialist subject in it's own right, so the standard points to other standards for detailed guidance.

Systematic Capability

- When using an element or device that has been designed in accordance with IEC 61508, the Systematic Capability is determined from tables and measures defined in IEC 61508 parts 2 & 3 as part of the original design / assessment.
- Hardware fault tolerance in both IEC 61508 and IEC 61511 is defined as “ability to continue to perform a required function or operation in the presence of faults or errors”.
 - i.e. hardware fault tolerance = 1, means that the function will still operate in the presence of 1 undetected fault.
- When considering Systematic Capability, Two identical elements or devices are likely to be affected by the same systematic faults.
 - So if one device fails due to a systematic fault, then a second identical device in the same environment is likely to fail at the same time.
 - Therefore two identical devices may not meet the Systematic Capability criteria required.
 - i.e. two identical devices each with SC=2, if used in a 1oo2 configuration so that they will have 1 level of hardware fault tolerance, will only meet SIL 2 requirements, even though they may meet the hardware fault tolerance and PFD / PFH requirements for SIL 3.
- The above information is not always clear in product safety manuals.

Summary

- IEC 61511 Ed 2 is largely based on IEC 61508 route 2H.
- FDIS currently scheduled for vote during 2015.
- Hardware fault tolerance requirements defined without the need to calculate the safe failure fraction.
- Requirements directly related to IEC 61508 assessed element / devices are not duplicated in IEC 61511, but must still be met.
- Some changes are likely to occur between the CDV and FDIS versions to comply with IEC Guide 104.

FS 2014

Machinery Sector
Functional Safety Standards

Machinery Sector Functional Safety Standards

- In the machinery sector there are two key standards for functional safety.
 - ISO 13849 (Parts 1 &2)
 - IEC 62061
- Both “harmonised” to the Machinery Directive
 - (Presumption of Conformity)

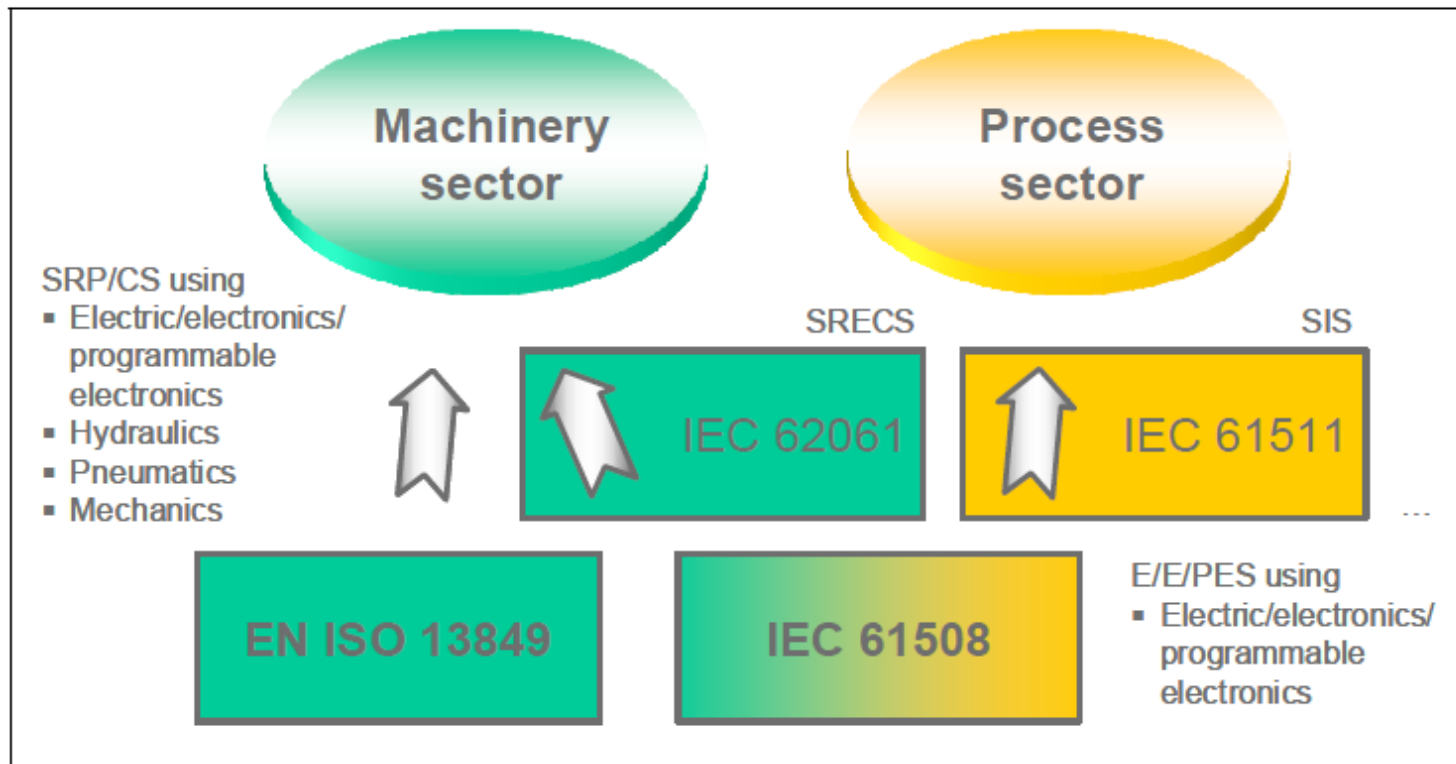
Machinery Sector Standards

Figure 3.1:

Scope of various generic standards concerning functional safety;

SRP/CS: safety-related parts of a control system; SRECS: safety-related electrical control system;

SIS: safety instrumented system; E/E/PES: electrical/electronic/programmable electronic system



Source: BGIA Report 2/2008e

Technical Reports

- Technical reports were issued by both the IEC and the ISO in 2010
 - ISO/DTR 23849 and IEC/TR 62061-1
- “Safety-related control systems can be designed to achieve acceptable levels of functional safety using either of the two standards by integrating non-complex SRECS (safety-related electrical control system) subsystems or SRP/CS (safety-related parts of a control system) designed in accordance with IEC 62061 and ISO 13849-1, respectively.

Technical Reports

- “Both standards can also be used to provide design solutions for complex SRECS and SRP/CS by integrating electrical/electronic/programmable electronic subsystems designed in accordance with IEC 61508.”

Technical Reports

- “Both standards currently have value to users in the machinery sector and benefits will be gained from experience in their use. Feedback over a reasonable period on their practical application is essential to support any future initiatives to move towards a standard that merges the contents of both IEC 62061 and ISO 13849-1.”
- “Differences exist in detail and it is recognized that some concepts (e.g. functional safety management) will need further work to establish equivalence between respective design methodologies and some technical requirements.”

ISO 13849 Current Status

- DIS of 13849-1 Amendment 1 released for voting August 2013
- Includes some technical changes as well as updated references
- Publication possibly during Qtr. 3 2015
- ISO 13849-2:2012 Safety of machinery — Safety related parts of control systems
 - Part 2: Validation

IEC 62061 Current Status

- IEC 62061:2005 +A1:2013
 - Incorporating corrigenda July 2005, April 2008 and February 2010
- The standard is in “Maintenance Phase” and no further work is planned whilst the work to merge the standards is in progress

IEC/ISO 17305

- Still at a very early stage
- Scope is to “combine” IEC 62061 and ISO 13849
- First CD should be published by the end of this year
- No reliable prediction of publication date
- Perhaps unlikely to be before 2018!

Cross Reference Guide

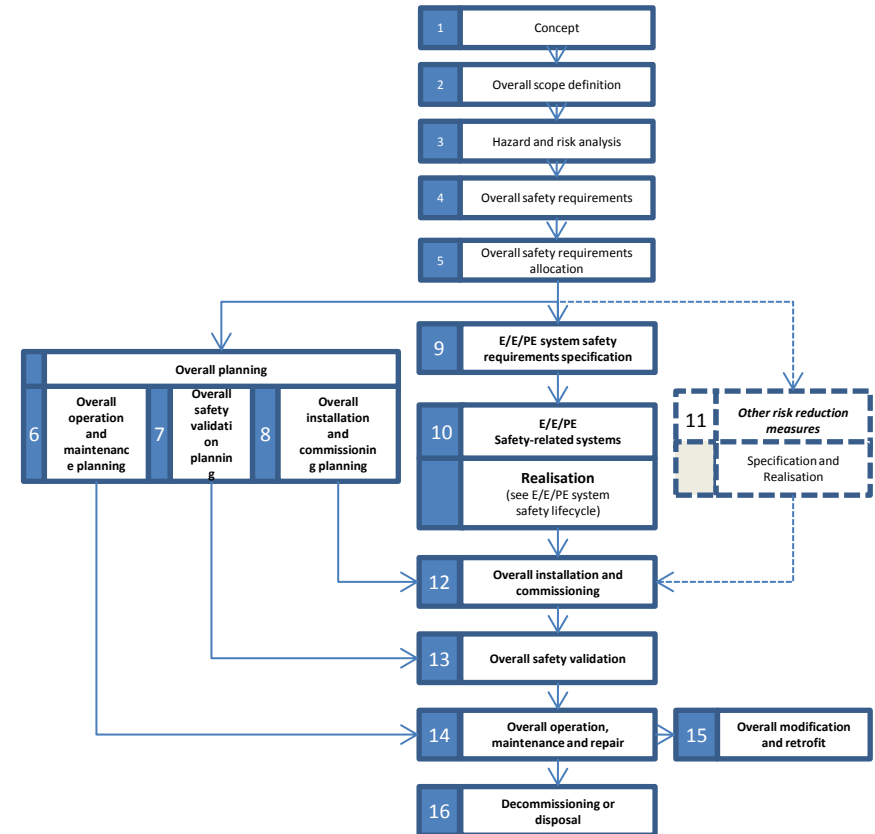
This guide sets out to explain where the details for different safety lifecycle activities can be found in the standards for the Machinery Sector:
IEC 62061 and ISO 13849.

The overall safety lifecycle model contained in IEC 61508 has been used as the reference point.

To navigate click on one of the buttons below and then click on an individual phase

Phases
1-5

Phases
6-16



Cross Reference Example

5	Overall safety requirements allocation		
Objectives	To allocate the safety functions, contained in the specification for the overall safety requirements (both the safety functions requirements and the safety integrity requirements), to the designated E/E/PE safety related systems and other risk reduction measures; To allocate a safety integrity level to each safety function to be carried out by an E/E/PE safety-related system.		
IEC 61508		IEC 62061	ISO 13849
Part 1 Clauses 7.6.1 7.6.2		Clause 5 5.2.1.3 – Specifications for each SRCF shall comprise the functional requirement (5.2.3) and the safety integrity requirement (5.2.4)	Clause 4 4.2.2 – For each safety function the characteristics and the required performance level shall be specified

Questions?



IEC 62061 and ISO 13849 A cross reference guide



Product Service

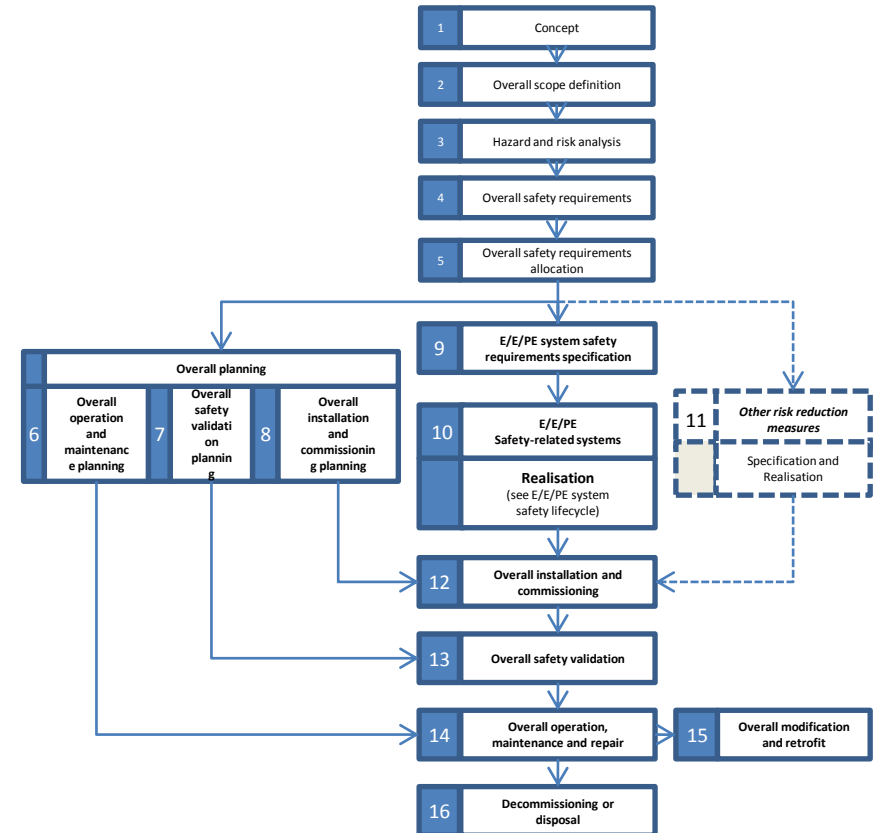
This guide sets out to explain where the details for different safety lifecycle activities can be found in the standards for the Machinery Sector:
IEC 62061 and ISO 13849.

The overall safety lifecycle model contained in IEC 61508 has been used as the reference point.

To navigate click on one of the buttons below and then click on an individual phase

Phases
1-5

Phases
6-16





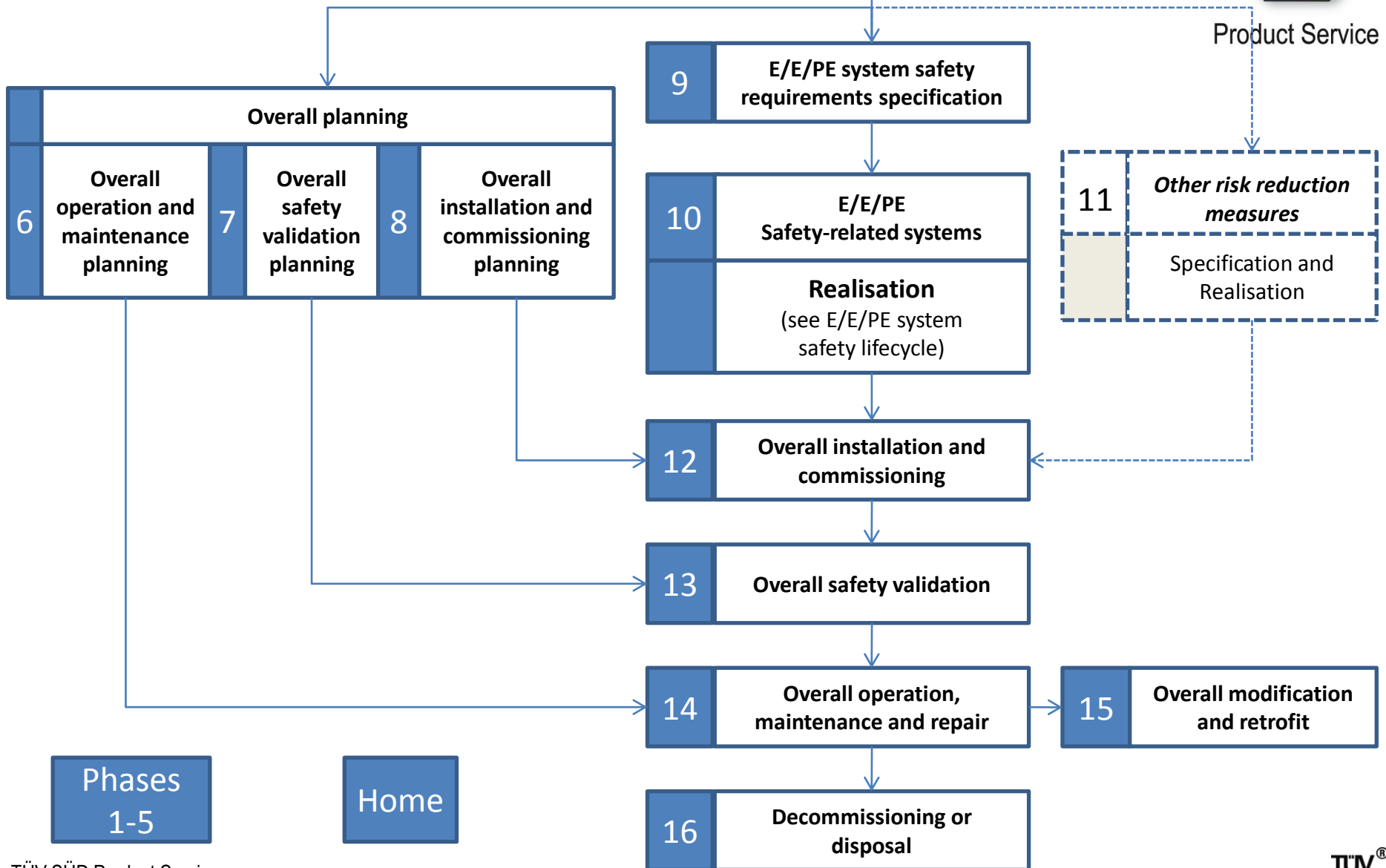
Home

Phases
6-16

Realisation Etc.



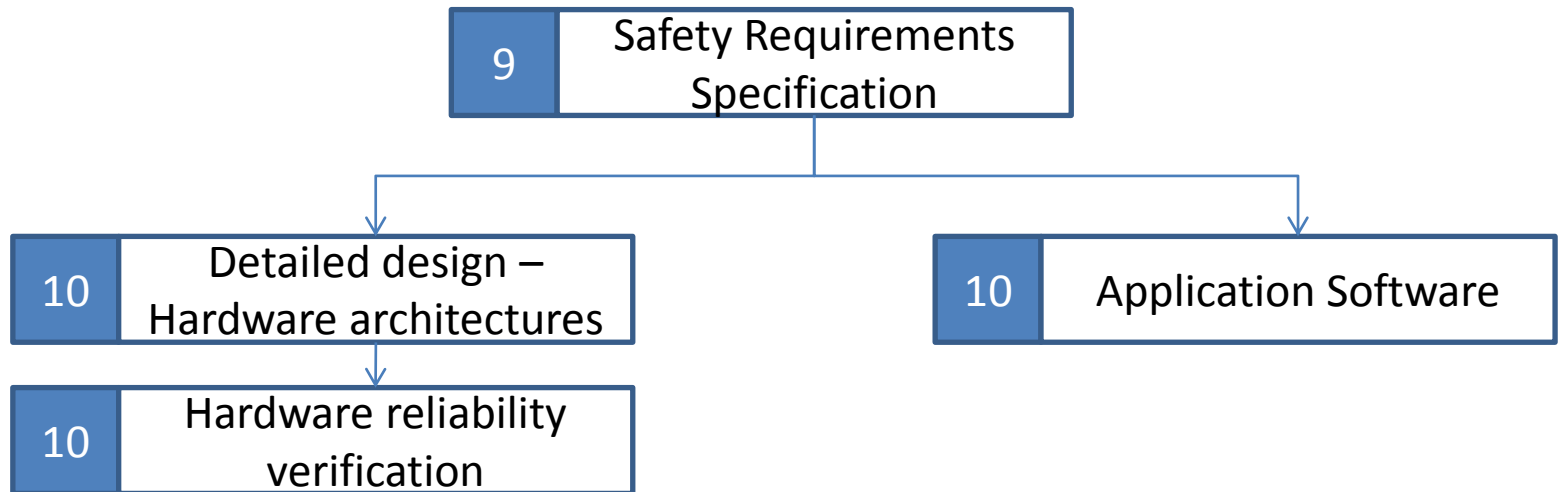
Phase 5



Detailed Realisation Phases



Product Service



Home

Phases
1-5

Phases
6-16



Product Service

1

Concept

Objectives

To develop a level of understanding of the EUC and its environment (physical, legislative etc.) sufficient to enable the other safety lifecycle activities to be satisfactorily carried out.

IEC 61508

Part 1 Clauses
7.2.1
7.2.2

IEC 62061

Not Covered
The scope of 62061 is the “design, integration and validation” of SRECS.
Note: Clause 4
“Management of functional safety” specifies the management and technical activities that are required

ISO 13849

Not Covered
The scope of 13849-1 is the design and integration of SRP/CS



Phases
1-5

Home

Phases
6-16



Overall scope definition



Product Service

Objectives

To determine the boundary of the EUC and the EUC control system; To specify the scope of the hazard and risk analysis (for example process hazards, environmental hazards, etc.).

IEC 61508	IEC 62061	ISO 13849
Part 1 Clauses 7.3.1 7.3.2	Not covered In the introduction Figure 1 references ISO 12100 and 14121 for the design and risk assessment of the machine Note: 12100 and 14121 are now combined	Not covered Clause 4.1: The SRP/CS shall be designed and constructed so that the principles of ISO 12100 and ISO 14121 are fully taken into account



Phases
1-5

Home

Phases
6-16



Hazard and risk analysis



Product Service

Objectives

To determine the hazards, hazardous events and hazardous situations relating to the EUC and the EUC control system (in all modes of operation), for all reasonably foreseeable circumstances, including fault conditions and reasonably foreseeable misuse (see 3.1.14 of IEC 61508-4);
 To determine the event sequences leading to the hazardous events; The scope will be dependent upon the phase reached in the overall, E/E/PE system and software safety lifecycles (since it may be necessary for more than one hazard and risk analysis to be carried out). For the preliminary hazard and risk analysis, the scope will be as defined by the output of the overall scope definition.

IEC 61508	IEC 62061	ISO 13849
Part 1 Clauses 7.4.1 7.4.2	Not covered In the introduction Figure 1 references ISO 12100 and 14121 for the design and risk assessment of the machine Note: 12100 and 14121 are now combined	Not covered Clause 4.1: The SRP/CS shall be designed and constructed so that the principles of ISO 12100 and ISO 14121 are fully taken into account



Phases
1-5

Home

Phases
6-16



Overall safety requirements



Product Service

Objectives

To develop the specification for the overall safety requirements, in terms of the safety functions requirements and safety integrity requirements, for the E/E/PE safety-related systems and other risk reduction measures, in order to achieve the required functional safety.

IEC 61508	IEC 62061	ISO 13849
Part 1 Clauses 7.5.1 7.5.2	Not covered In the introduction Figure 1 references ISO 12100 and 14121 for the design and risk assessment of the machine Note: 12100 and 14121 are now combined	Not covered Clause 4.1: The SRP/CS shall be designed and constructed so that the principles of ISO 12100 and ISO 14121 are fully taken into account



Phases
1-5

Home

Phases
6-16



Overall safety requirements allocation



Product Service

Objectives

To allocate the safety functions, contained in the specification for the overall safety requirements (both the safety functions requirements and the safety integrity requirements), to the designated E/E/PE safety related systems and other risk reduction measures; To allocate a safety integrity level to each safety function to be carried out by an E/E/PE safety-related system.

IEC 61508	IEC 62061	ISO 13849
Part 1 Clauses 7.6.1 7.6.2	Clause 5 5.2.1.3 – Specifications for each SRCF shall comprise the functional requirement (5.2.3) and the safety integrity requirement (5.2.4)	Clause 4 4.2.2 – For each safety function the characteristics and the required performance level shall be specified



Phases
1-5

Home

Phases
6-16



Overall operation and maintenance planning



Product Service

Objectives

To develop a plan for operating and maintaining the E/E/PE safety-related systems, to ensure that the required functional safety is maintained during operation and maintenance

IEC 61508

Part 1 Clauses
7.7.1
7.7.2

IEC 62061

“Planning” is not covered separately.

ISO 13849

Not covered
Note: ISO 12100 is referenced in clause 9 (Maintenance)



Phases
1-5

Home

Phases
6-16



Overall safety validation planning



Product Service

Objectives

To develop a plan for the overall safety validation of the E/E/PE safety-related systems.

IEC 61508

Part 1 Clauses
7.8.1
7.8.2

IEC 62061

Clause 4.2.1 (h)
Sets out the
requirements of as
validation plan

ISO 13849

13849-2 – Validation
Clause 3.4 sets out the
requirements for a
validation plan



Phases
1-5

Home

Phases
6-16





Objectives

To develop a plan for the installation of the E/E/PE safety-related systems in a controlled manner, to ensure that the required functional safety is achieved; To develop a plan for the commissioning of the E/E/PE safety-related systems in a controlled manner, to ensure that the required functional safety is achieved.

IEC 61508

Part 1 Clauses
7.9.1
7.9.2

IEC 62061

Clause 6.13.2.1 – A
SRECS shall be installed
in accordance with the
functional safety plan for
the final system
validation (clause 4.2.1
item (h))

ISO 13849

Not covered



Phases
1-5

Home

Phases
6-16





Objectives

To define the E/E/PE system safety requirements, in terms of the E/E/PE system safety function requirements and the E/E/PE system safety integrity requirements, in order to achieve the required functional safety

IEC 61508

Part 1 Clauses
7.10.1
7.10.2

IEC 62061

Clause 5
5.2.1.3 – Specifications
for each SRCF shall
comprise the functional
requirement (5.2.3) and
the safety integrity
requirement (5.2.4)

ISO 13849

Clause 4
4.2.2 – For each safety
function the
characteristics and the
required performance
level shall be specified



Phases
1-5

Home

Phases
6-16





Objectives

To create E/E/PE safety related systems conforming to the specification for the E/E/PE system safety requirements (comprising the specification for the E/E/PE system safety functions requirements and the specification for the E/E/PE system safety integrity requirements).

IEC 61508

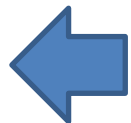
Part 1 Clauses
7.11.1; 7.11.2
Part 2 for Hardware
Part 3 for Software

IEC 62061

Included in Clause 6.
Control of systematic
faults is part of this
clause.
SRECS architecture is
described by subsystems
detailing Hardware Fault
Tolerance and Diagnostic
Coverage

ISO 13849

Clause 4.4 gives the
overall requirements.
Clause 6 describes
designated architectures
as categories (B, 1 – 4).
Categories state the
required behaviour of a
SRP/CS in respect of it's
resistance to faults etc.



Phases
1-5

Home

Phases
6-16





Objectives

To create E/E/PE safety related systems conforming to the specification for the E/E/PE system safety requirements (comprising the specification for the E/E/PE system safety functions requirements and the specification for the E/E/PE system safety integrity requirements).

IEC 61508

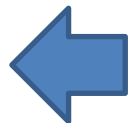
Part 1 Clauses
7.11.1; 7.11.2
Part 2 for Hardware
Part 3 for Software

IEC 62061

Subsystems can be
evaluated for random
hardware failures
according to formulae
given in clause 6.7.8.2
Verification is primarily
achieved by testing –
Clause 6.12

ISO 13849

Clause 4.7
The PL achieved by each
safety function shall
match the required PL
(PLr). Figure 5 describes
the relationship
between Category,
 $MTTF_d$ and DC_{avg}



Phases
1-5

Home

Phases
6-16





Objectives

To create E/E/PE safety related systems conforming to the specification for the E/E/PE system safety requirements (comprising the specification for the E/E/PE system safety functions requirements and the specification for the E/E/PE system safety integrity requirements).

IEC 61508

Part 1 Clauses
7.11.1; 7.11.2
Part 2 for Hardware
Part 3 for Software

IEC 62061

Clause 6.10
Requirements for
software based
parameterization as well
as application software
using LVL. Modular
structured programs
with documentation that
can be verified by testing

ISO 13849

Clause 4.6
Allows for development of
embedded software to PLd and
application software for all PL's.
Uses a 'V' model to describe the
software safety lifecycle. Has
requirements for software
based parameterization.
Modular and structured
programs that can be verified
by testing



Phases
1-5

Home

Phases
6-16



Other risk reduction measures



Product Service

Objectives

To create other risk reduction measures to meet the safety functions requirements and safety integrity requirements specified for such systems (outside the scope of this standard).

IEC 61508

Part 1 Clauses
7.12.1
7.12.2

IEC 62061

Not covered

ISO 13849

Not covered



Phases
1-5

Home

Phases
6-16



Overall installation and commissioning



Product Service

Objectives

To install the E/E/PE safety-related systems; To commission the E/E/PE safety-related systems

IEC 61508	IEC 62061	ISO 13849
Part 1 Clauses 7.13.1 7.13.2	Clause 6.13 A SRECS shall be installed in accordance with the functional safety plan for the final system validation (Clause 4.2.1 item (h))	Not covered



Phases
1-5

Home

Phases
6-16



Overall safety validation



Product Service

Objectives

To validate that the E/E/PE safety-related systems meet the specification for the overall safety requirements in terms of the overall safety functions requirements and the overall safety integrity requirements, taking into account the safety requirements allocation for the E/E/PE safety-related systems developed according to 7.6.

IEC 61508	IEC 62061	ISO 13849
Part 1 Clauses 7.14.1 7.14.2	Clause 8 8.2.2 – Each SRCF specified in the SRECS requirements specification, and all the SRECS operation and maintenance procedures shall be validated by test and/or analysis	ISO 13849-2 Safety of machinery – Safety-related parts of control systems – Part 2: Validation This standard has detailed requirements for validation



Phases
1-5

Home

Phases
6-16



Overall operation, maintenance and repair



Product Service

Objectives

To ensure the functional safety of the E/E/PE safety related systems is maintained to the specified level; To ensure that the technical requirements, necessary for the overall operation, maintenance and repair of the E/E/PE safety-related systems, are specified and provided to those responsible for the future operation and maintenance of the E/E/PE safety-related systems

IEC 61508	IEC 62061	ISO 13849
Part 1 Clauses 7.15.1 7.15.2	Clause 7 - Information for use of the SRECS shall be provided to enable the user to develop procedures to ensure that the required functional safety is maintained during use and maintenance of the machine	Clause 9 – Maintenance Simply states that the information for use of the SRP/CS shall include instructions for the maintenance (including periodic inspections) of the SRP/CS. Note: ISO 12100 is referenced



Phases
1-5

Home

Phases
6-16



Overall modification and retrofit



Product Service

Objectives

To define the procedures that are necessary to ensure that the functional safety for the E/E/PE safety-related systems is appropriate, both during and after the modification and retrofit phase has taken place

IEC 61508

Part 1 Clauses
7.16.1
7.16.2

IEC 62061

Clause 9 – Modification
This clause specifies the modification procedure(s) to be applied when modifying the SRECS during design, integration and validation (e.g. during SRECS installation and commissioning).
Modification after the SRECS has been put into operation and use is not considered by 62061

ISO 13849

Modifications during software development covered in clause 4.6 – Software safety requirements.
Modification after the machine has been put into use is only briefly mentioned in the documentation requirements of clause 11 – Information for use



Phases
1-5

Home

Phases
6-16



Decommissioning or disposal



Product Service

Objectives

To define the procedures that are necessary to ensure that the functional safety for the E/E/PE safety-related systems is appropriate in the circumstances during and after the activities of decommissioning or disposing of the EUC

IEC 61508

IEC 62061

ISO 13849

Part 1 Clauses
7.17.1
7.17.2

Not covered

Not covered



Phases
1-5

Home

Phases
6-16



RAILWAY FUNCTIONAL SAFETY STANDARDS

Roger Short

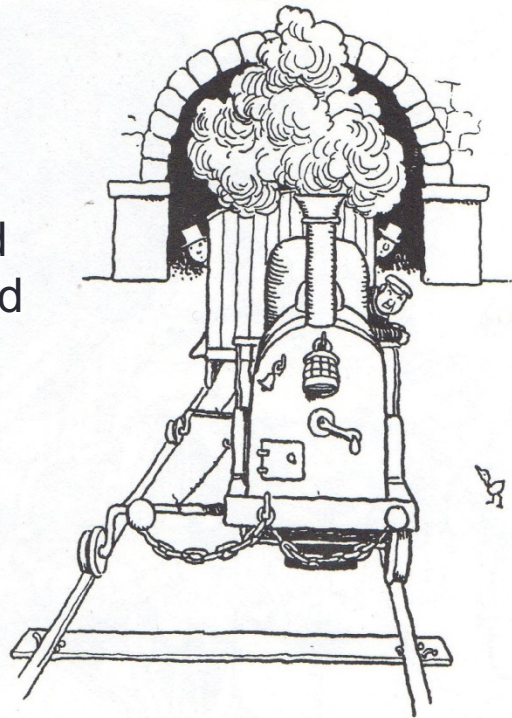


**Institute of
Measurement
and Control**

**FUNCTIONAL SAFETY
2014**

From the Early Days

It was soon realised that railways needed standards



The Standards Families

Railway Family



CENELEC
+ IEC Clones

EN 50126

EN 50128

EN 50129

E/E/PE Family



IEC

IEC 61508



EN 50126

Grew up in the
same town as
61508 part 1

Railway applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) -

- Came from a similar background to IEC 61508 part 1.
- Broadly comparable but more detailed, quasi-textbook in places.
- Applicable to all railway systems and technologies, not just E/E/PE.
- Not confined to safety aspects
- Covers **R**eliability, **A**vailability, **M**aintainability, **S**afety

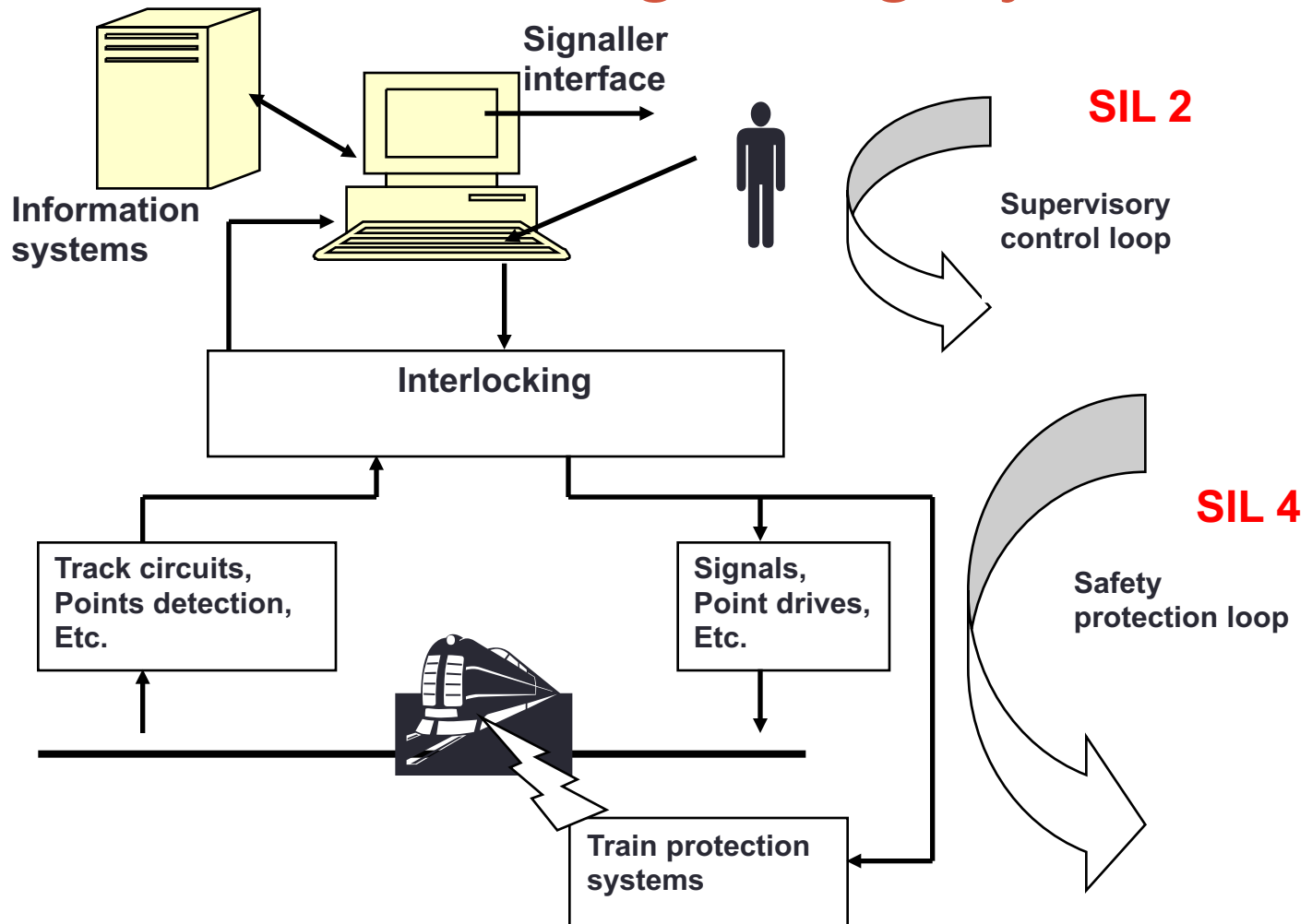
EN 50128

**Railway applications —
Communication, signalling
and processing systems —
Software for railway control
and protection systems**

Younger half-sister
of 61508 part 3.
Distinct family likeness

- Grew up alongside IEC 61508 part 3
- Notable differences:
 - Only 2 SILs (SIL4 \equiv SIL3, SIL2 \equiv SIL1)
 - Different recommendations for SIL techniques

2-SIL Architecture of Signalling Systems



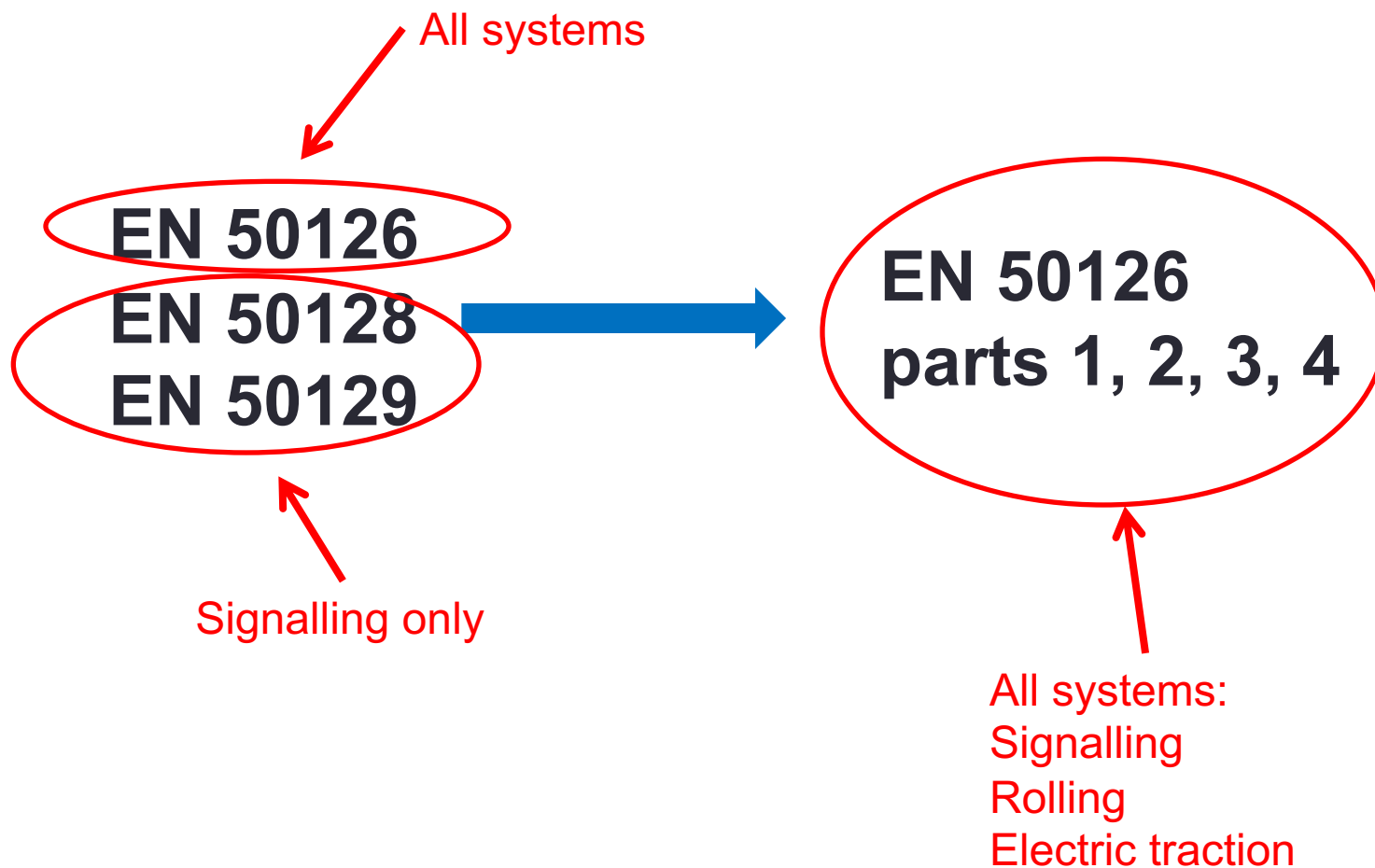
EN 50129

Distant cousin
of 61508 part 2

Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling

- Grew out of railway signalling R&D of the 1980s
- Central concepts
 - Safety Lifecycle
 - System architectures
 - SIL
- Structured around production of a safety case
- Includes catalogue of electronic component failure modes

Developments



You may also like

BRITISH STANDARD

BS EN
50159-1:2001

**Railway applications—
Communication,
signalling and
processing systems —**

Part 1: Safety-related communication
in closed transmission systems

BRITISH STANDARD

BS EN
50159-2:2001

**Railway applications—
Communication,
signalling and
processing systems —**

Part 2: Safety related communication in
open transmission systems

- EN 50159 deals with transmission of safety data and commands over general-purpose comms networks.
- Not railway specific
- Not technology specific

DEVELOPMENT AND FIELD RESULTS OF A SIL2, WIRELESS IR GAS DETECTOR

Knut Sandven, Håkon Sagberg, Britta Fismen, Jørgen Svare, Niels Aakvaag
GasSecure AS
Hoffsveien 70C
0377 Oslo
Norway

ABSTRACT

Infrared hydrocarbon gas detectors are essential for safety at oil and gas installations, but cables for power and communication complicate installation. A detector with a low-power optical design based on a Microelectromechanical system (MEMS) gives several years of reliable battery operation. This detector communicates wirelessly. The main challenges with safe wireless communication are to guarantee a short response time and to immediately detect loss of contact with detectors. This detector has proven to have reliable operation in various challenging environments. Test results from one year offshore operation in the North Sea are reported.

INTRODUCTION

Reliable and fast detection of hydrocarbon gas leaks is important for safety in the petroleum industry. Infrared absorption measurement is a widely used and approved method. Point detectors are installed at strategic locations and measure the gas concentration of the air flowing naturally into the detector's measurement volume. The measurement itself is not particularly challenging from a spectroscopist's point of view, since explosive mixtures of hydrocarbons in air typically absorbs more than 10% of the power in a wide spectral band using a pathlength of only 10cm. However, the real challenge lies in designing a reliable, practical, and not too expensive instrument also satisfying the following requirement: No recalibration shall be necessary during a lifetime of up to 20 years, in a wide operating temperature range and harsh environment (1).

There are also strict requirements on the probabilities for false negatives (non-detection) and false positives (false alarms). A few commercially available gas detectors have demonstrated, they satisfy the requirements above. However, the energy consumption is on the order of 3W to 5W, and as much as 80% of the detection system cost may come from installing cables for power supply and communication. Therefore, there is a demand for battery operated, wireless detectors.

GasSecure of Norway has developed a wireless, infrared based gas detector satisfying the above requirements of high reliability with fast response time and no recalibration. The detector has proven performance in challenging climates from arctic to tropical. Typical battery lifetime is two years with continuous monitoring.



FIGURE 1. THE MEMS-BASED INFRARED GAS DETECTOR GS01 WITH BATTERY COMPARTMENT TO THE RIGHT, WEATHER PROTECTION TO THE LEFT, ELECTRONICS AND SPECTROMETER IN THE STEEL HOUSING AND ANTENNA ON TOP.

ENERGY-EFFICIENT SENSOR SYSTEM

Several techniques are implemented for reducing energy consumption from watts to milliwatts, and three of the most important are:

1. The infrared sensor works in combination with an ultrasonic sensor allowing the more energy consuming infrared sensor to spend much of its time in a standby state.
2. The wake-up time of the infrared sensor is short, and a complete measurement takes only 0.5 second.
3. A compact and simple optical design makes efficient use of the light from a small source.

By default the infrared sensor will execute an optical measurement every third second providing reliable infrared gas concentration measurements. This main loop is represented as the solid line in FIGURE 2. In addition to the infrared sensor, an ultrasonic sensor is included to continuously measure the air composition by measuring the speed of sound by ultrasonic pulses.

The speed of sound in a gas mixture depends on the average molecular weight and the temperature. Two piezo-electric ultrasonic transducers are used to send a pulse through the measuring volume (inside weather protection) and receive the reflected pulse about 0.4 milliseconds later. The actual time delay is measured with accuracy better than 100ns. A small, fast, and accurate temperature sensor (NTC) resides in the same volume. When temperature is corrected for, any significant remaining change in time-of-flight is assumed to

be due to an increased concentration of hydrocarbons in air, unless proven otherwise by the optical sensor.

The dashed lines in FIGURE 2 represent an option to skip the optical measurement and use the previous measurement value, provided that the ultrasonic measurements prove there is no significant change in the air composition (2). Every fifth minute the optical measurement will execute, to perform diagnostics on the optical sensor, regardless of the ultrasonic measurement.

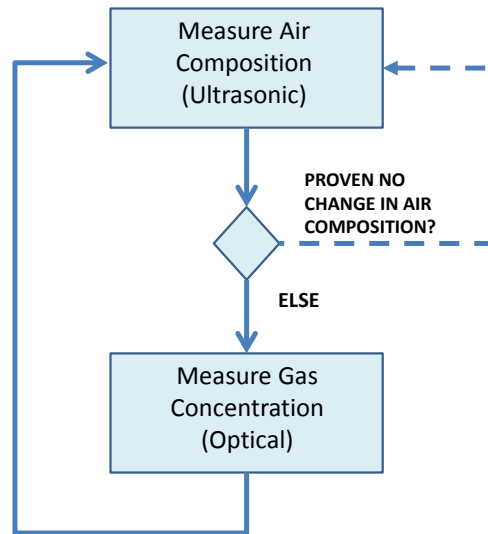


FIGURE 2. FLOWCHART SHOWING THE OPERATIONAL PRINCIPLE OF THE TWO SENSORS IN THE GAS DETECTOR.

INFRARED SENSOR DESIGN

For the two-sensor combination to work, the infrared sensor must be able to shift from standby mode to active mode in milliseconds and produce reliable output within one second, before it goes back to standby. It must also be energy-efficient. It is found that such an infrared sensor could be made based on a voltage-controlled holographic MEMS chip (3, 4) that can switch between measurement and reference wavelength bands. A complete measurement takes 0.5s, and is completely self-contained, with no additional filtering. Each measurement represents the actual gas concentration in the cell. FIGURE 3(a) shows a drawing of the infrared sensor. The core of the spectrometer system is a micro-electromechanical system (MEMS) that disperses, focuses, and modulates the incident light. By applying a control voltage to the MEMS chip, the filter switches between the measurement state (central absorption band) and the reference state (double sideband), shown in FIGURE 3(b), at a frequency of 1kHz. The filter shapes are designed to give approximately equal power in the two states when there is no gas present, and the difference signal can be measured with greater accuracy than the signal levels corresponding to each filter state separately. The same light source and detector are used for the gas and reference measurements.

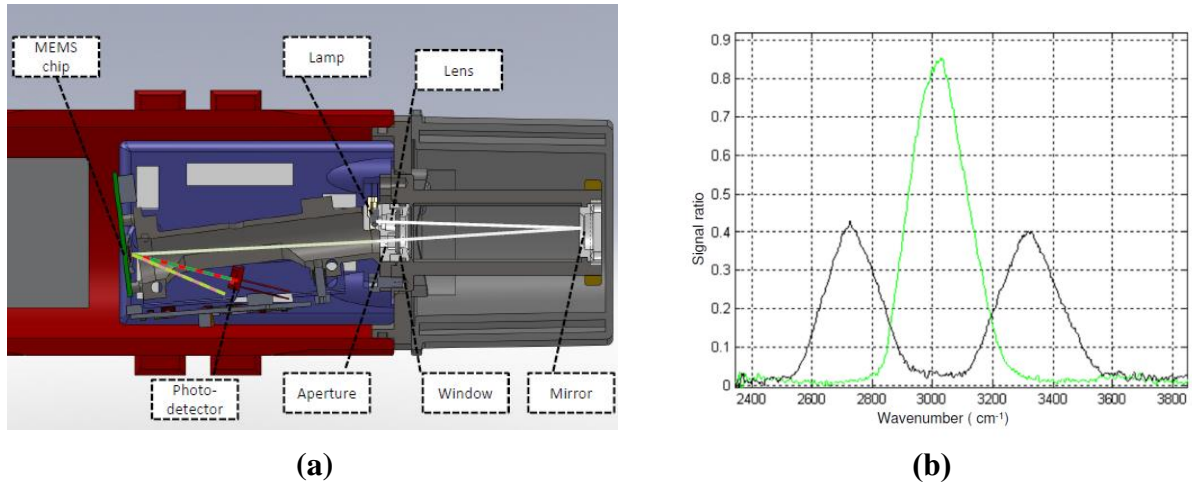


FIGURE 3. THE MEMS-BASED INFRARED GAS SENSOR.

(a) OPTOMECHANICAL DESIGN SHOWING THE MAIN OPTICAL COMPONENTS, THE BEAM OF BROAD BAND LIGHT (WHITE LINE), AND THE FILTERED AND MODULATED BEAM (RED AND GREEN DASHED LINE).

(b) THE FILTER FUNCTIONS USED FOR METHANE DETECTION, CORRESPONDING TO THE TWO STATES OF THE MEMS (GREEN AND BLACK), MEASURED USING AN EXTERNAL INTERFEROMETER.

The energy consumed during a single gas concentration measurement has been measured to 140mJ. Approximately two thirds is required by the light source, and one third by the microcontroller and electronic circuitry. If triggered every minute, the average power becomes 2.33mW. This allows several years of operation on a lithium-thionyl chloride battery pack with a volume less than 250cm³. Because a complete measurement takes less than half a second, the response time is dominated by the measuring frequency and the diffusion of gas into the measuring volume through the weather protection. The weather protection is designed to protect against the environment but will allow gas to freely flow through, there are no filters or humidity absorbers.

COMPARISON WITH NON-DISPERSIVE INFRARED GAS DETECTORS

Unlike a laboratory spectrophotometer that can be manually recalibrated as a part of the measurement procedure by subtracting the dark signal and normalizing the response of the photo-detector(s), an infrared gas sensor must rely on built-in mechanisms to compensate for drifting source intensities, detector response, and various other error sources. The simplest non-dispersive infrared (NDIR) gas sensors have only one wavelength channel and are considered unreliable for safety applications. More advanced detectors use a combination of reference wavelengths and/or reference light paths to achieve self-calibration. A typical configuration of a double-compensated detector uses four measurements to calculate gas concentration (two wavelengths combined with two detectors measuring internal and external light paths). Ideally this method eliminates error sources such as drifting source intensities or dirty optical windows. When concerned about energy consumption, there are some

disadvantages with the double-compensated system as described: Rapid infrared source modulation is required, and energy is lost in the heating and cooling cycle. There is also an arrangement of beam splitters that result in lost light. In order to achieve stable measurements there must be a certain degree of thermal equilibrium in the system. This often requires start-up times from tens of seconds up to several minutes, and excludes intermittent operation with short duty cycles.

SAFE WIRELESS COMMUNICATION

Energy constraints for battery powered instruments limits, the rate at which the instruments can report process values. For most process monitoring applications, this is not a major obstacle as the process values in question tend to change relatively slowly. For safety applications, the picture is somewhat different. For most safety applications continuous monitoring is necessary and a short latency (response time) needs to be guaranteed if a safety critical situation arises. However, the average bandwidth requirement is modest. Thus the primary difficulty in designing a wireless safety system is having a guaranteed short latency while not depleting the batteries. In addition, full control of all network message traffic is required, and loss of contact with a device must be identified immediately.

The wireless gas detector is intended for monitoring applications as well as for safety applications. For safety applications, the communication with the controller needs to meet reliability requirements according to Safety Integrity Level 2 (SIL 2) guidelines as described in IEC 61508 Ed.2.0 (5).

NETWORK TOPOLOGY

Wireless communication from the gas detectors is based on the standard protocol ISA100.11a (6). The gas detectors may be installed in full mesh topology, star topology or in a combination of the two topologies. It is possible to provide redundant paths between the controller and wireless gas detectors via redundant field access points, and to provide multiple communication paths from the wireless gas detectors to multiple redundant field access points. The ISA100.11a standard defines the many basic functions which improve data transfer reliability in communication. If the normal path used by a gas detector is obstructed or becomes unavailable, the gas detector will transmit its data along a redundant path. This leads to immensely stable and predictable networks.

The deployment of a wireless gas detector network is simple. The gas detectors are placed in their desired locations and powered on. Subsequently, each gas detector will spend some initial time conferring with its neighbors, obtaining an image of the network and the available paths to the network access point. The network information will include not only what neighbors are available for communication, but also the associated quality of each individual link. The aggregated information is stored in the network manager, which is responsible for scheduling communication opportunities.

Once the network has stabilized, the traffic intensity drops. However, the gas detectors will continue to update their neighbor link information, including the possible removal or addition

of gas detectors. In this way the network becomes adaptable to changes in the topology or of the environment.

Access points can be field connected with standard Ethernet, Fiber, Wireless or even existing 1.5mm² three wire field cabling. This makes deployment strategy very flexible and based upon what infrastructure is available today and what requested by the user.

SAFETY MECHANISMS IN WIRELESS NETWORKS

For safe communication satisfying IEC 61508 SIL 2 level, four error handling mechanisms must be supported:

- sequence numbering
- timeout in the absence of response
- device code name
- data consistency checking

The purpose of these mechanisms is to detect failures of the safety device in terms of packet loss, unacceptable network delay, bit errors, replay attacks, etc.

Several options exist for implementing the four required safety features. One approach is to base the product on a certified implementation of an open safety protocol. PROFIsafe over PROFINet (7) and ISA100.11a has been chosen due to the widespread use of the former in process control applications (8). PROFIsafe executes the task of safe communication between host and field device. It can target safety function up to SIL3. All the communication devices between the field device (gas detector) and the host (safety controller) are considered to be part of a black channel.

Upon a request packet from the safety controller, the gas detector needs to respond to that packet, containing the four above-mentioned mechanisms, within the process safety time. Process safety time is normally set to 60 seconds for gas detection systems. If the device does not respond before the safety time elapses, the device is marked as unavailable in the control system. It is fundamental to the operation of all safety systems that the exchange of safe packets is initiated by the controller and that there is a one-to-one correspondence between the packet sent and the packet received. Once the controller receives a response, a new request can be issued.

In order to fulfill the requirement of fast response time in a gas detection system, there needs to be opportunities to send uplink packets approximately once every two seconds. The gas detector will therefore, during setup, request that bandwidth is set aside for this uplink transmission rate. Normally responses are delayed on purpose to save battery, and the transmit opportunity is most often not used by the gas detector. However, the fact that bandwidth has been reserved ensures that the gas detector can respond immediately if a gas concentration is measured (9). Thus, most uplink packets will be safe responses, sent within the process safety time, only containing status information in the detector. It will serve primarily as an "alive" signal, indicating to the safety system that the detector is operating as it should and that the communication link is open. This sequence of packets is shown in FIGURE 4.

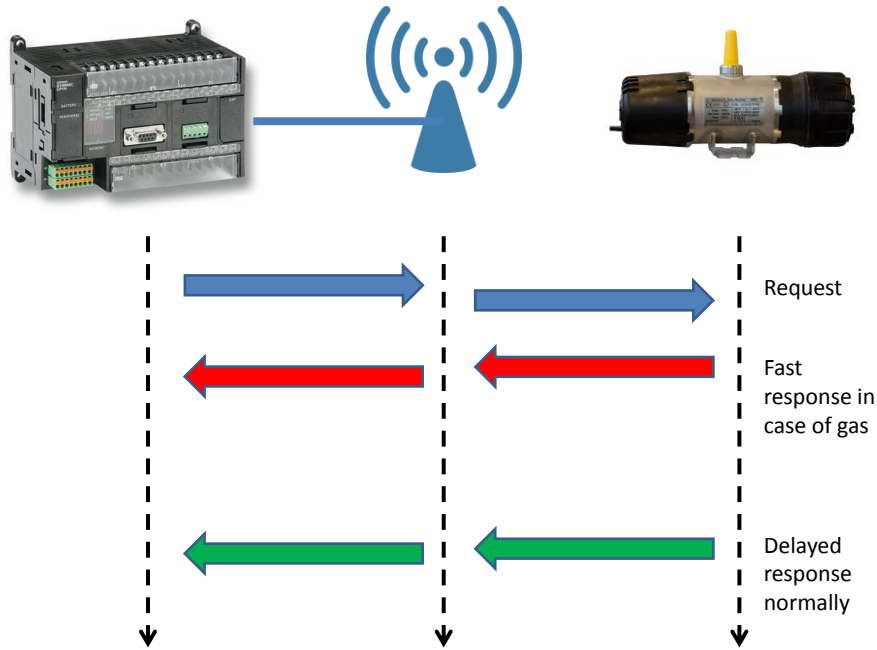


FIGURE 4. A SIMPLIFIED VIEW OF THE GAS DETECTOR COMMUNICATION WITH A SAFETY CONTROLLER THROUGH A GATEWAY ACCESS POINT.

RESULTS FROM FIELD INSTALLATION IN THE NORTH SEA

Three networks of in-total 20 gas detectors were installed at Gullfaks C in January 2013, see FIGURE 5. Gullfaks C is an oil and gas field in the North Sea operated by Statoil. The platform is an old installation having had several add-ons over its more than 25 year lifetime. It has many obstructions from heavy steel decks, structures and machinery that could put the detectors' communication system to the test.



FIGURE 5. STATOIL'S GULLFAKS C PLATFORM WITH INDICATION OF GAS DETECTOR PLACEMENTS.

DETECTOR LOCATIONS

Detector locations were partly chosen to challenge and test the gas detector in the most harsh conditions in the North Sea and partly to increase detection coverage at Gullfaks C in a module where only open path detectors were in use. Ten of the detectors at Gullfaks C have been installed shoulder-to-shoulder with Statoil's legacy wired gas detector to compare response times. Locations where there were problems with condensation and beam block on existing wired detectors were chosen. In addition, locations were chosen where strong and turbulent winds were expected, rapid temperature fluctuations and high humidity.

All three gateways communicate back to one fire and gas node executing the safety logic and displaying the result on an ABB safety system in the central control room. The wired side of the installation, from the gateway and beyond, uses PROFINet.

Main results from the now one year in operation include:

- Stable operation in North Sea environment with availability comparable to wired detectors.
- Actual small gas leakages detected at two instances and with faster response time than the legacy system.
- No drift and stable zero point, no calibration required.
- Response time equal to state-of-the art wired detectors.
- Typical battery lifetime of two years.

RESPONSE TIME

All gas detectors were tested with calibrated 50% LEL methane and flow rate 10l/min. On locations where the wireless gas detectors were installed next to wired detectors, the two detectors were exposed simultaneously through common test gas tubing. The response time from gas flow is open to display at the operator control panel in the central control room were measured, see TABLE I. The tests showed that the response time is essentially equal for both detectors; however the response of the wireless gas detector is quicker to show the correct level of gas. All readings of the wireless gas detector are stand-alone and no filtering is applied as is the case for other infrared detectors.

TABLE I. RESPONSE TIMES OF 10 WIRELESS GAS DETECTORS FROM EXPOSURE TO READING AT OPERATOR CONTROL PANEL.

Tag	Time [s]
DG-M24T-78	6.5
DG-M24T-76	5
DG-M24T-70	5
DG-M24T-72	4.5
DG-M24T-74	6.5
DG-M24T-71	3
DG-M24T-69	3
DG-M24T-73	5
DG-M24T-77	6
DG-M24T-75	7

BATTERY LIFETIME

The battery capacity depends on several factors, most importantly are operational temperature and current draw characteristics. There are two Lithium Thinoyl Chloride (10) battery cells included in the wireless gas detector battery pack. Based on the current draw characteristics, which will vary depending on environment and communication requirements, and taking a conservative approach, the expected battery capacity is 14mAh. Based on the wireless gas detector's measured current draw at Gullfaks C, a battery life of two years is expected, as can be seen from FIGURE 6. Remaining battery life is reported to the control system to allow for maintenance planning.

Three of the twenty gas detectors are placed on especially challenging locations to stress the optical sensor, i.e. with water running over the detector. Power consuming heaters on mirror and window are applied to remove condensation. These are not included in the statistics. On these most challenging locations, the battery lifetime is less than one year.

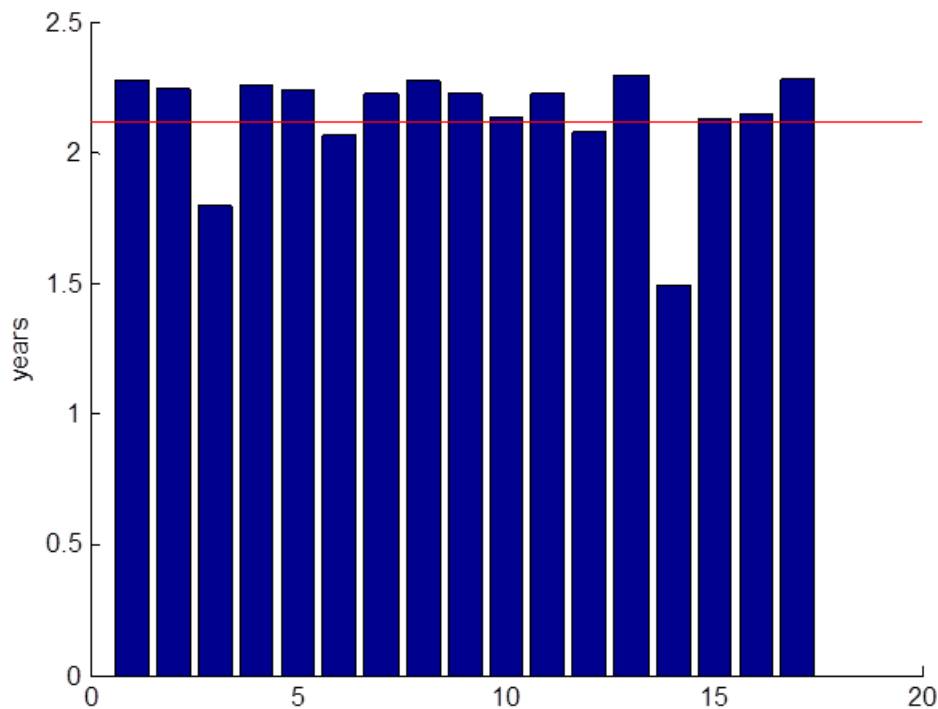


FIGURE 6. ESTIMATED BATTERY LIFE ON WIRELESS GAS DETECTORS INSTALLED AT GULLFAKS C FROM MEASURED ACTUAL CURRENT DRAW. RED LINE SHOWS AVERAGE CONSUMPTION AT 2.1 YEARS.

CONCLUSIONS

A new wireless, battery powered gas detector is demonstrated that is capable of providing reliable detection of hydrocarbon gases in harsh offshore environments, with fast response time and typical two years battery lifetime and no re-calibration.

REFERENCES

1. Sagberg H., Fismen B.G., Bakke K.A.H., Johansen I.-R., Tschudi J., “Gas sensors”, Patent application, WO2012GB53021, 05 December 2012.
2. Moe, S. T., Østbø N.P., Sandven K., Sagberg H., “Detector system and method to detect or determine a specific gas within a gas mixture”, Patent application, WO2009011593, 17 July 2007.
3. Sagberg H., Bakke T., Johansen I.-R., Lacolle M., Moe S. T., “Two-state Optical Filter Based on Micromechanical Diffractive Elements”, presented at the IEEE/LEOS International Conference on Optical MEMS and Nanophotonics, Hualien , Taiwan, August 2007.
4. Sagberg H., Lacolle M., Johansen I.-R., Løvhaugen O., Solgaard O., Sudbø A. S., “Micromechanical gratings for visible and near-infrared spectroscopy”, JSTQE 10, pp. 604–613, (2004).

5. IEC 61508 ed2.0 (2010-04), "Functional safety of electrical/electronic/programmable electronic safety-related systems"
6. "ISA-100 Wireless Compliance Institute", Web site, Retrieved March 13, 2014
7. PROFIsafe web portal, <http://www.profibus.com/technology/profisafe/>, Retrieved March 13, 2014
8. GasSecure, "Wireless communication in safety systems", available at: <http://www.gassecure.com/>, Retrieved January 24, 2014
9. Aakvaag N., Sandven K., "Wireless Sensor Networks", Patent application, WO2012GB51330, 13 June 2012.
10. Overview of Lithium Thionyl Chloride batteries from Tadiran, <http://www.tadiranbatteries.de/eng/products/lithium-thionyl-chloride-batteries/overview.asp>, Retrieved March 13, 2014

GAS

SECURE

GAS

SECURE

First wireless, infrared gas detector

Development and Field Results of a SIL2, Wireless IR Gas Detector

IMC Functional Safety 2014, 4th of November 2014

Jorgen Svare – jorgen.svare@gassecure.com

Business Development Director

The GS01 - The first wireless, infrared hydrocarbon gas detector

The GS01

Stainless steel body, intrinsic safe and in-field replaceable battery package



Features:

- Fast response (5 s)
- Two years battery life
- High reliability – SIL2, incl. communication
- No recalibration

The challenge: Reducing energy consumption

From 5 W to 5 mW energy consumption...

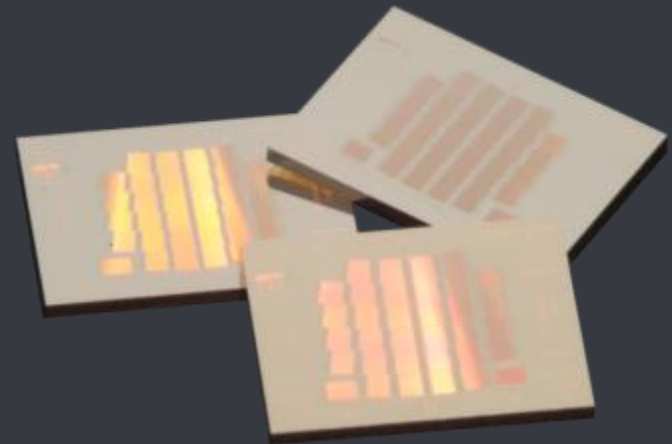
... using MEMS technology



Typical wired

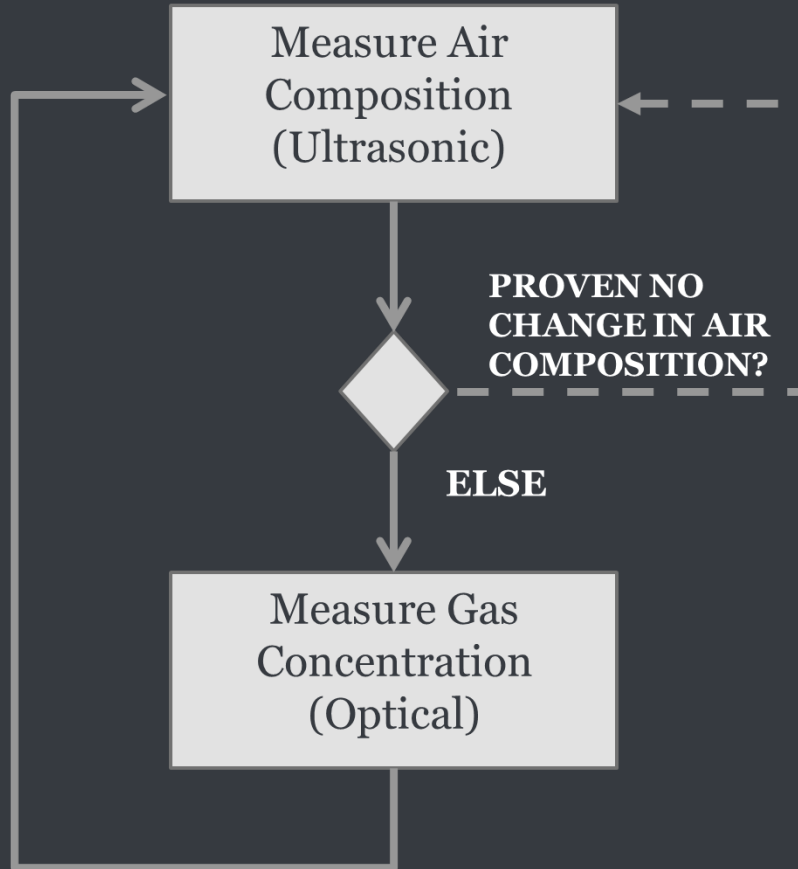


Battery operated
requirement

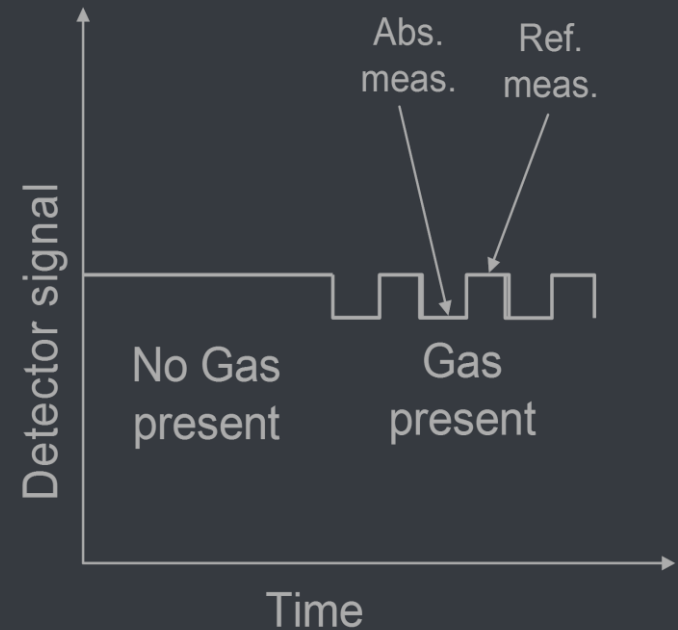
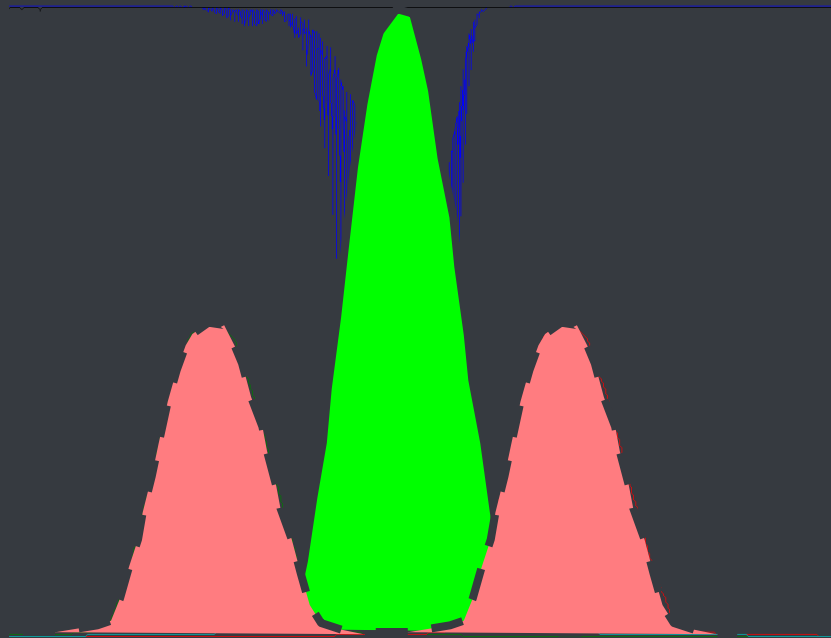


- High reliability
- Low power
- Fast response
- No recalibration

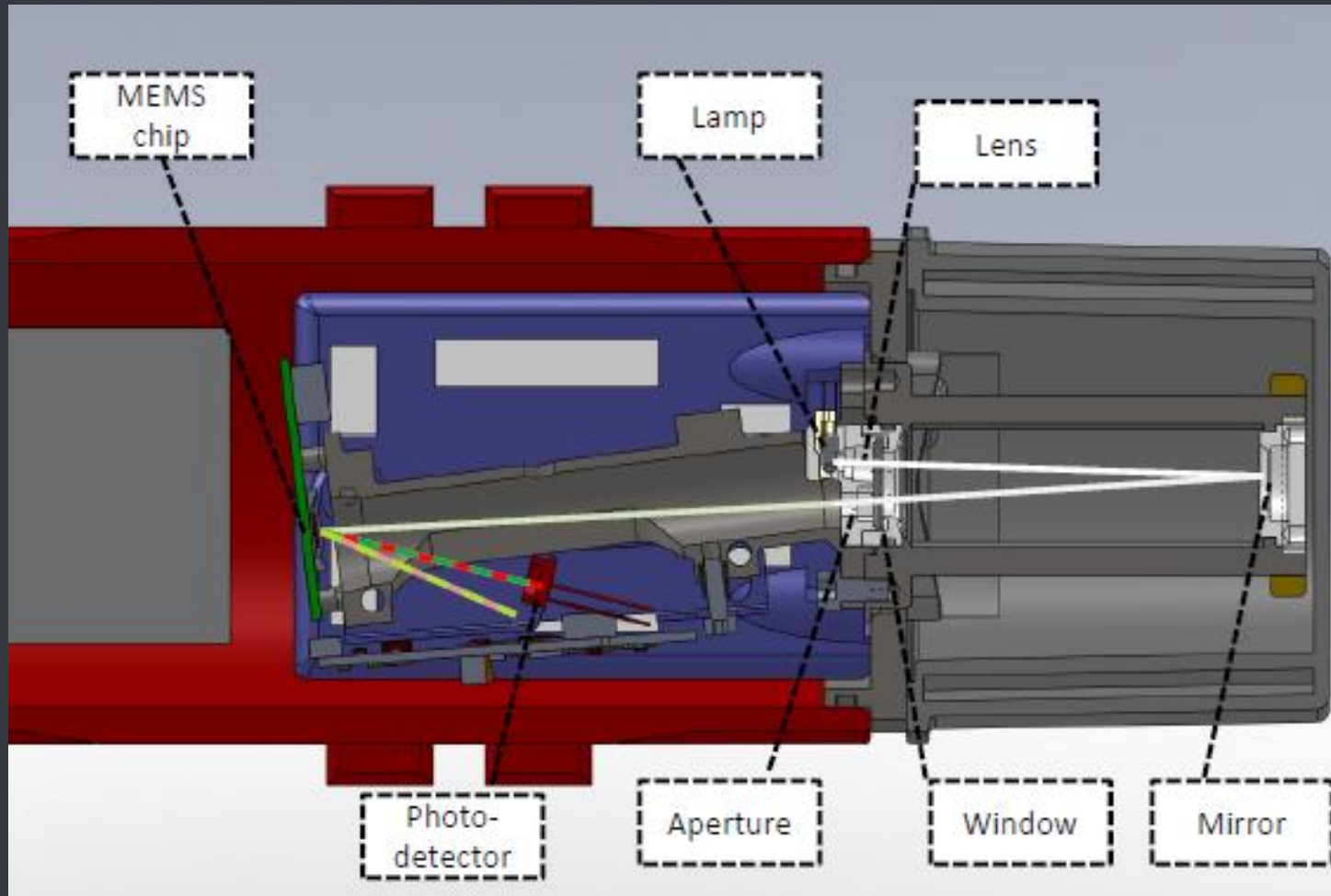
Two sensors are used in combination
in order to save energy

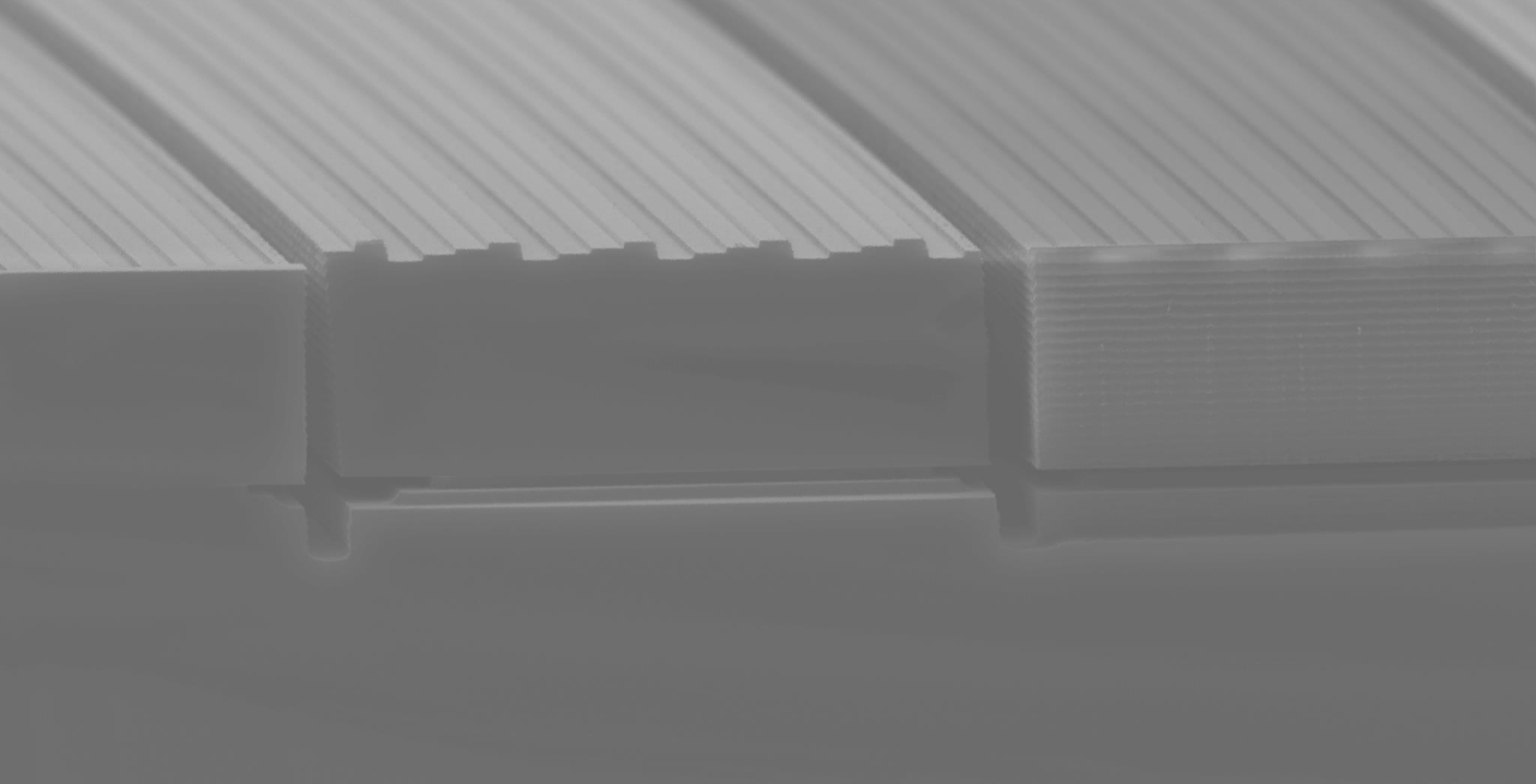


Two reference wavelengths ensure a reliable zero signal

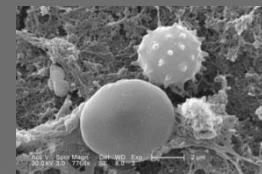


Optical sensor completely redesigned using MEMS technology





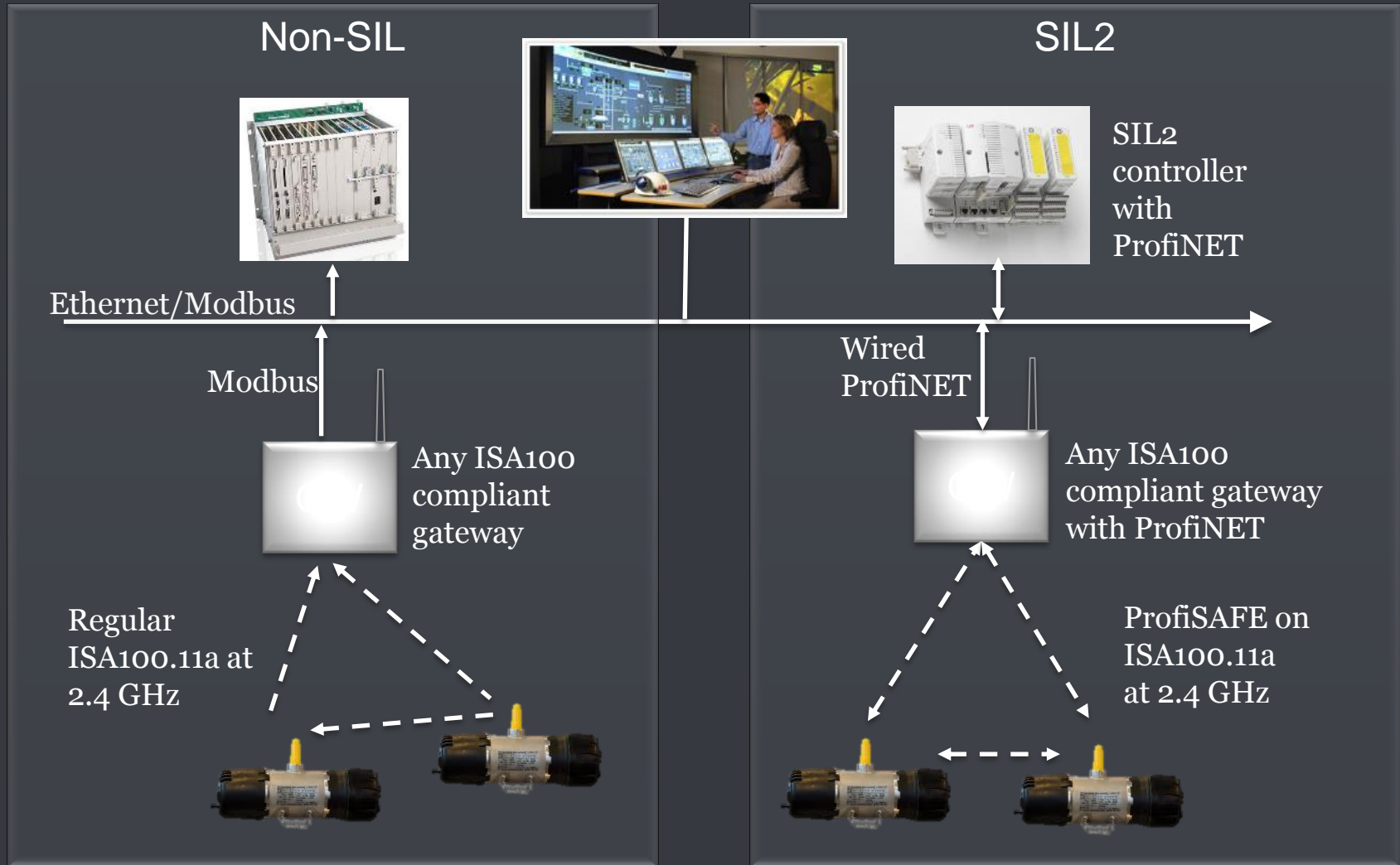
The smallest feature sizes are 1-3 μm
The four-level grating relief profile is
etched with an accuracy of about ± 20 nm



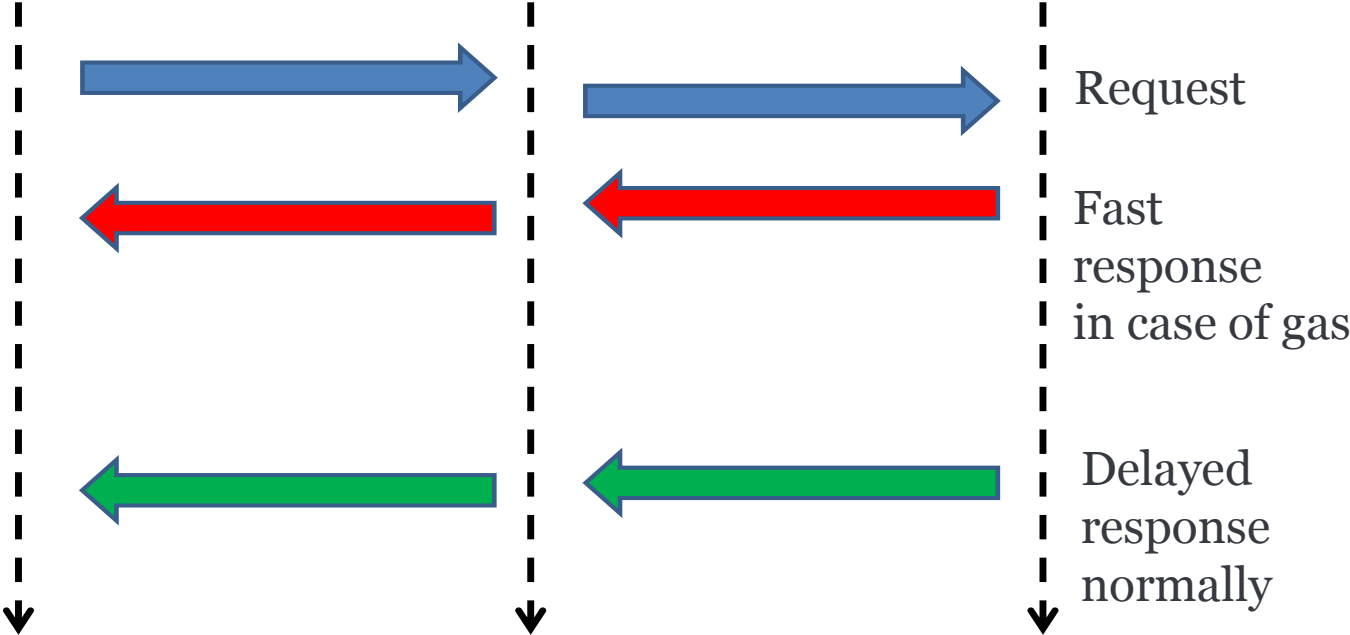
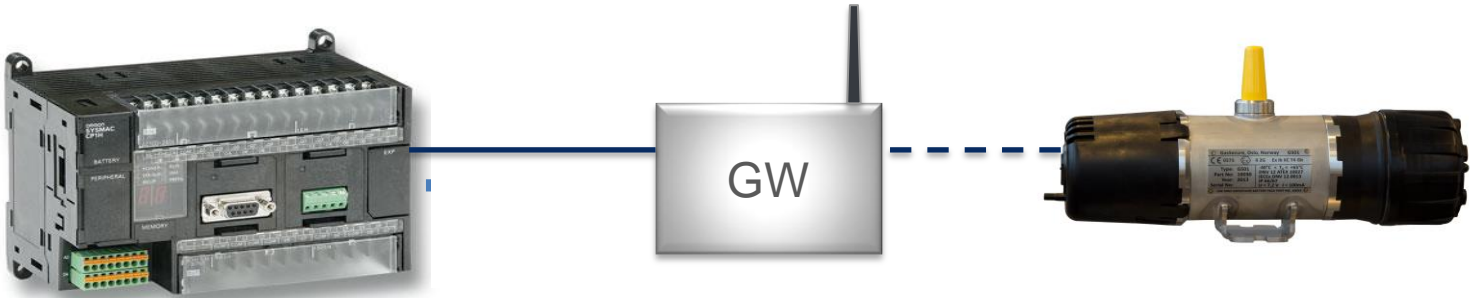
WD	HV	Spot	Tilt	Mag	Det	X: -7.30 mm
10.43 mm	20.0 kV	4.0	-4.5 °	2646x	Etd	Y: 13.76 mm

—20 μm —

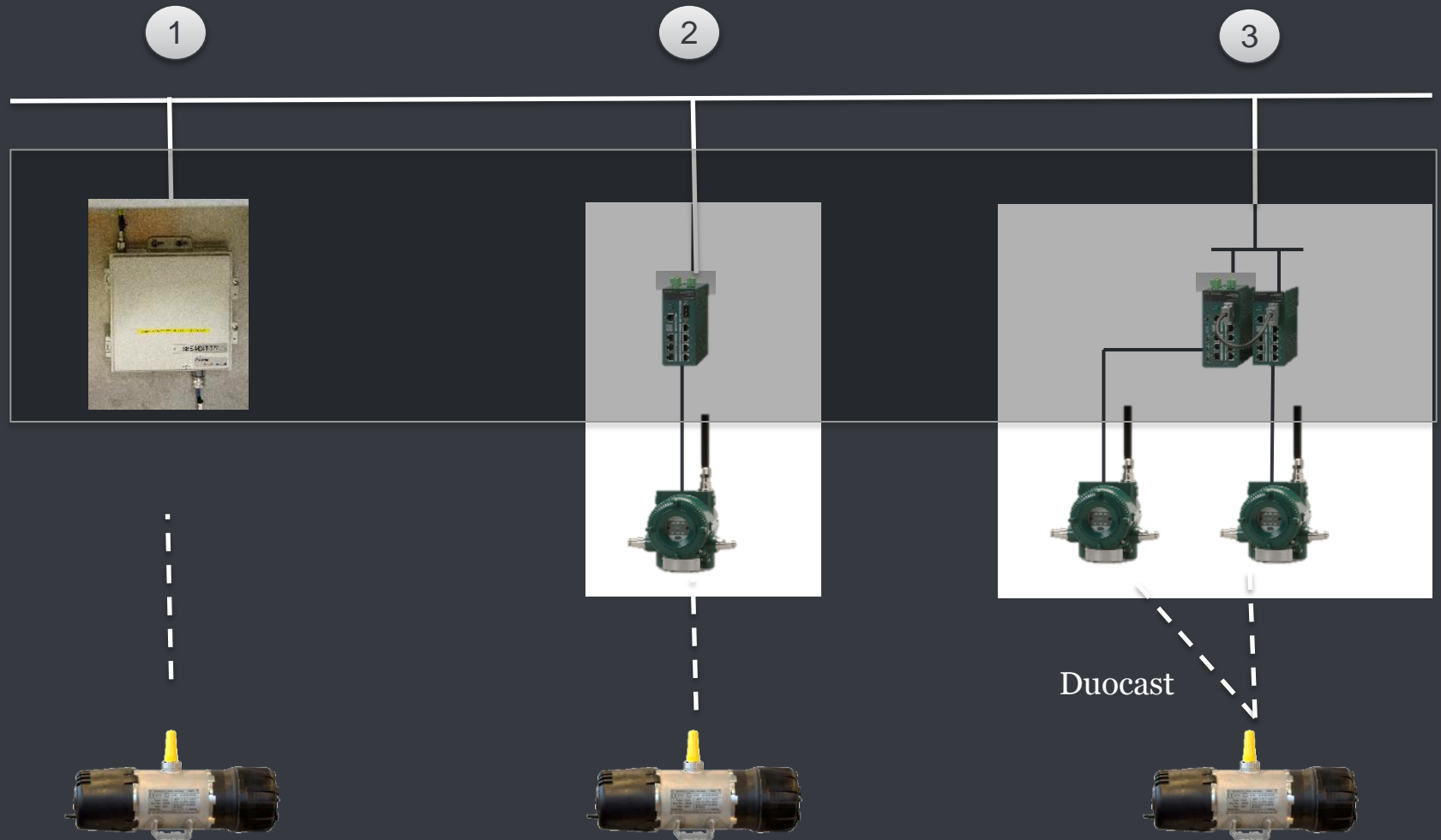
Communication is SIL2 suitable with a safety layer on top of standard wireless protocols



Bandwidth reserved for fast response



Gateway options



Certifications

Product:

- ATEX and IEC-Ex
- Performance IEC 60079-29-1
- Reliability IEC 61508 ed.2.0
- Various country specific radio certificates



Company:

- ISO 9001:2008
- Achilles JQS



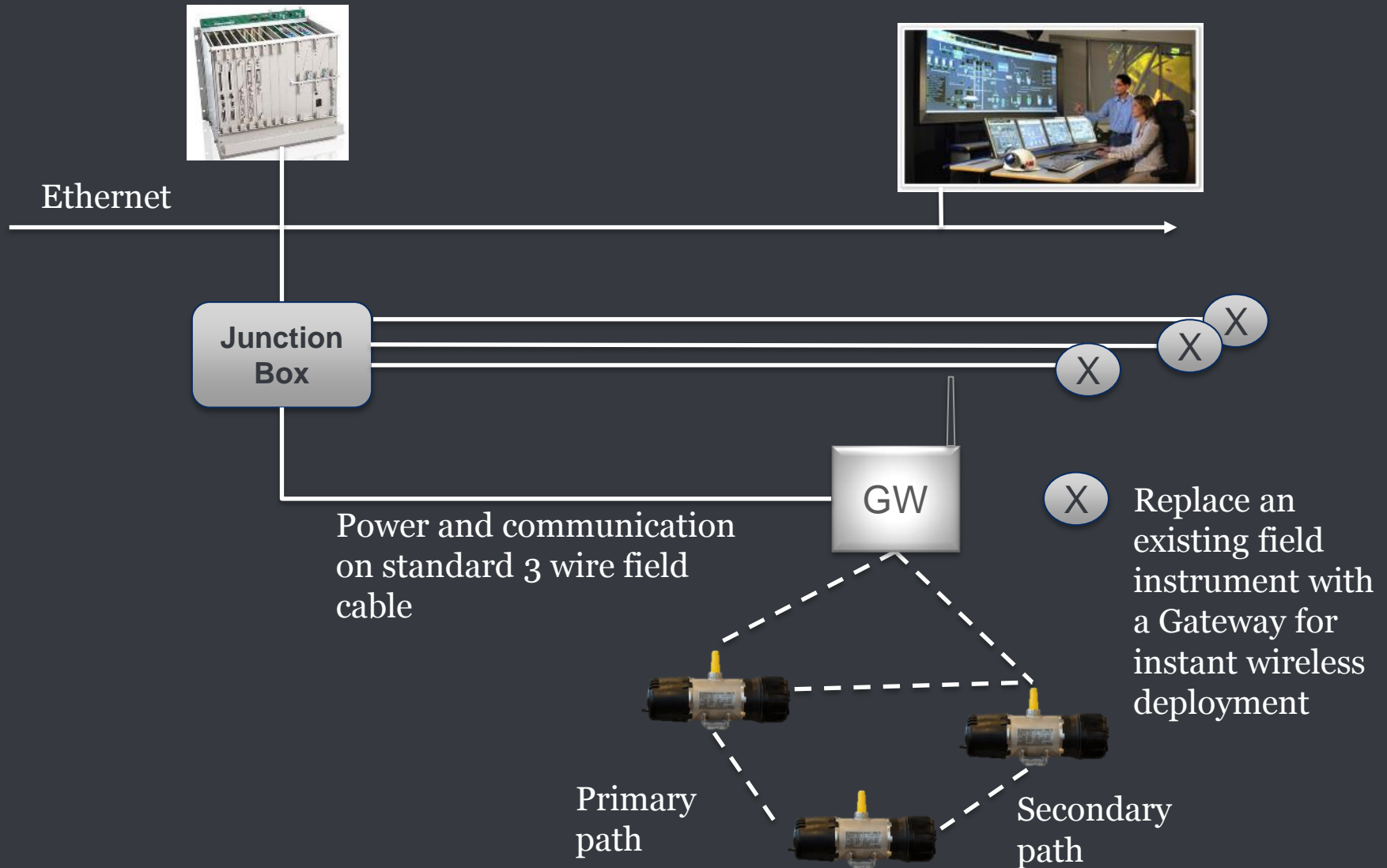
Offshore installation in the North Sea



10 detectors,
2 levels, one gateway

10 detectors, weather and
comparison tests

Reuse of field cabling



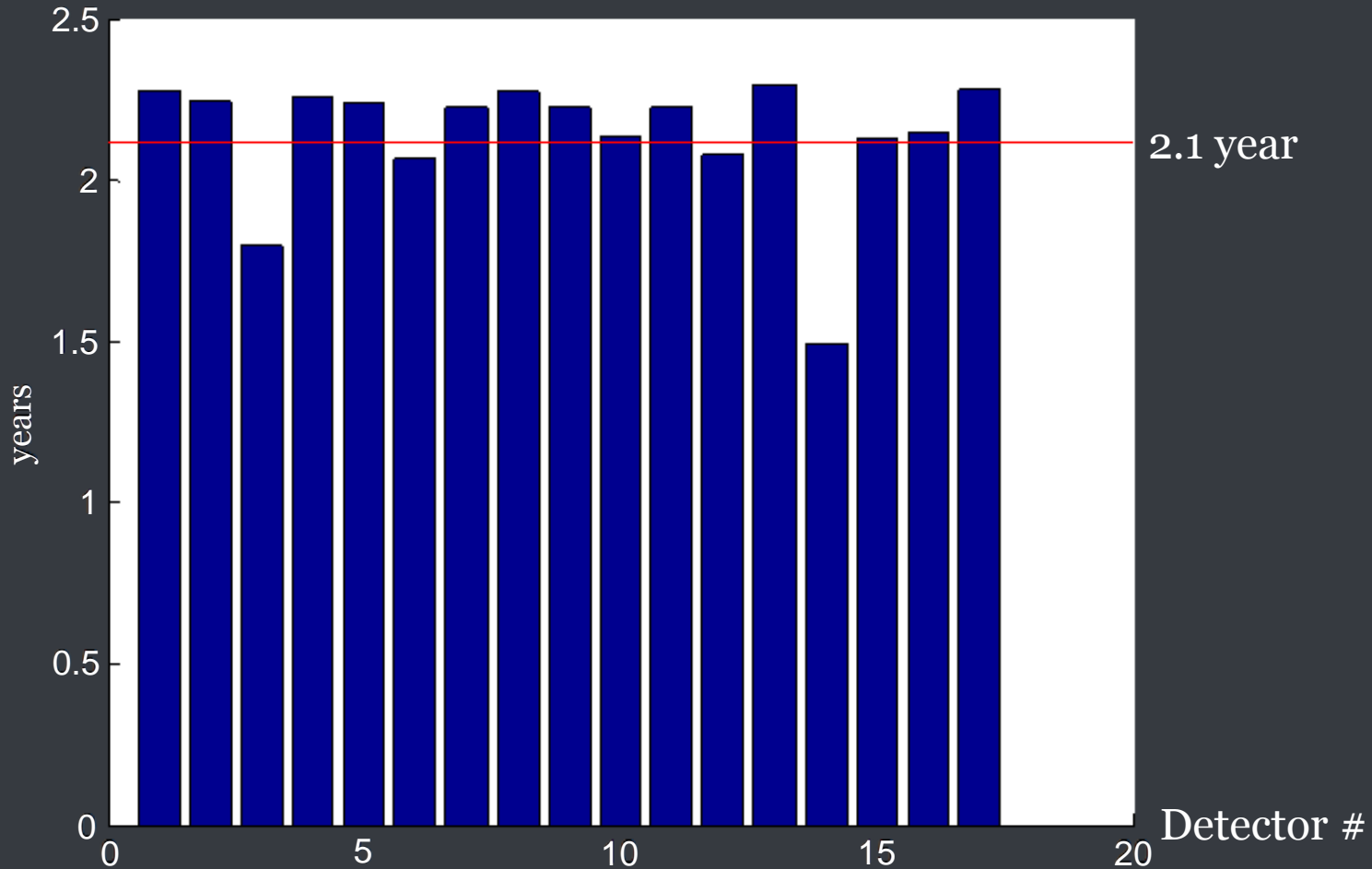
Response time measurements

- All measurements with methane test gas 50%LEL
- Flow rate 10L/min
- Weather cap volume approx. 0.5 l
- Time measurements are taken from opening of gas flow to sound alarm in control room

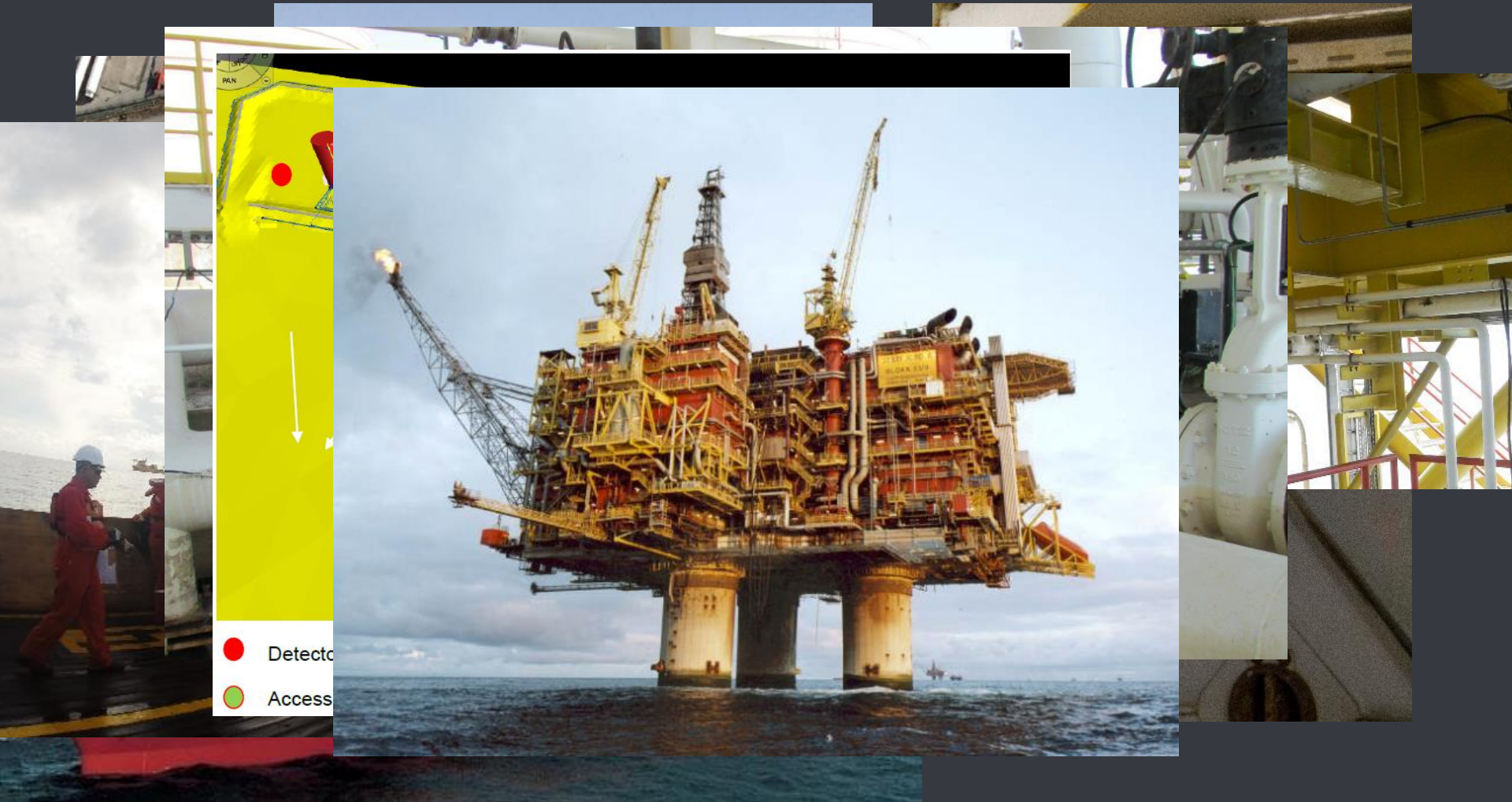


Tag	Time [s]
DG-M24T-78	6.5
DG-M24T-76	5
DG-M24T-70	5
DG-M24T-72	4.5
DG-M24T-74	6.5
DG-M24T-71	3
DG-M24T-69	3
DG-M24T-73	5
DG-M24T-77	6
DG-M24T-75	7

Average battery lifetime > 2 years



Other installations verify similar results and robust environmental performance



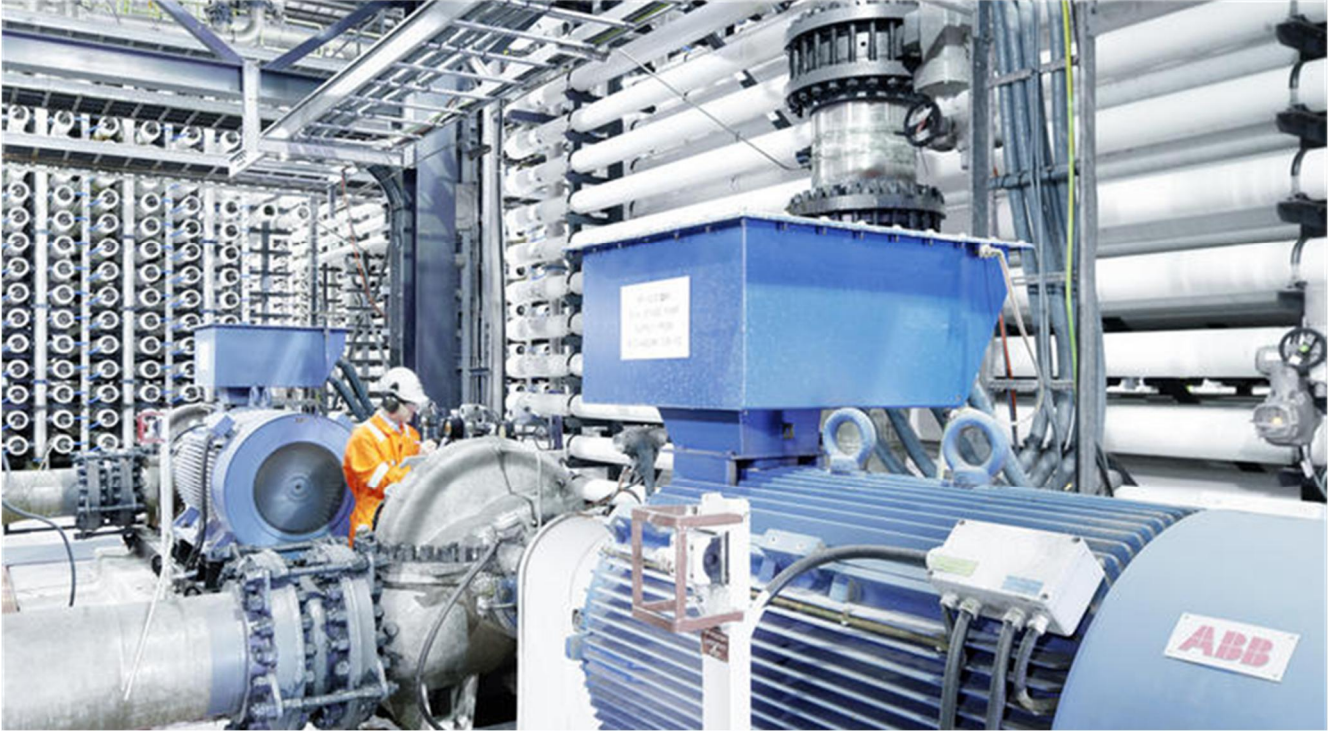
An offshore oil rig at night, illuminated by its own lights. A tall crane structure is visible on the left, and the main processing deck is on the right. The sky is dark and cloudy.

WIRELESS GAS DETECTION

ABB Paper

Functional Safety Conference 4/5 November 2014

A practical view of risk reduction management for safety critical applications Luis Duran/Mike Krywonos



Abstract

Best in Class companies (both National and Global) continue to invest in safety systems; this in most cases is because safety is at the core of their production process and among their key performance metrics, closely linked to their productivity.

Many unfortunate industrial accidents such as the recent explosion of the Deep Water Horizon with the largest marine oil spill in history are evidence of the negative consequences they have on people, environment, production assets and corporations.

This paper discusses the accepted definition of safety and risk reduction in the industry and will discuss the best practices applied by engineers in the design of products for mission critical functions and the implementation of those products in projects.

Both in product design and implementation, this session will dedicate special attention to methodologies or work processes used to reduce potential common cause failures that might impair the operation of the safety system and ultimately expose the facility to a higher risk; and the human factor considerations recommended to ensure proper operation upon a critical condition or an emergency in the industrial process.

Keywords:

Safety, Risk Reduction, Safety Systems, Independent Protection Layers, Common Cause Failures, Functional Safety Management System, IEC61508, IEC61511, TÜV, third party certification, Human Factors

1. Introduction

Best in Class companies worldwide, defined as such for their high percentage of Overall Equipment Effectiveness (OEE) and low injury frequency rate; continue to show strong initiatives intended to expand the safety of their operation. From executive sponsored programs at the corporate level to the definition of proactive risk management strategies, these companies are investing in safety systems and processes; simply because in most cases, safety is identified among the core values of those companies, at the center of their production process and among their key performance metrics, closely linked to their productivity.

There are numerous publications and records of Industrial Accidents, a large number of them with terrible consequences, including not only loss of human life or environmental impact but also affecting the production assets in the site. As an example, in researching for this paper, the authors found record of at least 20 “notable” oil and gas offshore blowouts between 1980 and 2010.

For this paper, the authors compared two serious incidents in the Oil & Gas sector; Piper Alpha operated by Occidental Petroleum and Deep Water Horizon leased to BP. Although both incidents are 22 years apart from each other and occurred in different geographies and have many differences in causes and consequences, each incident illustrates the risk and the potentially catastrophic dimension this industry must confront and the impact on people, environment and corporations, which might cease to exist after these incidents.

2. Defining Safety and Risk

Safety is defined in the industry as a reduction of existing risk to a tolerable or manageable level while risk is a combination of the probability of a harmful incident and magnitude of the harm.

Traditional design practices allocate the risk reduction across different and independent protection layers. The rationale behind it is simple “any system that can fail will fail” so the engineering best practice is to distribute the risk reduction tasks across multiple independent functions or systems. One of these systems is a Safety Instrumented System.

2.1. Safety Instrumented Systems one of many Independent Protection Layers to Reduce Risk

A Safety Instrumented Systems (SIS) is a mission critical system designed following international design practices such as IEC61508 [1] Functional Safety Standard to reduce risk to the people in and around the production environment, the environment, the production asset and the business. In many cases the Safety Instrumented Systems are the last resource to prevent disaster.

SIS performance is measured by Safety Integrity Level (SIL) SIL 1 low, SIL 3 high or Risk Reduction Factor.

As mentioned earlier, the Safety Instrumented System is one of many functionally independent systems each intended to perform a task, as shown on Table 1 typically referred to as Independent Protection layers [2]

Table 1: Expected Functionality of Independent Protection Layers

Layer of Protection	Expected Functionality
BPCS:	Keeping the process under control
Alarms:	Alerting the operator of abnormal conditions and providing guidelines for appropriate operator response
SIS:	Automatically taking the process to a safe condition in case the abnormal condition goes out of control and the operators can't take any corrective action in time
Other layers:	Intended to mitigate the consequence of the hazard

The concept of Independent protection layers (IPL) can also be illustrated in Figure 1

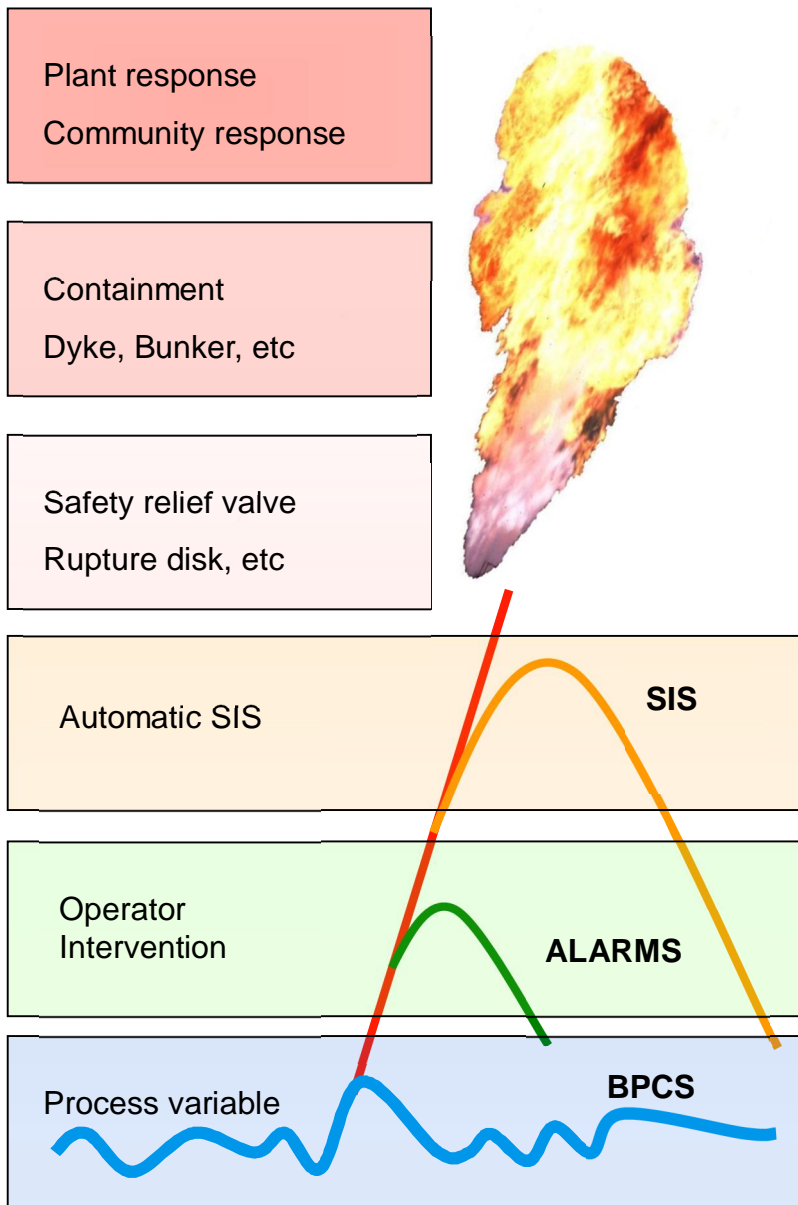
3. Common Cause Failures

The idea of functional independent systems is an attempt to avoid Common Cause Failures (CCF).

Common Cause Failures [3] are failures that might affect more than one of these protection layers at the same time. As engineers, the tendency will be to focus on elements such as Heat, Humidity, Shock, and radio interference among others. However this paper also considers, with special interest, the human elements related to the design of safety critical systems which can contribute to additional failures.

As with other systems, some SIS problems are related to the Commercial Off the Shelf (COTS) products designed for a specific function (i.e. hardware limitations or poor documentation) while other problems are related to the use of those COTS product such as misapplication, user application programming or poor maintenance practices. Both areas can be addressed by implementing appropriate design best practices to reduce risk.

Figure 1: Independent Protection Layers



The industry has conceived these “best practices” as a series of steps that must be performed before putting one of these systems into operation (design, installation and commissioning). This paper will describe the two areas:

- Product Design and Implementation of the Commercial Off-the-Shelf (COTS) Product
- Application Design

3.1. Reducing Common Cause Failures by Design

Traditionally or historically, Systems designed for SIS functions have relied on physical separation and redundancy [4] to reduce common cause failures. The authors identified technology changes across multiple generations of SIS over a period of 30 years. However over the same time frame the industry applied lessons learned from incidents to develop best practices in design and implementation of systems, the international industry standards used more often are IEC61508 and IEC61511 [5] (Figure 2).

3.2. Hardware Fault Tolerance (1st Generation SIS)

1st Generation systems rely on Hardware Fault Tolerance or redundancy to achieve reliability and availability as required for these applications, this practice is rooted in the late 1970s and early 1980s technology. As the majority of these systems were designed prior to the release of the Functional Safety standards, they do not follow the best practices found with regards to design, documentation and testing found in those standards.

3.3. 2nd Generation Systems

As the standards became available (mid 1990s), vendors started to apply the design best practices and to pursue certification to those standards. This generation of systems was produced having third party assessment and certification but continued to rely on Hardware Fault Tolerance to satisfy the performance requirements. The authors found that a large portion of the systems applied as SIS in the market today, although designed to satisfy Functional safety standards haven't change dramatically in their use of hardware fault tolerance and basic software and hardware diagnostics.

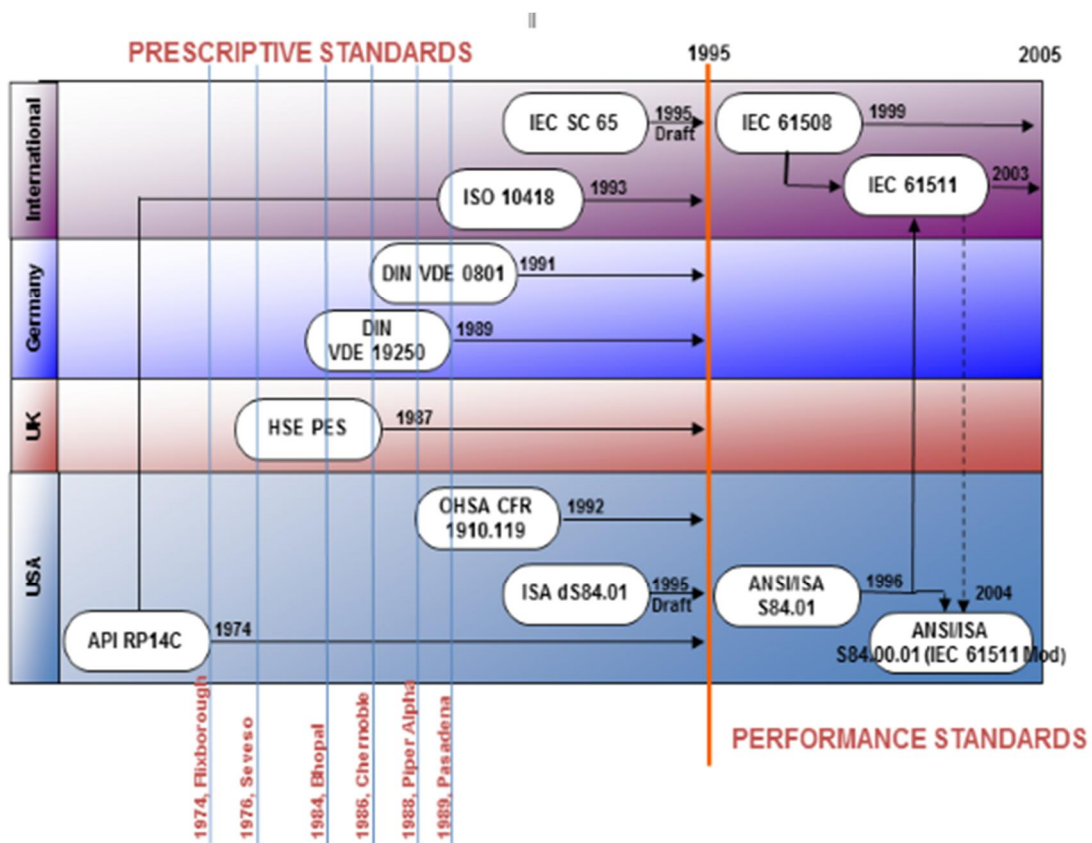
3.4. Diverse Architecture and Implementation of a 3rd Generation Systems

A more recent and different type of system, uses diverse redundancy, diverse implementation and active diagnostics [6] and can deliver not only reliability and availability required for the application while minimizing common cause failures found by the use of the same technology but also introduce additional protection to systematic failures normally related to human factors.

3.4.1 Hardware Design – Diverse Hardware

This newer generation of systems use diverse processing hardware (multiple technologies) such as diverse operating systems and diverse hardware and diverse redundancy, both enhanced with diverse implementation (different implementation teams).

Figure 2: Evolution of National Prescriptive Standard to International Performance Base Standards



3.4.2 Application Execution in a SIL Compliant Environment

The use of diverse operating systems (using different technologies) including the use of third party certified COTS and different execution path with different compiler rules extends the risk reduction found in the hardware design to the firmware/software environment in the system, including the use of limited variability software functions and provision of systematic capabilities as specified in the Functional Safety standards for critical applications.

3.4.3. Systematic Capabilities and Human Error

The concept of systematic capabilities and its associated performance measurement was introduced in the latest revision of IEC61508 standard; the concept did not exist as such in 1st Generation systems and was emerging in 2nd generation systems.

3.5. Safety and Network Security

1st and 2nd generation Safety Systems were not designed to reside on a networked plant. For the most part, these systems allowed some communication interface or gateway but were not intended for integration. In general, therefore, 1st and 2nd generation Safety System are not equipped to counter security threats like those the industry has experienced in recent years.

A brief analysis of the definitions will clearly show that Safety issues are random in nature and statistical analysis is possible security intentional in nature and statistical analysis will not measure performance.

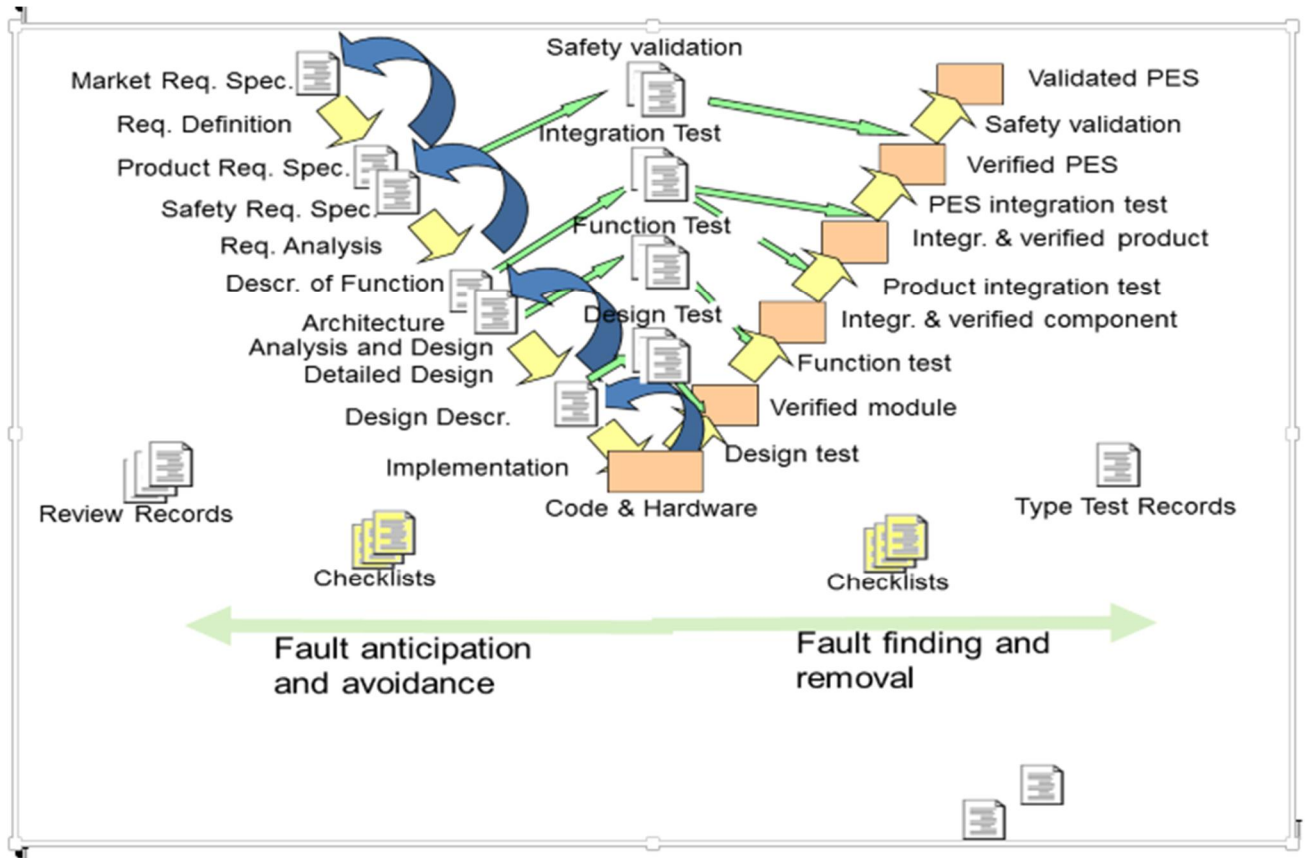
The authors concur with industry standards and experts in the field. Network security may affect system performance and the safety of the installation. A system can't be safe without it being secure.

3.6. Design Best Practices and V-Model

As indicated earlier, industry standards in Functional Safety introduced the concept of Functional Safety Management System (FSMS) which includes a series of steps in the design, documentation and testing of the system, and should include Network Security as well.

Today product development or design organizations responsible for releasing COTS products (hardware and software) intended for safety applications use design best practices as the V-Model (Figure 3) and are evaluated by a third party organization (i.e. TUV) and their FSMS is approved prior to the assessment of their products.

Figure 3: Product Development V-Model



4. Engineering best practices to reduce risk in application design

As indicated previously, best practices in design apply both in the design of a Commercial Off-the-Shelf (COTS) Product and the Application Design or the application of a COTS tailored to reduce a particular risk in an industrial installation.

Best Practices in Application Design will apply a model similar to the V-Model used in the development of a product (Figure 3) and reinforced by a structured Quality Management system appropriate for Functional Safety applications.

Application Design starts with Hardware Design following the COTS Product's Safety Manual and considers the particularities of the application as described on the Application Safety Requirements Specification to design a system that is less susceptible to product failures by considering aspects such as:

- Power feeds and Power Supplies
- CPUs
- I/O Modules Hardware
Application Software
- Networks

4.1. Hardware

It is clear that hardware is not perfect, it is subject to failure, and the application design must consider failure recovery modes or additional risk reduction methodologies or options including such diverse methods of performing shutdowns as:

- Hardwired pushbutton
- Hardwired logic systems (with appropriate SIL rating)
- Solid State relays, etc.

4.2. Software

One critical aspect that has gained visibility in recent years is the software design of the application. Efforts in this area include the development of a well-documented Software Functional Design and appropriate selection of software tools and libraries to meet the Safety Integrity Level (SIL) required for the application. Software design also includes Code Review practices including Independent Validation and Verification depending on the SIL, competence of the programmer and other elements described later in section 5.1. The features available in the COTS product addressing the systematic capabilities requirements are a valuable asset for the programmer and contribute to reducing potential errors that will later affect the safety of the installation.

4.3. Functional Testing and Periodic Proof Testing

Another critical aspect is Functional Testing and Periodic Proof Testing, particularly because Not ALL System Faults are Self-Revealing and Covert Faults that may inhibit SIS action on Demand can only be detected by testing the entire system. This requires not only a Full Functional Test prior to commissioning, typically conducted as an integration test in the vendor or System Integrator's facility (as well as later in the final instrumentation room in the plant), but also Periodical Functional Tests using a documented procedures to Detect Covert Faults and covering the entire SIS.

Functional Testing should record and analyze activation of SIS functions, and spurious activation of an Emergency Shutdown Valve due to a Process Shut Down, but this does not test the Entire Function of the same valve during an ESD action.

5. Automation can't check for human intervention

Once the design is complete, all of these systems will have different degrees of interaction with users, and different types of users with different levels of competence depending to their role (i.e. operation, maintenance personnel and engineers)

The most sophisticated automation can't prevent human error, industrial plants are designed with the highest accuracy in mind, with several separate safety loops often checking the integrity of process systems. This apparatus however can't check for human intervention and a small human error could cause an enormous catastrophe. 70% of reported incidents in the oil and gas industry worldwide are attributable to human error and account for in excess of 90% of the financial loss to the industry.

Results from research conducted by the Health and Safety Executive and published in the book "Out of control: Why control systems go wrong and how to prevent failure" [7] show the impact of the human element in industrial incidents throughout a project lifecycle. This is shown on Figure 4.

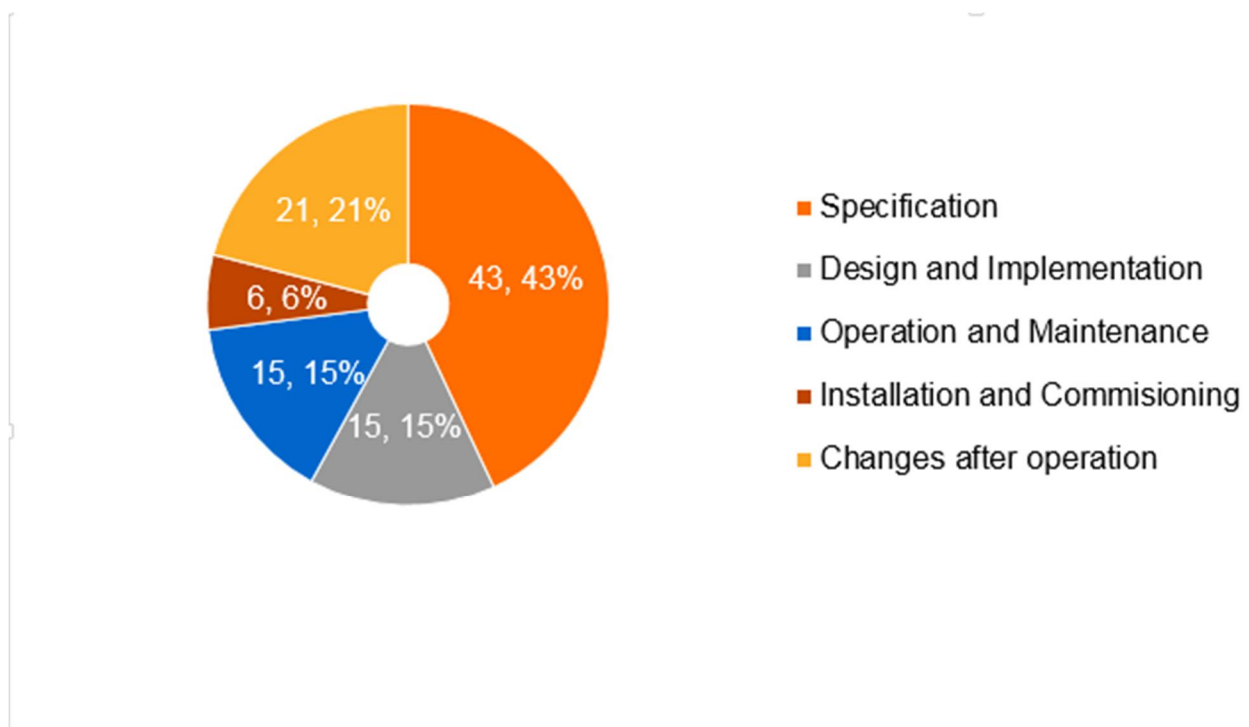
International Functional Safety Standards (IEC 61508 and IEC61511) and previously ISA 84 introduced the concept of the Safety Lifecycle, describing the phases that should take place from concept to design to implementation and operation of a Safety Instrumented System. The Safety Lifecycle is a step in the direction of reducing the impact of human factors by establishing the proper design best practices, documentation reviews and validation and verification steps in the execution of a safety project. Additionally the standards introduce two important elements: Competence of Personnel mentioned briefly in Section 4.2 and Functional Safety Management System (FSMS).

Recent changes to International Functional Safety Standard IEC61508 have turned the requirements on FSMS and Competence of Personnel into normative clauses of mandatory compliance instead of a recommendation as was presented in the previous version of the same standard.

5.1. Functional Safety Management System (FSMS) and Competence Requirements

A Functional Safety Management System (FSMS) consists of proven and validated procedures, methodologies, templates and report outlines, covering those essential elements of hazard and risk assessment; SIL determination; SIS design and SIL capable hardware, SIS installation, SIS commissioning and validation and SIS operations and maintenance. A FSMS is used in the design of a COTS product and during the Application Design. It's typically an extension of the existing Quality Assurance/Quality Management process and has a lifespan from conception to decommissioning of the SIS and beyond to become part of the organization best engineering practices and work processes.

Figure 4: Root Cause of Control System Failures



As indicated, the safety standards call for competence of personnel. This requirement shouldn't be interpreted as a need for safety experts in every aspect of the design, commissioning or operation and maintenance of a SIS, but instead as the need for an evaluation of the appropriate expertise and experience required to perform a particular job function in any phase of the safety lifecycle. In practical terms, those involved with activities related to a safety system should have demonstrated "competence" either by formal training, certification or accreditation or on-the-job relevant experience.

The reader might conclude that the standards today require competent and independent review groups because system designers don't trust product designers or other application designers and therefore we would rather be safe than sorry.

6. Summary

In summary:

- Best in Class companies link safety to their success and invest in programs and systems to reduce their risk
- Engineers have attempted to reduce risk by minimizing the potential for common cause failures
- Common cause failures can occur in products (hardware or software) or the implementation of the application
- The industry has conceived best practices (i.e. FSMS) to minimize the impact of human error
- Human factors can't be ignored in the design, particularly in the application design
- Enforcement of these best practices via formal FSMS has proven to be a way to reduce the risk introduced by engineers...it's vital!

7. References

[1] IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems International Standard 2010

[2] Integrating Control and Safety: Where to draw the line.

Robin McCrea-Steele, TÜV FSExpert, Invensys-Premier Consulting Services

[3] Common Cause and Common Sense, Designing Failure Out of Your SIS

Angela E. Summers, Ph.D. and Glenn Raney, Oct 2000

[4] Integrated but separate, Advances in integrated and safety control,

Roger Prew, ABB , June 2009

[5] IEC 61511 Functional safety - Safety instrumented systems for the process industry sector International Standard 2003

[6] Providing Independent Layers of Protection with Integrated Safety Systems

Luis M. Duran, ABB and Ron Johnson Dow Chemical, Oct 2009

[7] Out of control: Why control systems go wrong and how to prevent failure

HSE Books ISBN 0-7176-2192-8



Luis Duran

Functional Safety Conference 4/5 Nov 2014

A Practical view of Risk Reduction

Insert Subtitle (4th blue)

Table of Content

- Safety, Risk and consequences in industrial processes
- Understanding Safety and Risk
- Risk Reduction
 - Independent Protection Layers
 - Common Cause Failures
- Engineering practices to reduce risk
 - Product design
 - Application design
- Human Factors and Safety
- Functional Safety Management practices

Car safety: Costs much more than money

- Motor vehicle crash annual costs
 - 3.5 million injuries
 - 35,900 deaths
 - \$245 billion total estimated costs



National Safety Council Injury Facts, 2011

Car safety

Costs much more than money



Top priority for Best-in-Class Companies Safety



- Best-in-Class Companies (Top 20%) - 90% OEE (Overall Equipment Effectiveness) , 0.2 injury frequency rate
 - Executive leadership drives focus on safety
 - Establish a proactive risk management strategy
 - Invest in Safety Systems

Source: Aberdeen Group, October 2011

Is this a Safe Plant?

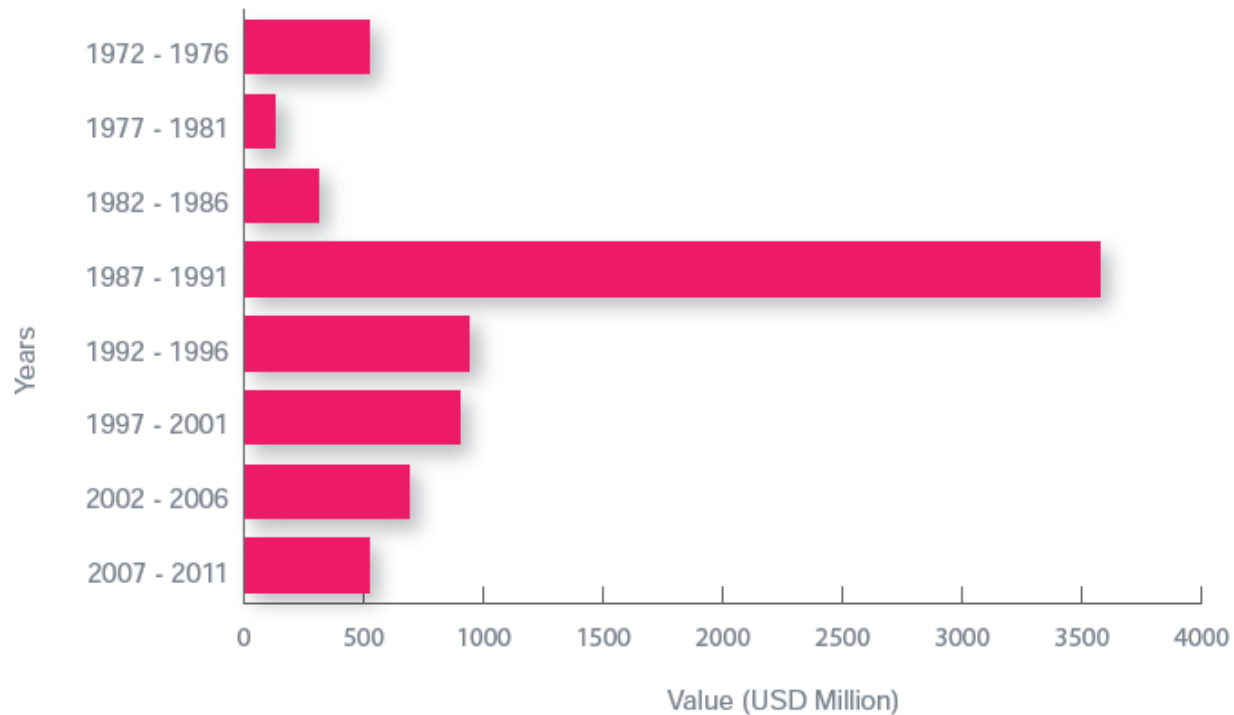


Manager:
I know everything is all right because I never get
any reports of things being wrong”.

Safety in the process industries

Losses continue worldwide

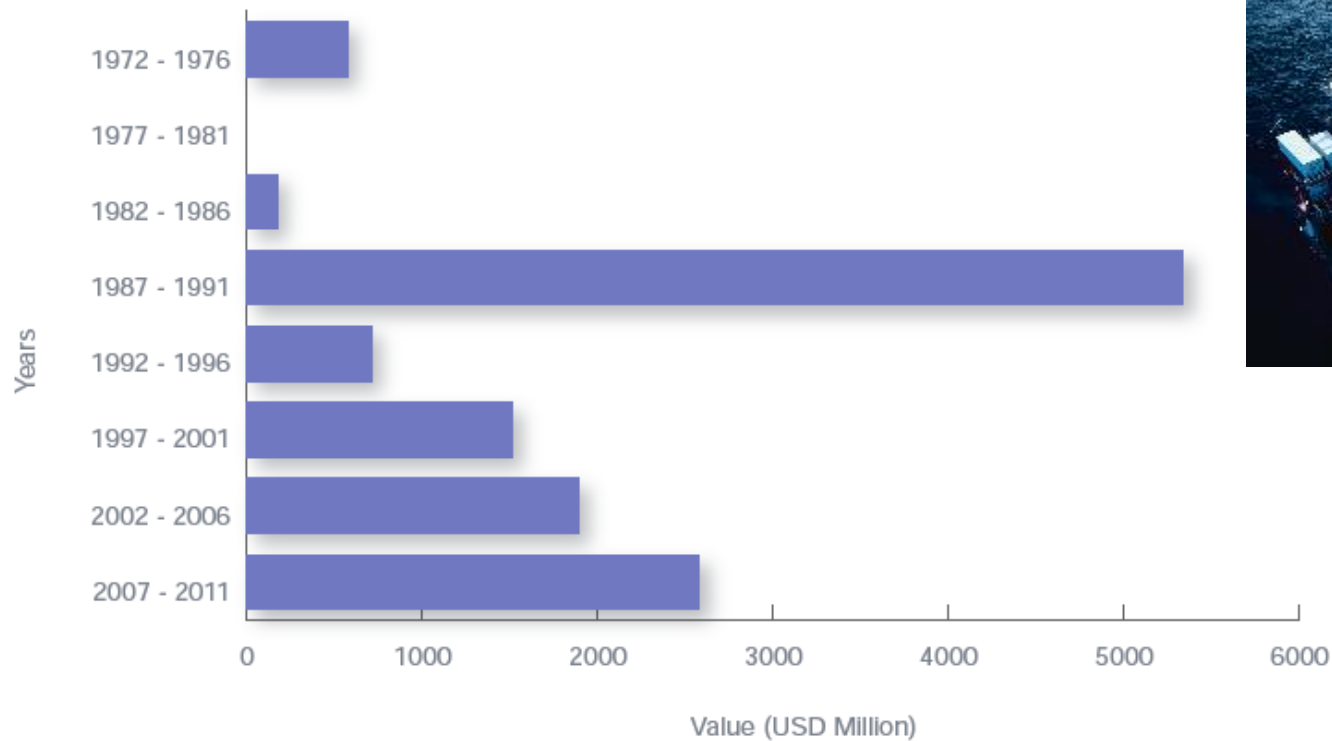
PETROCHEMICAL LOSSES IN FIVE YEAR PERIODS



Safety in the process industries

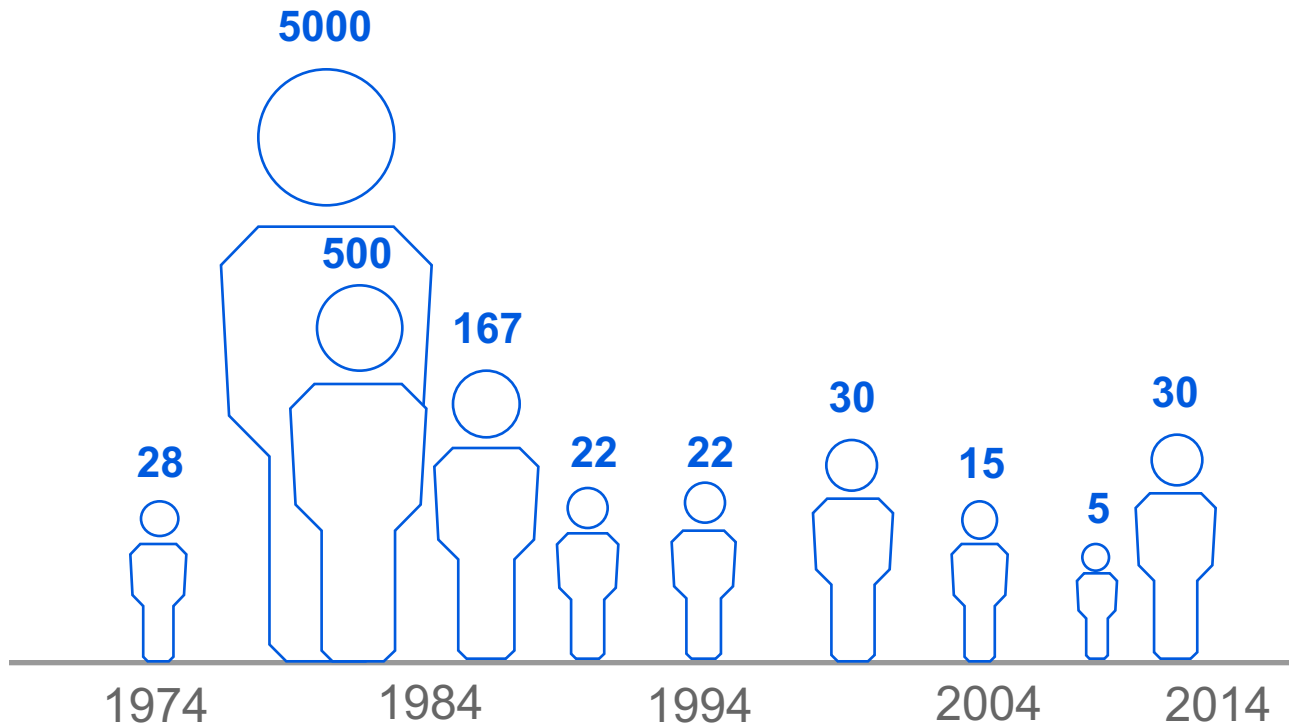
Losses continue worldwide

UPSTREAM LOSSES IN FIVE YEAR PERIODS

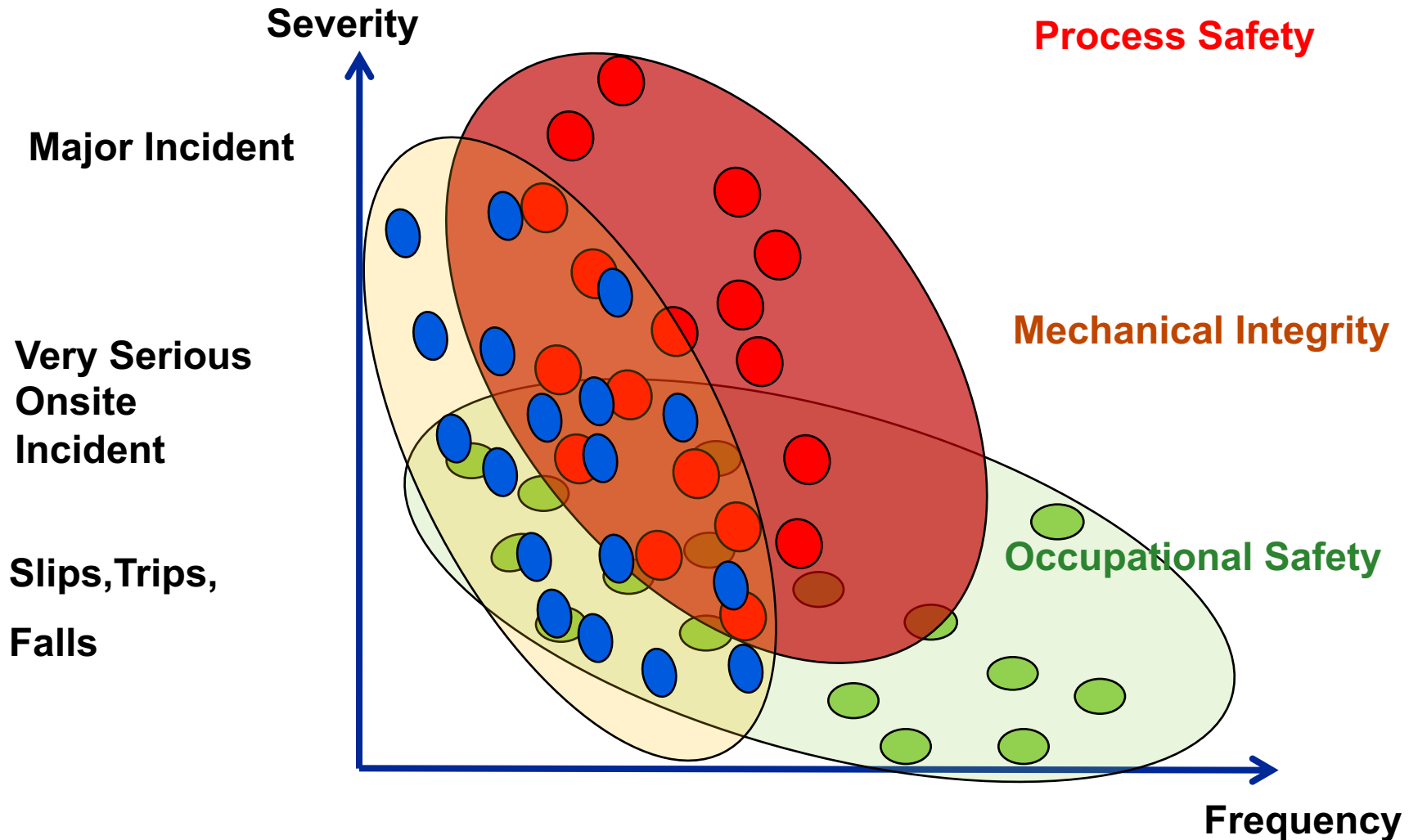


Safety in the process industries

Human consequences



Personal safety and process safety



Safety Instrumented Systems (SIS)

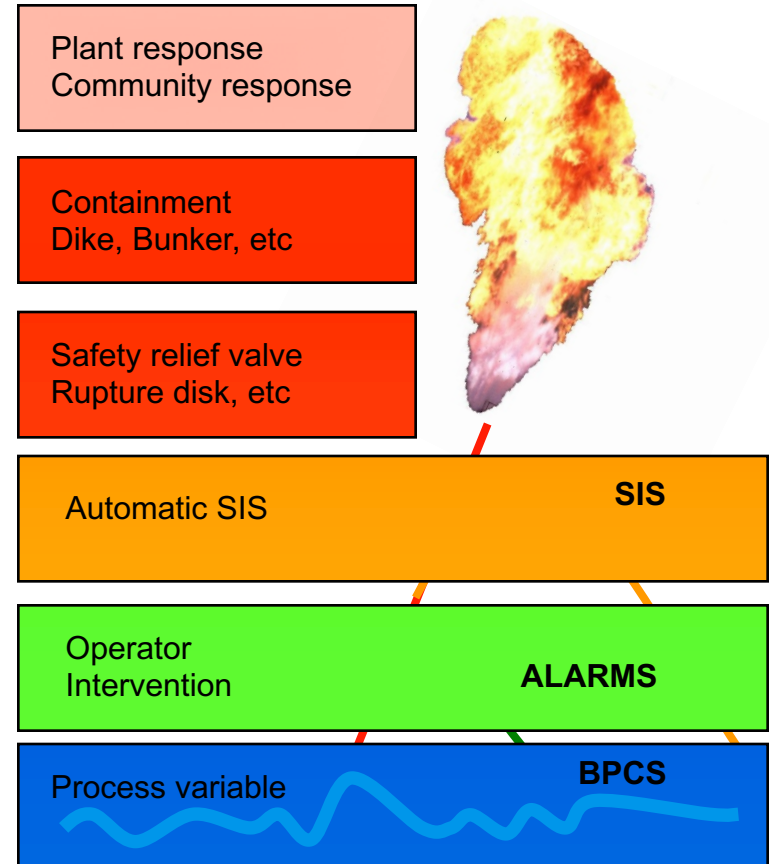


- SIS reduce risk and consequently protect
 - People,
 - Environment
 - Equipment and
 - Business
- SIS performance is measure by Safety Integrity Level (SIL)
 - SIL 1 (Lower)
 - SIL 4 (Higher)

Risk Reduction

Independent Protection Layers (IPL)

- Each IPL must independently protect against the hazard they are designed to safeguard
- Hazard occurs when a layer fails to respond to the process demand
- Objective of SIS IPL must be maintained



Any system that can fail will fail...

Common Cause Failures

- Common Cause Failures (CCF) occurs when a single failure from a common source of stress results in the failure of multiple components.

- Stress?

- Heat, Humidity, Shock, Vibration
- Chemical Corrosion
- Electrical Surge, Electrostatic Discharge
- Radio Interference



- Human Errors



Where are the SIS problems?

Problems may be related to...

Product

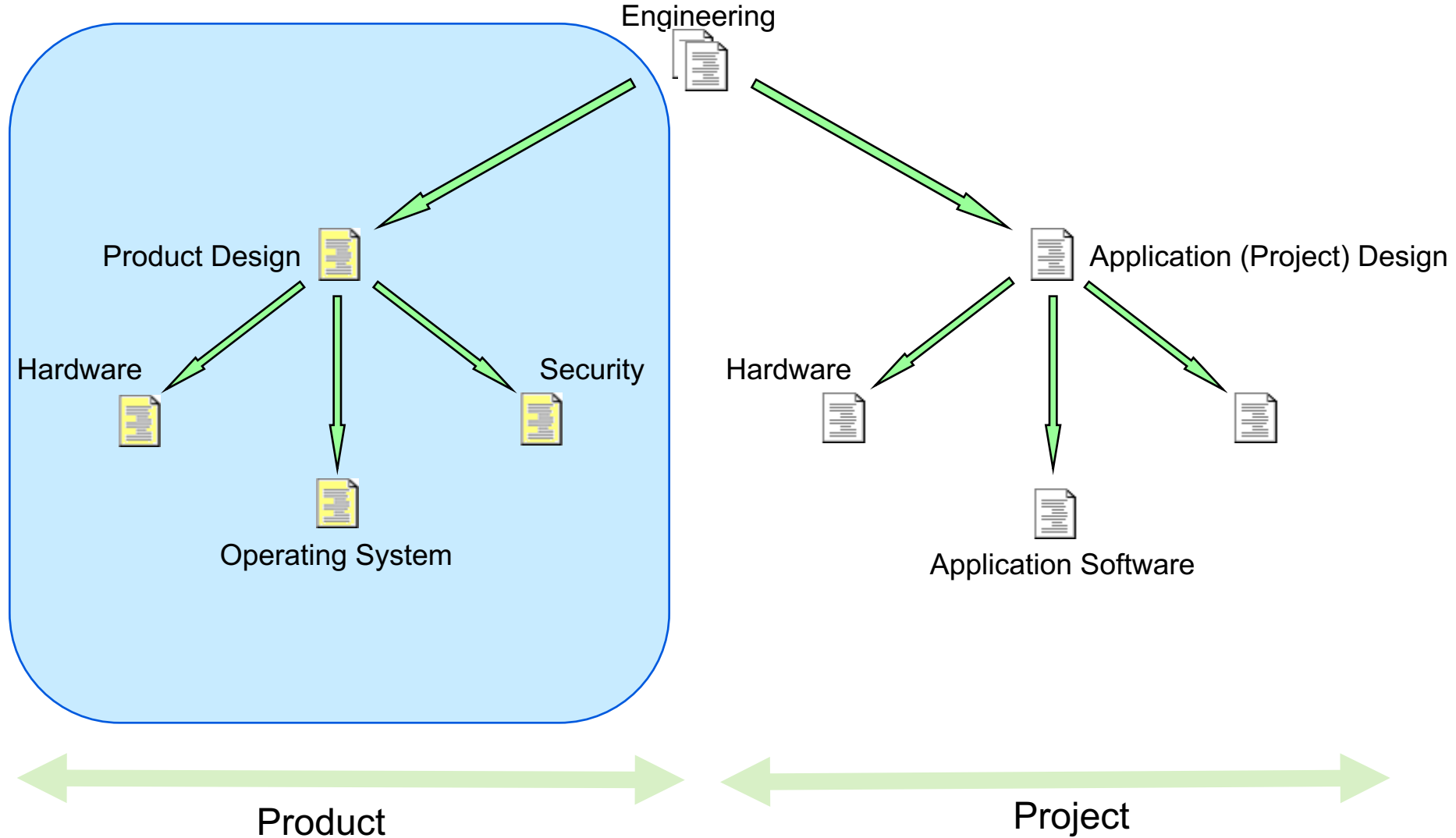
- Hardware
- Operating systems
- Lack of diversity
- Security vulnerabilities
- Documentation
- Ease of use

Project

- Hardware
- Programming
- Operation
- Maintenance
- Training
- Competency
- Security

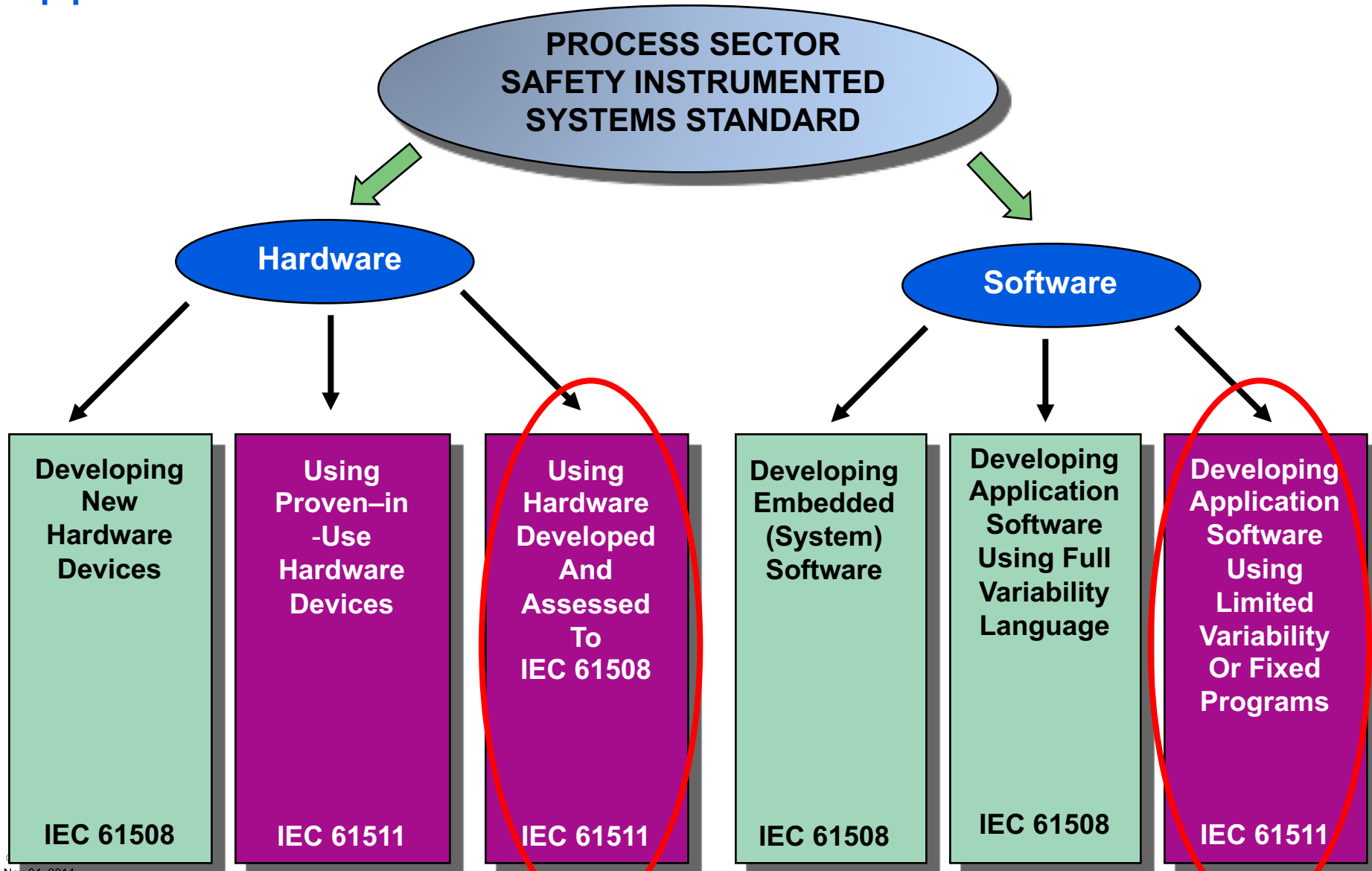


Engineering practices to reduce risk



Functional Safety Standards

Application of IEC 61508 and IEC 61511



Common Cause Failures Avoidance Design Strategies

Hardware

- Physical Separation
 - Redundancy and modularity
(different board, different racks)
- Diversity
 - Redundancy via different
technology
- Verification and Validation

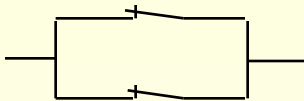
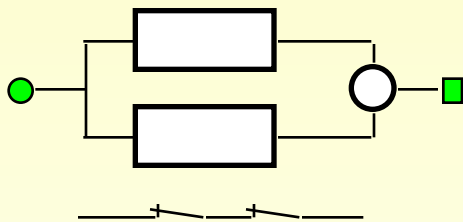
Software

- Physical Separation
 - Different execution path
- Diversity
 - Different object code
- Verification and Validation

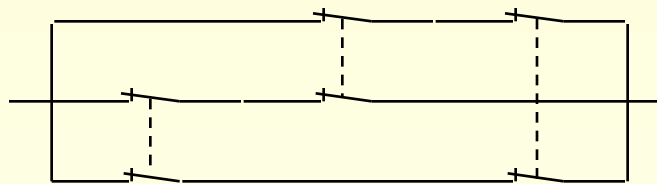
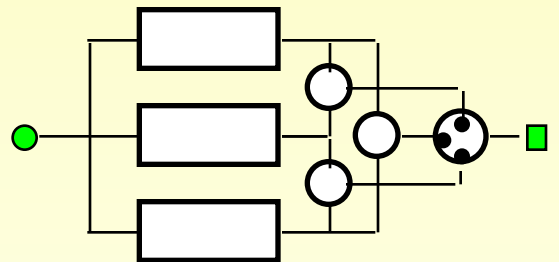


Hardware Fault Tolerant Architectures (1st Generation SIS)

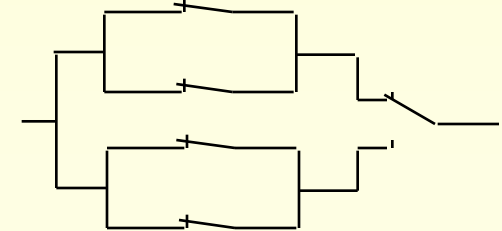
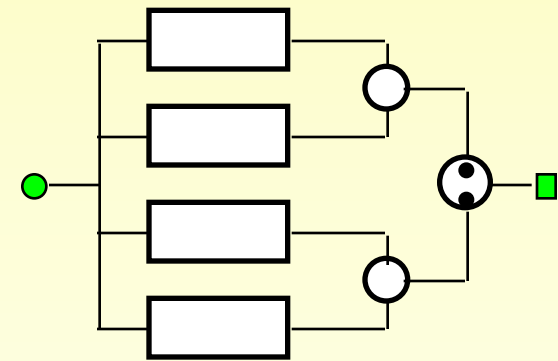
- Duplex
 - 1oo2D



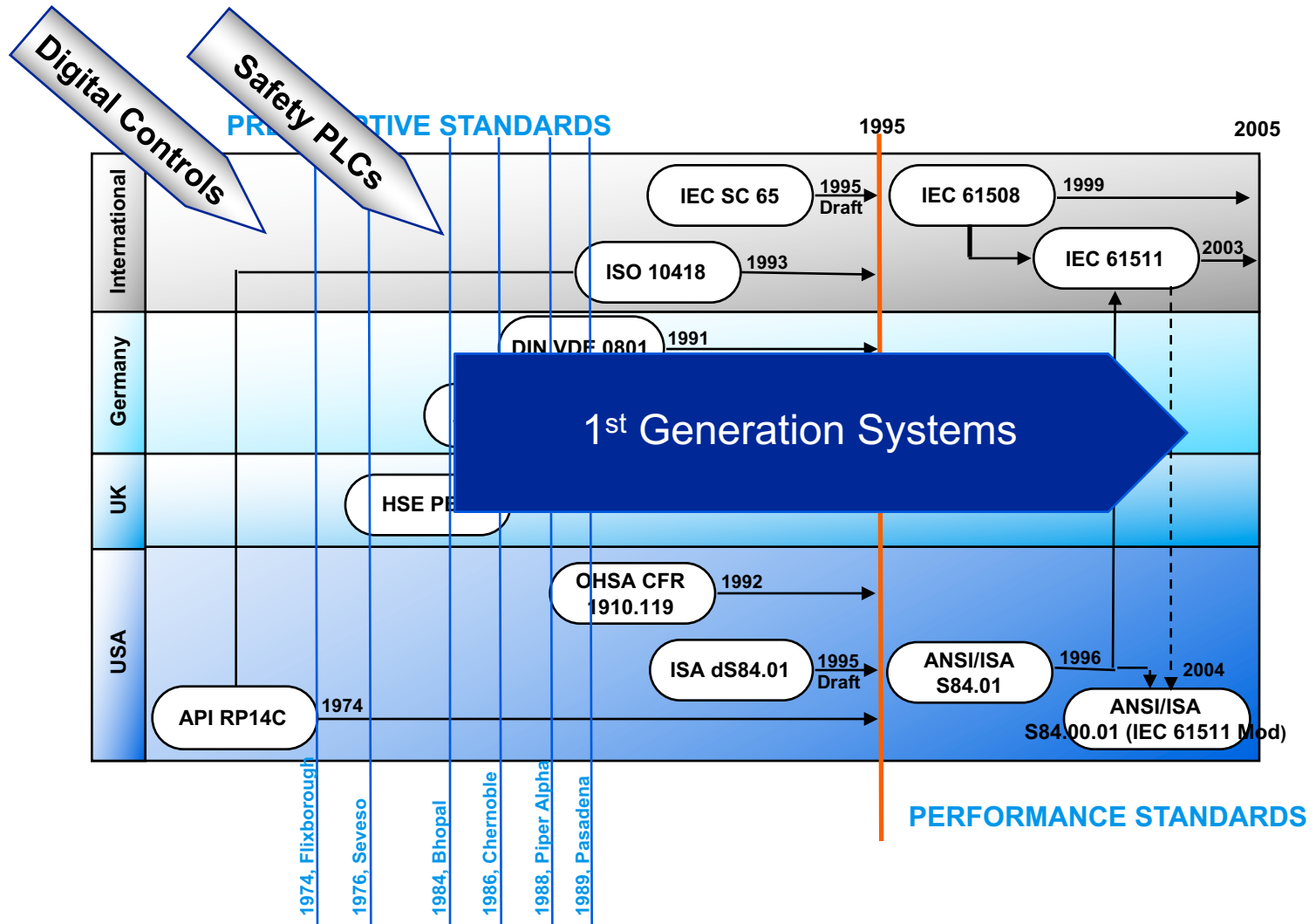
- Triplex
 - 2oo3



- Quad (Bi-Duplex)
 - 2oo4D

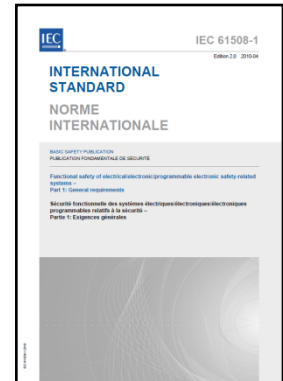


Safety Standards Timeline



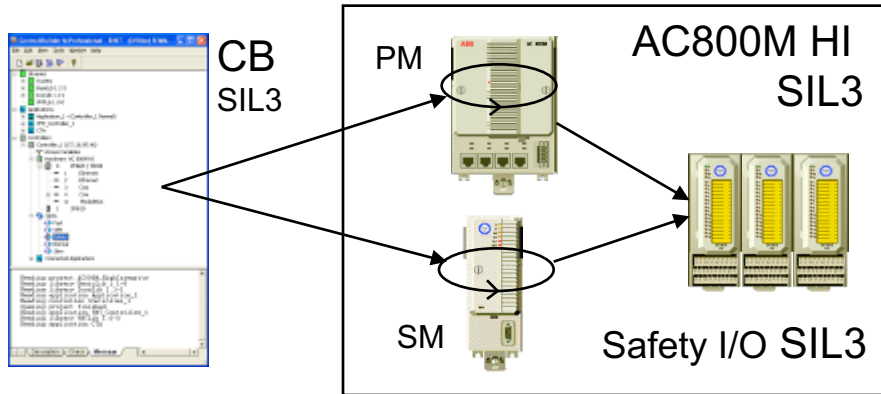
2nd Generation Safety Systems ...better but not perfect

- 2nd generation systems..
 - Were developed and certified in accordance to standards (i.e. IEC 61508)
 - Provide additional software diagnostics to help identify latent faults
- However, they still ...
 - Rely on redundancy for safety as well as availability
 - Focus on identical paths and voting for Safety (hardware fault tolerance)
 - Do not use diversity to eliminate common cause issues
- Certification is conducted by an accredited third party entity





3rd Generation Safety Systems

Diverse Architecture and Implementation, Certified



- Newer systems (i.e. SIL 3 800xA High Integrity controller) has parallel processing paths based on diverse technology
- Integrity voting between paths
- Built in active software diagnostics
- Controller and Supervision Module developed by diverse (different) teams (Vasteras and Malmo, Sweden) and tested by a third team (Oslo, Norway) by people with different backgrounds
- The two channel architecture meets SIL3 requirements for hardware fault detection and reaction

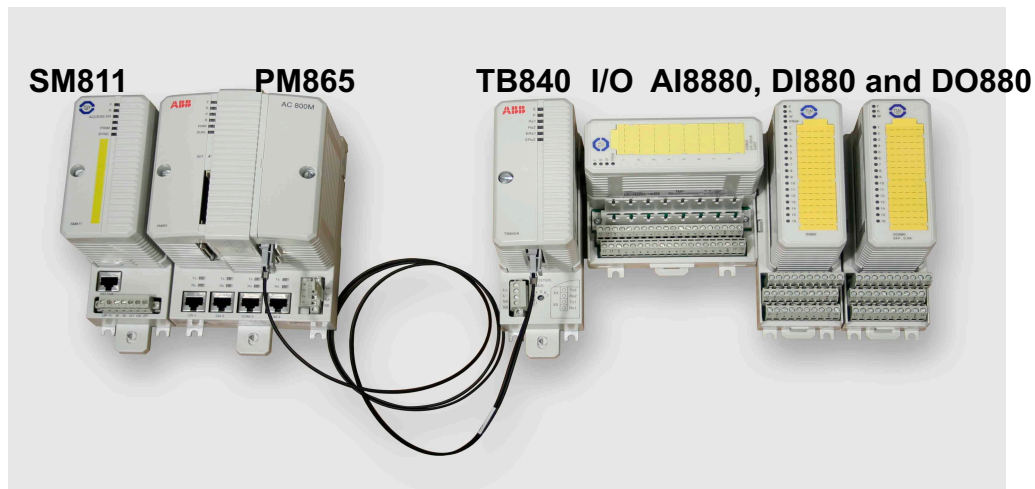
	HFT	
SFF (%)	0	1
< 60	—	SIL 1
60 - 90	SIL 1	SIL 2
90 - 99	SIL 2	SIL 3
> 99	SIL 3	SIL 4
	 1001D	 1002D

IEC61508-2 Table 3

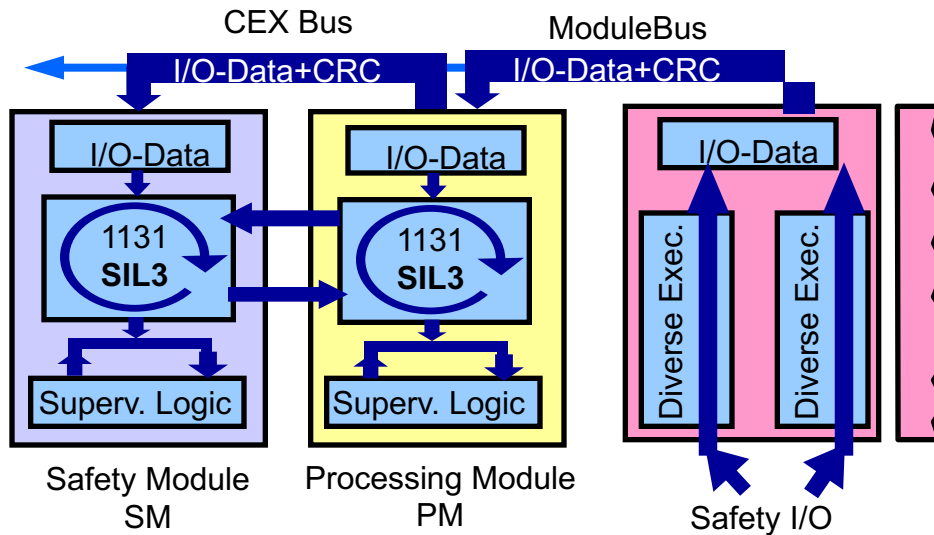
Hardware Design

Diverse hardware

- Controller diversity
 - Firmware
 - Development teams
 - Operating systems
 - Internal Firewalls
- Development teams
- I/O System diversity
 - Diverse hardware (FPGA and MCU)
 - Firmware



System 800xA High Integrity Application Execution



Parallel diverse execution allows a hardware fault tolerance of 1 for SIL3 applications

HFT = 1 (SIL 3 Execution)

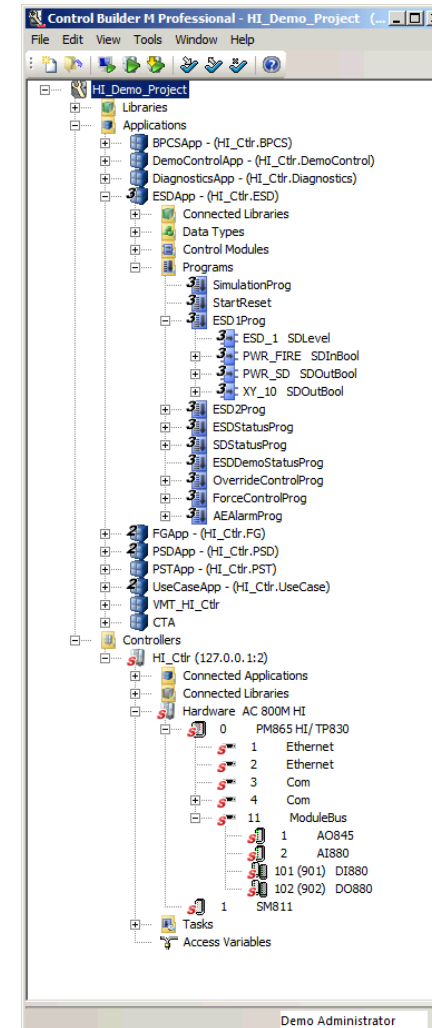
SFF	Hardware fault tolerance		
	0	1	2
< 60 %	Not allowed	SIL 1	SIL 2
60 % - < 90 %	SIL 1	SIL 2	SIL 3
90 % - < 99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

IEC 61508-2, Table 3

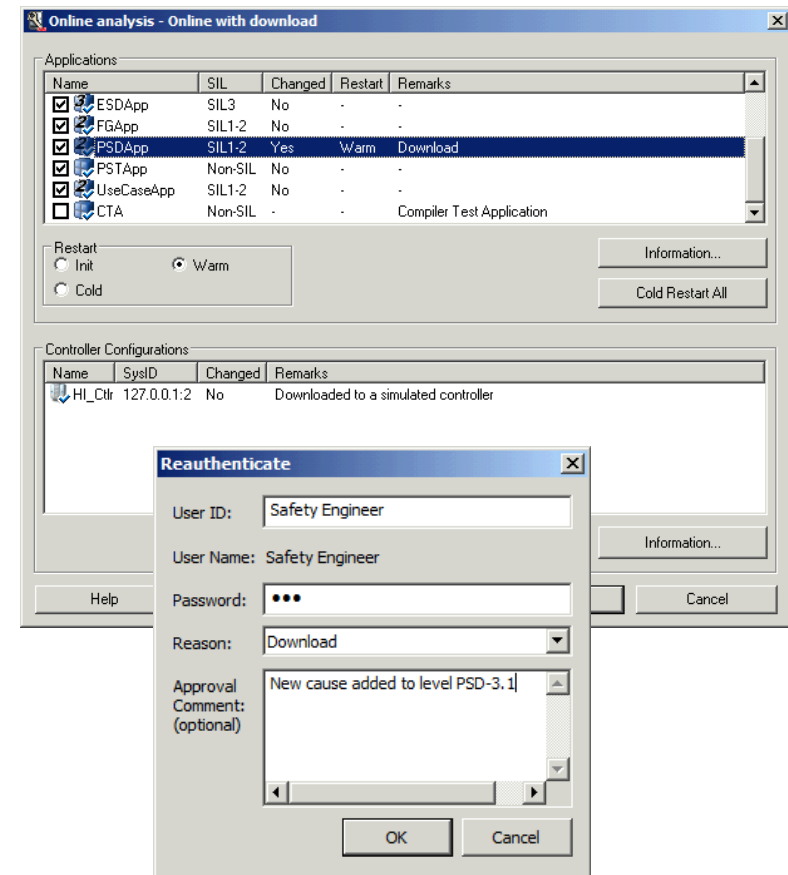
Safety System Engineering

SIL Compliant Application Environment

- Engineering tool automatically limits user configuration choices to ensure integrity
- Safety functions protect and control download to the process and runtime environment
 - Download is prevented unless all SIL requirements are met
- Embedded firewall mechanisms include:
 - CRC protection on different levels
 - Double code generation with comparison
 - Compiler with revalidation



- Concept developed for systematic safety integrity compliance for elements and sub-systems
- Replaces the term: “effectiveness against systematic failure”
- Measure on a scale 1-4 that the systematic safety integrity of an element fulfills the given safety function
 - Considering the instructions stated in the safety manual



Source: IEC 61508 Clause 7.4.7.6

- **Safety:**

Freedom from unacceptable risk of physical injury or of damage to the health of people, either directly or indirectly as a result of damage to property or to the environment.

IEC 61508

- **Security:**

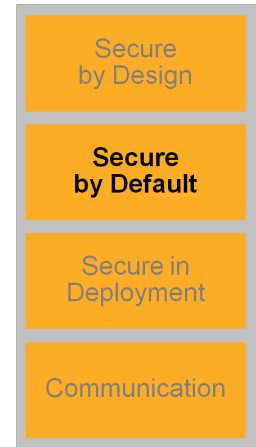
Preventing intentional or unintentional interference with the proper and intended operation, or inappropriate access to confidential information in industrial automation and control systems

ANSI/ISA-99.00.01-2007



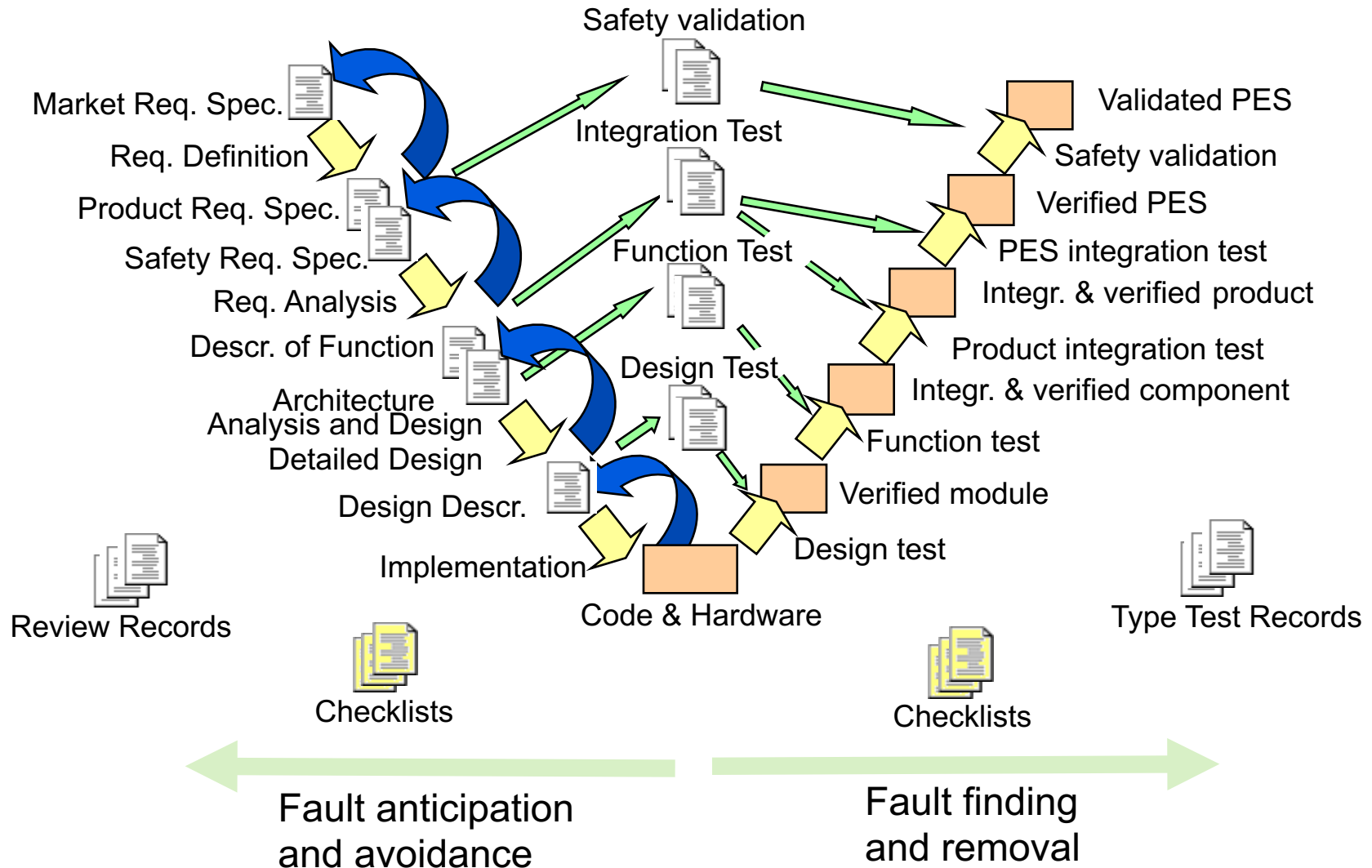
Secure by Default, Defense in Depth Certified SIL3 Communication

- SIL3 certified (IEC 61508) Communication Concepts
 - Access Control with Physical Key switch
Controlling configuration changes
 - SIL3 Peer-to-peer (Controller to Controller)
 - Safe Online Write (Operator Workplace to Controller)
 - Safe Project Download (Engineering Workstation to Controller)



Software and Hardware Development Model

Application of IEC 61508-1 V-Model



Safety System Development Procedures

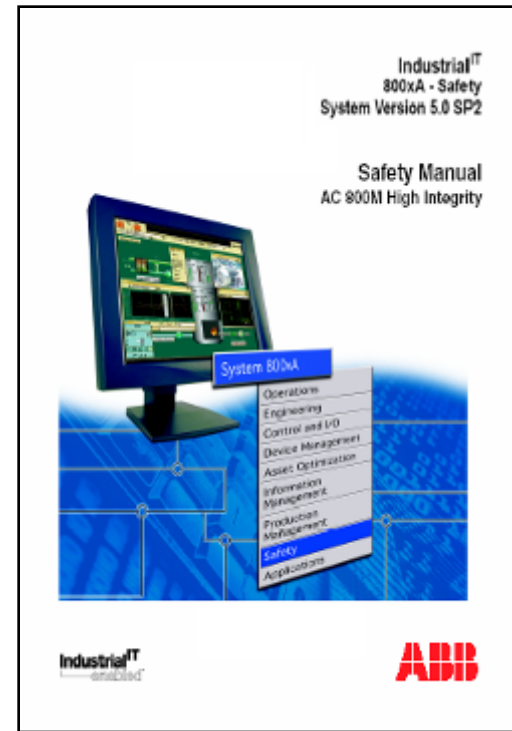
Follow a certified Functional Safety Management



Product Safety
Certificate

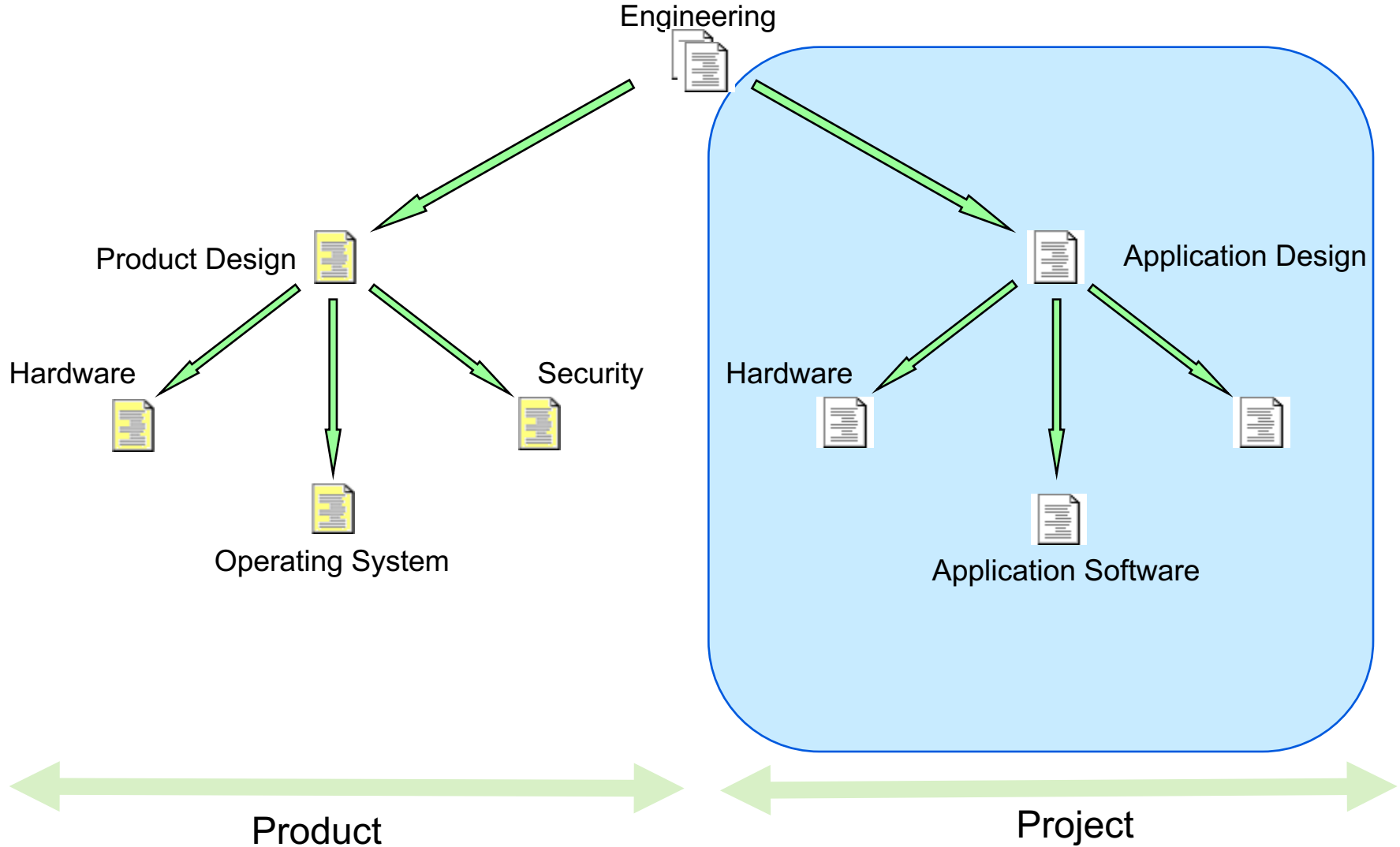


Development Department
Safety Certificate



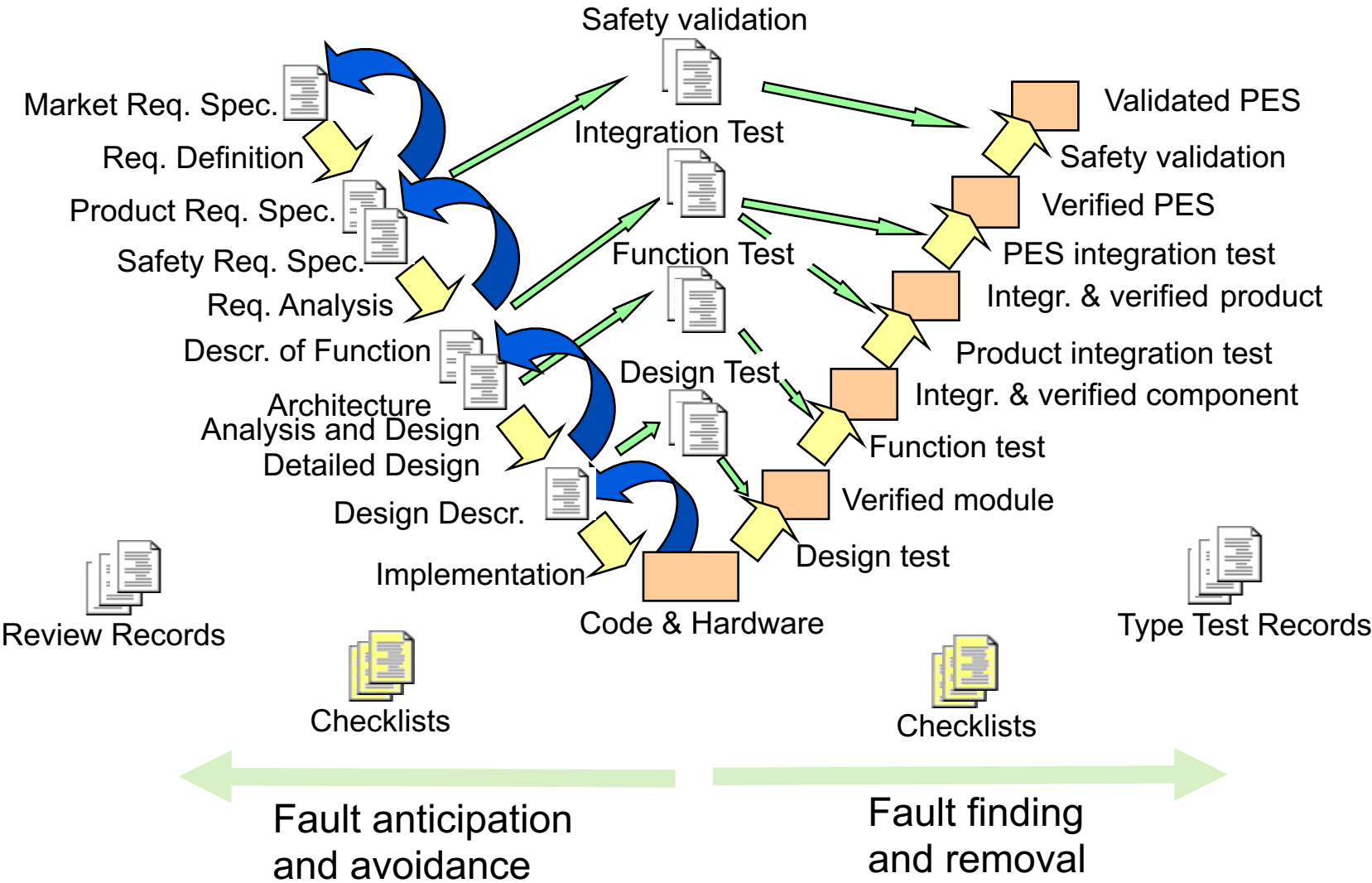
Safety Manual

Engineering practices to reduce risk



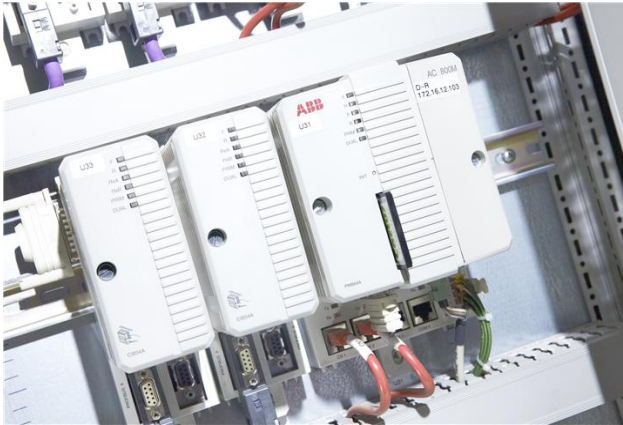
Software and Hardware Development Model

Application of IEC 61508-1 V-Model



- Production Hardware fails
 - Implement redundancy
 - Power feeds
 - Power Supplies
 - CPUs
 - I/O
 - Networks
 - Etc.



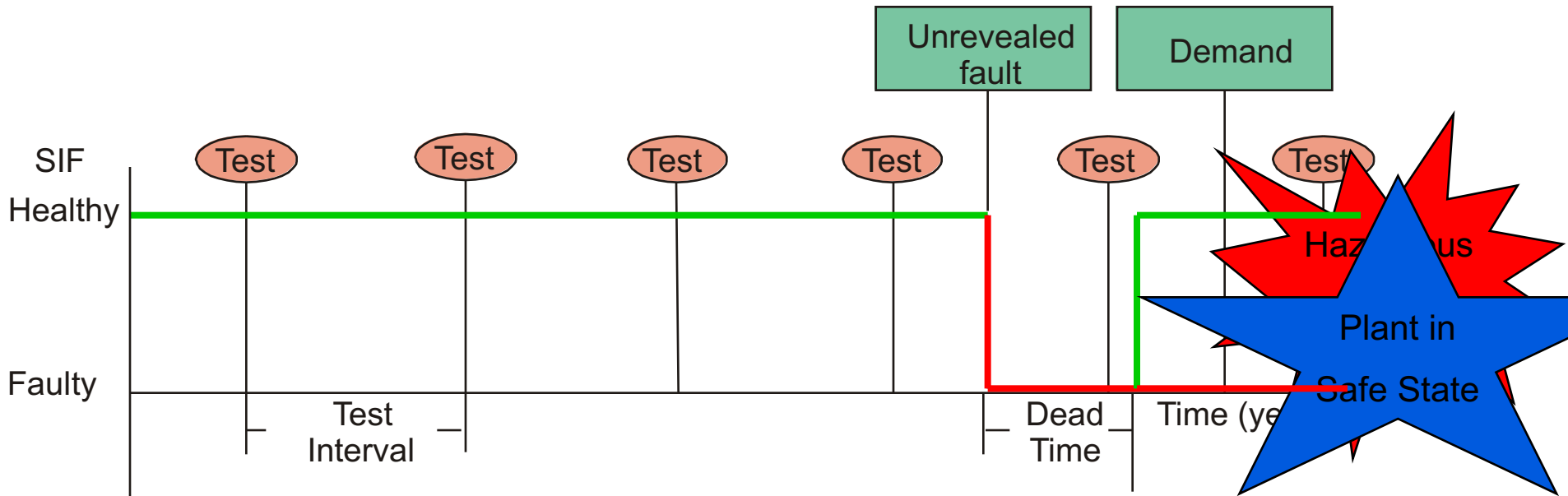


- Despite precautions hardware still fails
- Diverse methods of performing shutdowns are implemented
 - Hardwired wired pushbutton,
 - Hardwired logic systems (SIL4)
 - Solid State relays
 - Etc.

- Not ALL System Faults are Self-Revealing
- Covert Faults that may inhibit SIS action on Demand can only be detected by testing the entire system
- Periodical Functional Tests shall use a documented procedure to Detect Covert Faults
- The entire SIS shall be tested
- Functional Testing should Record and Analyze activation of SIS functions
- Spurious activation of an ESV due to a PSD, does not test the Entire Function of the same valve during an ESD action

Why Do We Test?

to expose un-revealed failures



How often should you test?

IEC61511-1 clause 16.3.1.3 states 'The proof test interval shall be as decided using the PFDavg calculation.'

Which is the ideal Control Room?



Losses

- Lost revenues due to facility down time
- Replacement costs for equipment and machinery that has been damaged
- Medical costs associated with injury
- Costs of disability payments
- Legal costs and lawsuits
- Fines due to non-compliance or environmental pollution
- Recruitment and training costs associated with replacing injured employees.

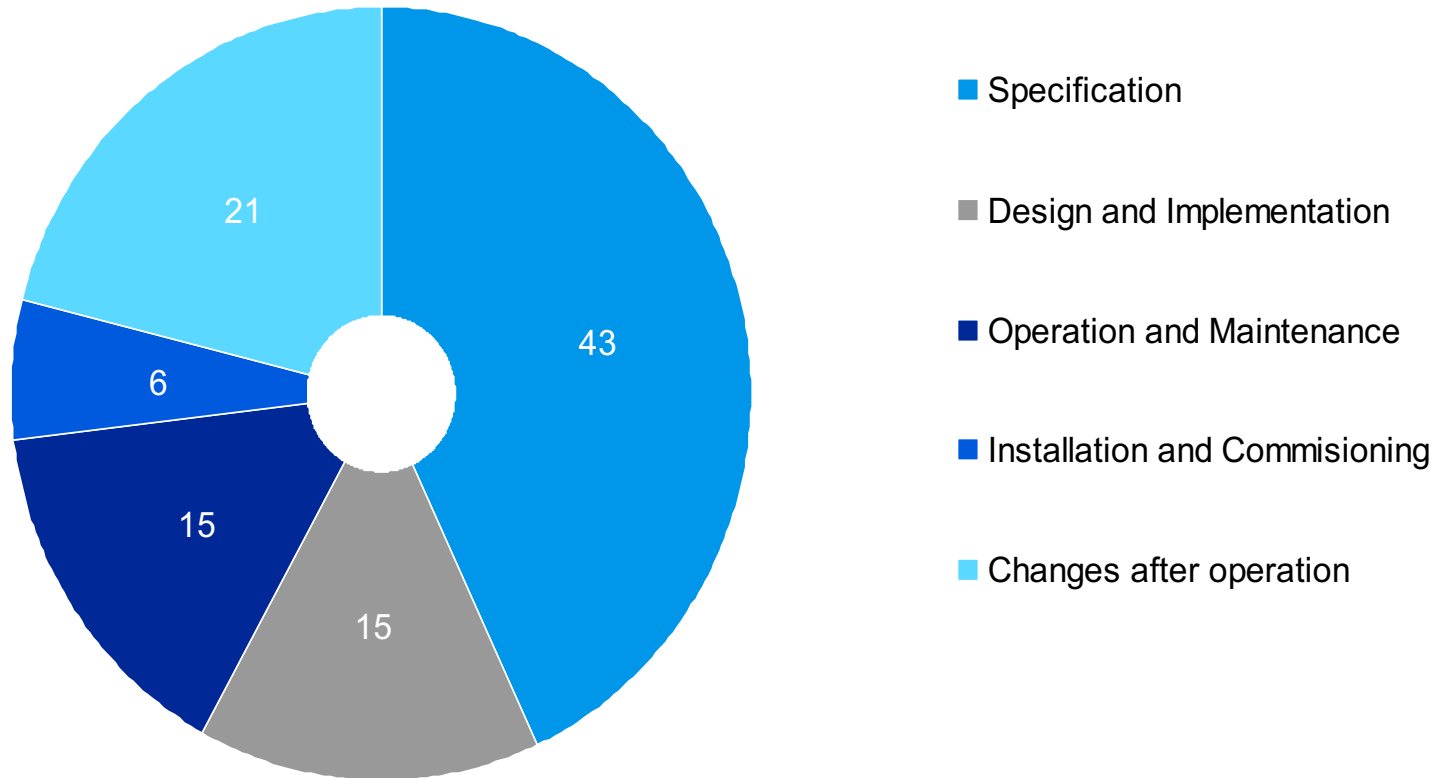
Automation can't check for human intervention

- Industrial plants are designed with the highest accuracy in mind, with several separate safety loops often checking the integrity of process systems.
- Can this apparatus check for human intervention?
- No, they can't!
- A small human error could cause an enormous catastrophe.
- Bear in mind that 70% of reported incidents in the oil and gas industry worldwide are attributable to human error and account for in excess of 90% of the financial loss to the industry.

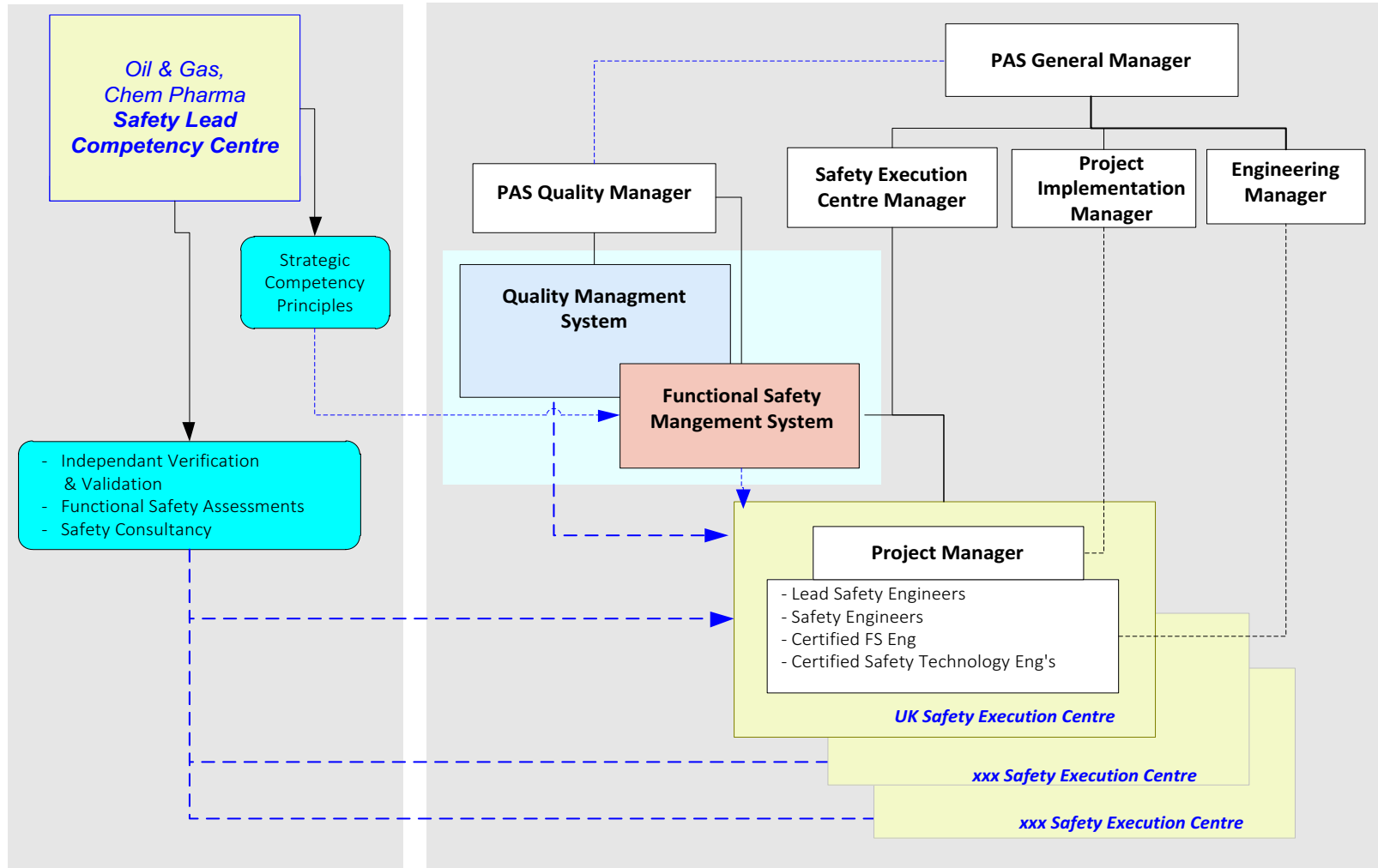


Primary Cause of SIS System Failure

Source: Out of control: Why control systems go wrong and how to prevent failure
HSE Books ISBN 0-7176-2192-8



Functional Safety Management System Organisational Structure



- Those carrying out a functional safety assessment shall be competent for the activities to be undertaken, according to the requirements

Table 4 – Minimum levels of independence of those carrying out functional safety assessment (overall safety lifecycle phases 1 to 8 and 12 to 16 inclusive (see Figure 2))

Minimum level of independence	Consequence (see 8.2.17)			
	A	B	C	D
Independent person	X	X1	Y	Y
Independent department		X2	X1	Y
Independent organization			X2	X

NOTE See 8.2.15, 8.2.16 and 8.2.17 for details on interpreting this table.

Source: IEC 61508 Clause 7.4.7.6

Management of Functional Safety Competency now normative

- Organizations **shall** appoint one or more persons with responsibility for one or more phases.....
- All persons, departments or organizations **shall** be identified, responsibilities clearly defined and communicated
- Activities related to management of functional safety **shall** be applied at the relevant phases
- All persons undertaking specific activities **shall** have the appropriate competence
- The competence **shall** be documented



Source: IEC 61508

- Best in Class companies link safety to their success and invest in programs and systems to reduce their risk
- Engineers have attempted to reduce risk by minimizing the potential for common cause failures
- Common cause failures can occur in products (hardware or software) or the implementation of the application
- The industry have conceived best practices (FSMS) to minimize the impact of human error
- Human factors can't be ignored in the design, particularly in the project design
- Enforcement of these best practices (FSMS) is a way to reduce the risk introduced by engineers... is vital!

Questions & Answers



Power and productivity
for a better world™



Trip Setting Nomination and Process Safety Time

Harvey T. Dearden BSc CEng FIET FInstMC FIMechE AFICChemE
Associate Consultant
HTS Engineering Group Ltd.

Any Safety Requirements Specification (SRS) worthy of the name will identify the trip setting and the process safety time (PST). This latter is defined in the IEC 61508 standard to be the 'period of time between a failure, that has the potential to give rise to a hazardous event, occurring in the EUC or EUC control system and the time by which action has to be completed in the EUC to prevent the hazardous event occurring'. (EUC stands for 'Equipment Under Control'.) This is not quite right however. Consider an example of a cooling water failure; this will lead to a temperature rise, but the initial rise before the trip point is reached does not constitute part of the PST. The PST is the time between the trip setting being reached and the time by which the action must be complete if the hazard is to be avoided. The process safety time is then useful as a component of the SRS in that it identifies the maximum acceptable total execution time of the Safety Instrumented Function (SIF).

Note that if the protection function is a permissive interlock (i.e. preventing an operation), there will not be a process safety time. If the function is for mitigation (e.g. fire detection), rather than prevention, typically the response time will not be an issue. If the function is a trip derived from detection of a binary status condition; drive on/off, valve open/closed, flame/no flame etc., then PST is determined directly by considerations of the process and plant design. If the trip is derived from a continuous process variable however e.g., pressure, temperature, level, then the PST becomes a function of the trip point nominated. The farther from the hazard point the trip setting is, the greater the PST. (Note that this is also true when a switch is used on a continuous process variable – the trip point is implicit in the switch setting or level location.)

Often the trip setting will be nominated as a judgement based on past practice and experience rather than any rigorous evaluation. Typically there will be a handsome level of conservatism in the specification of the true process limit e.g. equipment pressure or temperature rating, and a lack of conservatism in the nomination of a trip setting would not be potentially hazardous. For many applications, conservatism in the specification of a trip setting would not be a critical concern, but for some there may be profound implications for process performance and availability. It may be that the closer the process may approach a constraint the better the process yield or efficiency. This is one reason for improving process control; it may allow a set point closer to the trip setting through reduced process variability. A critical examination of the trip setting nomination may identify opportunities to revise the trip setting itself and allow operation with a reduced margin to the process limit.

The PST will also often also be nominated on the basis of established practice and judgement rather than any formal evaluation, but although it may not be recognised, implicit in a specification of PST for a continuous variable trip is the approach speed of the variable to the true constraint, since:

$$PST = (PV \text{ at Latest Acceptable Completion Time} - \text{Trip Setting}) \\ \div \text{Variable Approach Speed}$$

The actual trip point may differ from the trip setting because of uncertainty in the measurement comparison between the trip setting and the process variable:

$$\text{Actual Trip Point} = \text{Trip Setting} + \text{Trip Point Error}$$

The influence of trip point error is often so small that it may be disregarded, but this cannot always be assumed to be the case.

Explicit identification of the speed of approach to the constraint will allow a refined trip setting specification to be determined on the basis of the protection speed of response. Progressive throttling during shut-off, for example, may well mean that the approach speed will reduce once the protection is invoked, but typically a worst case linear approach speed would be used to estimate the trip margin. A full analysis of approach trajectory would have to include inertial effects and process dynamics and this degree of rigour would only be employed in exceptional circumstances.

A rule of thumb that is often adopted is to aim by design for the SIF response time (SRT) to be no more than half the PST. This is not an inviolable rule however; design considerations might mean that something longer than half is appropriate. Slavish adherence might well lead to the specification of larger actuators for instance, with unwarranted consequences for size, weight and expense. A discussion with the process engineer might well reveal that the declared PST is 'negotiable'. Even if the original PST is confirmed, a response time greater than half may be perfectly acceptable as long as there is confidence that the overall trip execution time will not grow to exceed the PST.

The appropriate trip setting for a process variable will be identified with a margin to the process limit and may be influenced by a number of considerations:

- The post trip increment in the process variable due to process lag e.g., fill line drain down inventory adding to a level, or temperature continuing to rise due to multiple order temperature lags.
- Uncertainty in the process variable measurement and the trip point
- Uncertainty in the specification of the process limit (e.g. bursting disc rupture)
- The amplitude of the process noise i.e. of the uncontrolled higher frequency fluctuations in the process variable; a trip point must be at least half this amplitude away from the hazard point.

The characteristics bearing on trip settings are illustrated in figure 1:

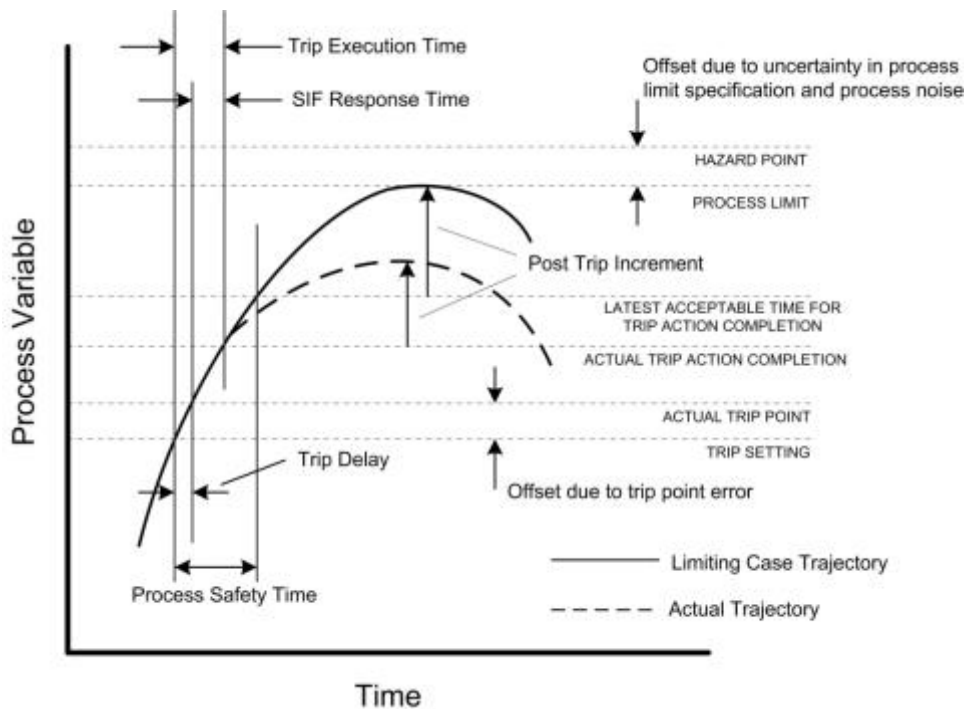


Figure 1; Trip Setting Characteristics

There is potentially some confusion over what constitutes the Hazard Point. As an example, if we consider loss of containment due to overpressure and rupture of the pressure envelope as the ultimate hazard, we will likely include mechanical relief as an independent layer of protection in our SIL determination analysis. The hazard point is then the potential rupture pressure and the true process safety time is the time to this rupture pressure; essentially we would be designing the SIF as a protection layer to cater for the possibility of mechanical relief failure. Note however that in designing a SIF to support this it is possible that the pressure excursion post trip could still trigger the mechanical relief even though this was not necessary to suppress the hazard. If avoidance of mechanical relief was a critical operational concern a new constraint on trip execution time would arise. If the hazard point was identified as the relief setting we would identify a shorter process 'safety' time; this would be conservative but might give rise to unwarranted difficulty in the SIF design. A critical review of the hazard specification and design options would be indicated.

The uncertainty in a trip point will be a function of the capability of the equipment; it will be determined by the accuracy and drift of the sensor system and the trip amplifier and the associated calibration interval. Typically the uncertainty of the trip amplifier will be so low relative to the process measurement uncertainty that it may be disregarded. The uncertainty may cause a trip to be delayed or advanced relative to the nominal trip setting. If the actual trip is closer to the constraint than the nominal setting, the trip will be delayed by a time corresponding with the trip point error and the speed of the process.

$$\text{Potential Trip Delay} = \text{Trip Point Tolerance} \div \text{Variable Approach Speed}$$

$$\text{Guaranteed Trip Execution Time} = \text{Potential Trip Delay} + \text{SIF Response Time}$$

The trip point tolerance (i.e. potential trip point error) may be established from a published safety specification identifying the appropriate tolerance, or it may be calculated from equipment performance specifications. This is not necessarily a straightforward matter however, a rigorous calculation must combine accuracy and drift specifications of the system components together with the calibration interval, and include installation effects and pertinent influence quantities such as equipment operating temperature and process operating conditions; this is beyond the scope of the present article. Note that some safety specification tolerances might well be an order magnitude greater than those simply identified by the more usual performance (accuracy) specifications. The performance and calibration of instrumentation systems is often identified using a 95% confidence level corresponding with two standard deviations of a normal distribution. This implies a 1 in 40 chance of a dangerous out of tolerance value from this consideration alone. This is not consistent with SIL performance requirements. It is here suggested that a tolerance established from published specifications (and incorporating drift, installation effects and influence quantities) should therefore typically be expanded by at least a factor two. (Giving a tolerance at approximately 99.994% confidence)

The ultimate requirement is that the SIF response time should not exceed the PST minus the potential delay due to trip point error.

$$\text{Maximum Allowable SIF Response Time} = \text{PST} - \text{Potential Delay}$$

A more refined rule-of-thumb as a design target would be to say that that the SIF response time should be no more than 50% of the maximum allowable.

Without this refinement it is conceivable that a design could appear to be satisfactory with an SRT of less than 50% of the PST, but potentially unsafe in that the trip point tolerance could mean an additional potential delay of more than the remaining PST. The 50% design rule makes allowance for increased SIF response times in the installed system. There is nothing substantiating the 50% figure however, it represents a judgement of what is a prudent allowance. If the design is found to breach the above rule-of-thumb (or is otherwise considered to be possibly insufficiently robust in terms of the timings), the options are:

- Engineer a reduced SIF response time
- Engineer a reduced trip point tolerance
- Consider whether the values for the process limit and/or approach speed may be revised
- Change the trip setting to increase the margin from the process limit
- Use more rigour in the analysis to demonstrate that the **guaranteed** trip execution time (i.e. that for which the declared failure rate used in the probability of failure on demand calculation is valid) is less than the PST.

Conclusion

The widely employed rule-of-thumb that SIF response time should be less than 50% of process safety time is potentially deficient in that it does not take account of a number of subtleties in the characteristics of trips relating to continuous process variables; in particular the uncertainty in trip

points. A more discriminating rule-of-thumb is to stipulate that the SIF response time should be less than 50% of the value that would otherwise cause the SIF execution time to match the PST. Breaches of this rule are not necessarily hazardous however and a more rigorous analysis of the system provisions may well demonstrate that values in excess of 50% are perfectly acceptable.

Minimising Systematic Failures in Safety Instrumented System Design - Achieving Higher Integrity

Cenbee CY Bullock

BEng(Hons), CFSE, CEng, MIMechE, MInstMC

PFS Consulting Ltd

Cenbee.bullock@pfsconsulting.co.uk

Phone: +44(0)7733 628 050

Copyright © 2014 reserved by Cenbee Bullock PFS Consulting Ltd

Prepared for Presentation at the
Institute of Measurement and Control
Functional Safety 2014

4th – 5th November 2014
London, UK

Minimising Systematic Failures in Safety Instrumented System Design

- Achieving Higher Integrity

Cenbee CY Bullock

BEng(Hons), CFSE, CEng, MIMechE, MInstMC

PFS Consulting Ltd

Cenbee.bullock@pfsconsulting.co.uk

Phone: +44(0)7733 628 050

Keywords: Systematic Failures and Human Errors

Abstract

“With most Safety Instrumented Systems now relying on software to achieve high integrity protection, how can the probability of dangerous or unexpected failures be minimised?

How does Human Error affect the integrity of Safety Instrumented Systems within different phases of the Safety Lifecycle activities? How do IEC61508/ IEC16511 apply to the challenges of eliminating Systematic Failures? How can we apply the IEC61508/IEC61511 Safety Lifecycle to minimise Systematic Failures within the design, engineering, installation and testing?”

This paper describes how to minimise systematic failures in Safety Instrumented System design by following the guidance from the International Standards Safety Lifecycle. It includes the different requirements for verifying electromechanical and programmable electronic systems. It also describes some typical examples of over estimation of human reliability during design, engineering, installation and test phases. These result in mistakes in engineering, additional design time and may have led to some of the unexpected incidents that have occurred in the past few decades.

This paper will touch on some of the Safety Lifecycle activities with emphasis on identifying typical human errors in the design and engineering process (including both type A and type B system architecture), and installation and testing. With reference to Human Reliability Analysis from various research resources, recommendations are made to reduce the incidence of Human Error and thus increase the integrity of Safety Instrumented Systems.

Introduction

In the past there has been a preconception that mainly programmable electronic systems will have systematic failures due to the complexity of the programming system and the unpredictability of software crashes. Investigation reports over the past few decades have shown that the causes of some of the major accidents were related to some kind of systematic failures and over 80% of these accidents are attributable in some degree to human failures, covering both Electro-Mechanical and Programmable Electronic systems.

This paper looks at why human errors occur and the means of minimising the systematic failures caused by human errors.

Failure

Failure is defined as the action or state of not functioning; the neglect or omission of the expected or required action. Failure occurs when a device (or system) does not perform its intended function.

There are two types of failures:-

- a) Physical failures, also known as random hardware failures
- b) Functional failures, also known as systematic failures

Random Hardware Failures

Random hardware failure is the failure of a component, device or system that occurs at a random time. Random hardware failures are normally well defined and well understood; they can be predicted and quantified in terms of probability with reasonable accuracy.

The causes of failure are normally a result of material depletion, fatigue or ageing.

Most established manufacturers keep records of their product's random hardware failures; otherwise generic failure data from recognisable industrial databases such as NPRD (Nonelectronic Parts Reliability Data), OREDA[®] or Exida can be referenced.

Systematic Failures

Systematic failure is a failure that cannot be predicted easily nor quantified statistically. It may occur while a system is functioning but the system does not perform as intended; or the reason for the failure may have existed throughout the project phases without being obvious to anyone.

The causes of systematic failures can be due to:

- a) Environmental influences such as flooding, earthquake, storm or electrical interference from surrounding high voltage equipment;
- b) Human error, such as design faults, inaccurate specification (either safety requirement specification or design requirement or both), operational errors, ambiguous procedures or instructions;
- c) Other factors, such as software bugs, software induced failures or incorrect data communication (e.g. incorrect sequence, data corruption, data loss).

It is not easy or even impossible to obtain reliability data for systematic failures since the causes of failure are widespread even within a particular industry. Currently there is a limited amount of research failure data available for certain typical failures but these should only be used for reference purposes.

In accordance with IEC61508-2 there are two types of system: Electro-mechanical systems are classified as type A, i.e. they do not consist of any microprocessor or programmable electronic functions (see 7.4.4.1.2 for detail); and Programmable Electronic systems are classified as type B (see clause 7.4.4.1.3 for detail). Both types are subject to Systematic failures, though some types of Systematic failure will only occur with type B systems (Fig. 1).

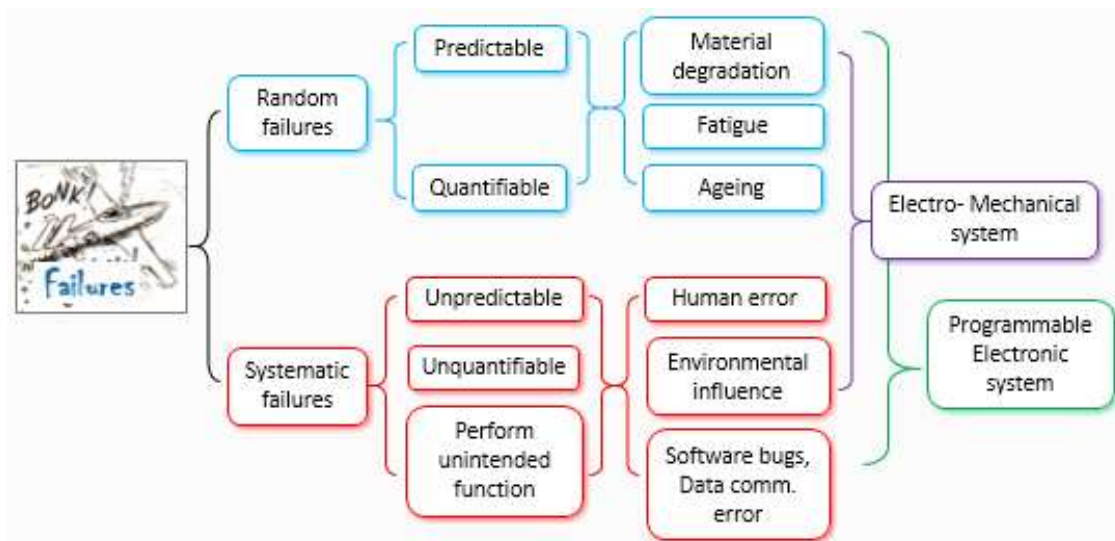


Fig.1 Types of failures

Safety Integrity

Safety Integrity is defined as “The probability of a Safety Instrumented Function satisfactorily performing the required safety functions under all stated conditions within a stated period of time.”

IEC61508 states

“In determining safety integrity, all causes of failure (both random hardware failures and systematic failures) that lead to an unsafe state should be included.”

With reference to a UK HSE study¹ on why control systems go wrong, most incidents happen because of errors in than one phase of the safety lifecycle (analysis, realisation and operation). The analysis also shows that the majority of the incidents were not caused by any failures of a device or control system but resulted from systematic failures. Fig. 2 shows the percentage of primary causes attributable to each phase of the lifecycle. The survey also shows that more than 80% of the failure causes are attributable, in some degree, to human errors.

¹ UK Health and Safety Executive, “Out of Control”, 2003

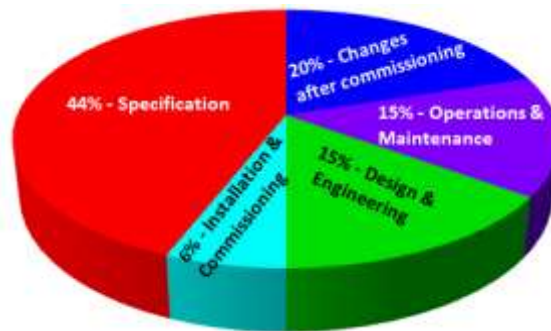


Fig. 2 Percentage of primary causes attributable to each phase of lifecycle (by UK HSE)

Why human errors?

Professor Reason², in a paper on clinical mistakes, states

“Human error problems can be viewed in two ways: the person approach and the system approach..... Each has its model of error causation and each model gives rise to quite different philosophies of error management. Understanding these differences has important practical implications for coping with the ever present risk of mishaps in Clinical practice.”

This concept is also applicable to other fields, not just clinical, and in order to minimise the systematic failures caused by human errors, it is essential to understand how a human’s mind works. A proverb from Sun Tzu³ says: “If you know the enemy and know yourself, you will not be imperilled in a hundred battles.”

Plato⁴ developed a cave allegory that describes three synopsis of the human mind:

- i. Imprisonment in the Cave
Perception – a human’s mind does not always see reality correctly;
- ii. Departure from the Cave
Adaptation – a human’s mind needs time to absorb new information or changes;
- iii. Return to the Cave
Ignorance – a human’s mind has a tendency to omit detail.

² Professor J Reason, “Human error: model and management” 18 March 2000

³ Sun Tzu, “Art of War” 6th Century BC

⁴ Plato, “Allegory of the Cave”

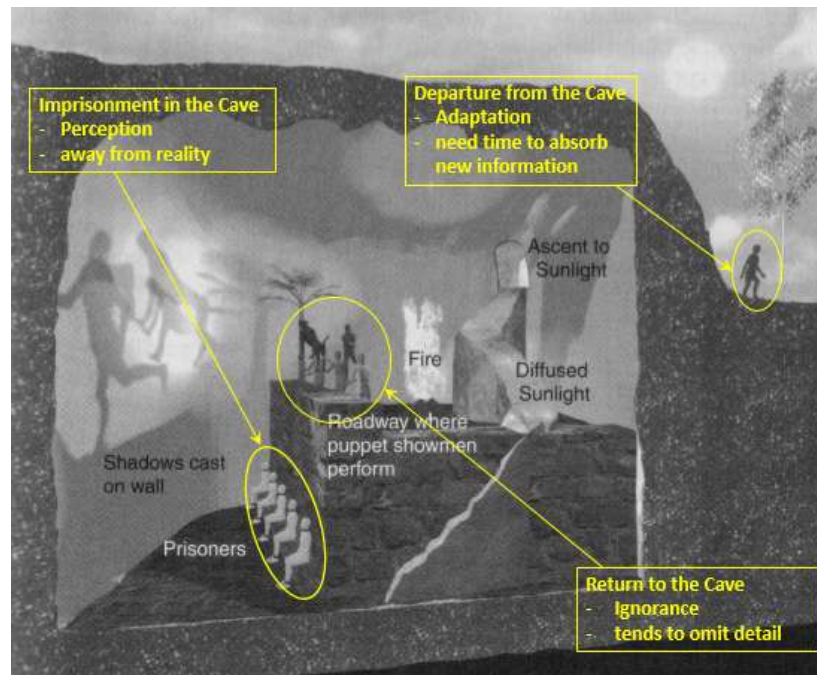


Fig. 3 Plato's Allegory of the Cave

A human's brain has a tendency to strive to process information quickly without rationally understanding it; consequently it omits detail which results in mistakes and errors.

The following is an example that shows that a human's brain is capable of accurately constructing words without the words being written correctly. Below is a paragraph written by G.E. Rawlinson⁵ that most people have the capability of reading accurately despite the letters being jumbled up,

"Aoccdrnig to rscheearch at Cambridge Uinervtisy, it deosn't matter in what order the letters in a word are, the only iprmoetnt thing is that the first and Isat ltteer be at the rghit pclae. The rset can be a toatl mses and you can sitll raed it wouthit porbelm. Tihs is bcuseae the huamn mnid deos not raed ervey lteter by istlef, but the wrod as a wlohe."

The above shows that human brain has the capability to interpret how it wants to read rather than reading it literally, i.e. it assumes corrections to the passage which may or may not align with what the author intended; this demonstrates all three synopsis of Plato's cave.

When may systematic failures be introduced?

ISA-TR84.00.02-2002 Part 2 states "Systematic failures may be introduced during the specification, design, implementation, operational and modification phase and affect hardware as well as software," i.e. at any stage in the safety lifecycle

The ISA standard shows the inclusion of both random hardware failures and systematic failures in SIL verification calculations for the average probability of dangerous failures on demand (PFDavg). It

⁵ G.E. Rawlinson, "The significance of letter position in word recognition" 1976

identifies the probability of dangerous systematic failures on demand (PFD_{sys}) of a process plant and the probability (P) of systematic failures caused by human errors including faults in design, installation, proof tests and in by-pass mode.

$$PFD_{avg} = \Sigma PFD_{sensor} + \Sigma PFD_{logic\ solver} + \Sigma PFD_{final\ element} + \Sigma PFD_{power\ supply} + \Sigma PFD_{systematic\ failures}$$

Where $PFD_{systematic\ failure} = PFD_{sys-process\ plant} + P_{sys-human\ error}$

And $P_{sys-human\ error} = P_{design\ error} + P_{installation} + P_{proof\ test\ error} + P_{bypassed}$

Unfortunately, it is not easy to model systematic failures accurately and they are rarely included in the SIL verification modelling. It is due to the difficulties in obtaining the failure rates and in most instances, systematic failures can be very specific to a particular operation and process plant.

In the 2nd edition of IEC61508, there are techniques and measures to control systematic failures under various stress conditions. Part 2 table A.15 to A.17 recommends some techniques and measures to demonstrate the systematic capability.

How to minimise systematic failures caused by human error?

Human error is one of main causes of systematic failures. If we refer to some of the research and studies, human mistakes and errors can occur throughout all the phases of the safety lifecycle.

The Swiss Cheese Model can be used to represent the safety lifecycle activities, with the holes representing human errors in the various phases (slices) of the activities. (Design, development and verification of Programmable Electronic Systems will be discussed in more detail in a later section). Some of the errors and mistakes may seem to be insignificant: for example, assuming competently trained duty operators would be available to cover all operating hours and are all fully appraised of the actions required when responding to safety critical alarms.; or, designing a safety instrumented function with SIL 2 requirement without understanding the implication of no segregation or independence between the basic process control system and the SIL rated system; or, through ignorance of environmental influences, installing sensitive electronic devices next to high voltage equipment. Unless these seemingly insignificant assumptions are addressed, and resolution is overseen and supported by the management team, these assumptions could lead to a major failure.

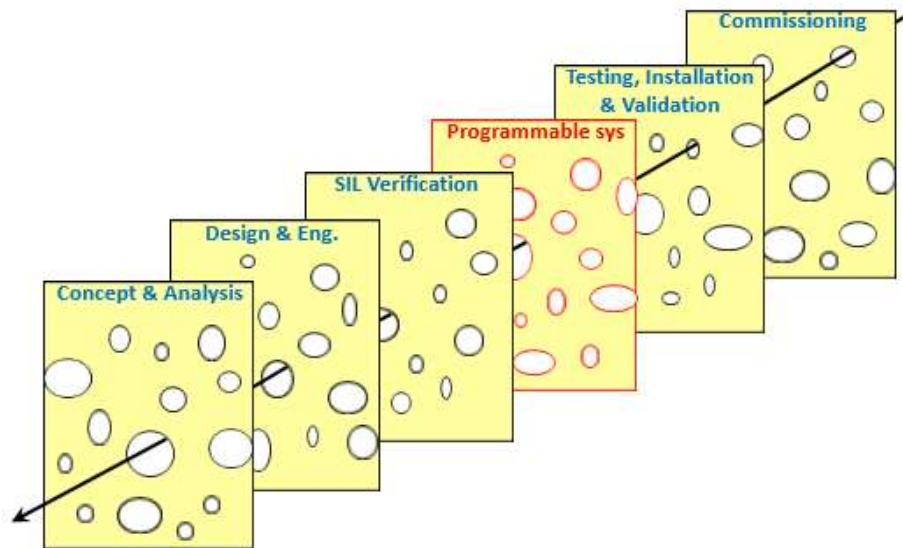


Fig. 4 – Swiss cheese model of the Safety Lifecycle

The illustration also tries to correct the general misconception that the majority of human errors lie in the later stage of the lifecycle activities: for example, restoring operations without resetting the bypass valve; a block valve associated with a relief valve is left closed after maintenance; or leaving a transmitter root valve closed.

With reference to some of the major accidents in the past few decades, human errors were found in various phases of the safety lifecycle. With reference to the UK HSE survey (see Fig. 2), 44% of the incidents were attributed to inadequate specification of the Safety Instrumented System. These could be caused by incorrect assumptions during the SIL determination workshop leading to an inaccurate safety requirement specification and an incorrect design requirement specification. For example, over claiming the risk reduction credit on an alarm system during the SIL determination workshop. When the wrong requirement is set out in the beginning, the activities that follow are almost certain to be incorrect. It often happens that such a mistake may only be discovered when site integration tests are carried out; or, for example, in the Buncefield oil storage depot fire, the system testing was not carried out prior to putting the system online with a consequence of major damage. This is similar to the domino effect - the system is so vulnerable that when the first domino falls down, the rest of the dominos will follow on and eventually the whole construction collapses.



Resolution – Applying a systematic approach

Whatever industry, whether it is a fully-automated or is operated by humans, there is always some degree of human involvement and it is unlikely that all possible systematic human failures can be avoided throughout the project lifecycle. A number of studies by various researchers have investigated how to minimise systematic human failures.

Professor J. Reason² states

“Human error problems can be viewed in two ways: the person approach and the system approach.

The person approach focuses on the errors of individuals, blaming them for forgetfulness, inattention, or moral weakness.

The system approach concentrates on the conditions under which individuals work and tries to build defences to avert errors or mitigate their effects.”

Recognising human weakness, with a constructive attitude, and applying a systematic approach to provide barriers to minimise systematic human failures is important for any successful operation.

Dr Nils Löber⁶ states

“Without constructive error attitude, safety instruments will never unfold their full protective potential.”

Fig. 4 shows the Swiss cheese model of human errors and mistakes through different phases of the lifecycle. Defences and barriers to minimise the possible systematic human failures throughout the safety lifecycle phases can be effected by applying a systematic approach and using the Safety Management Plan (or Management of Functional Safety).

The Safety Management Plan is a live document that needs to be updated accordingly for each of the different phases of the project. It is an overarching document and includes the safety lifecycle. It acts as road map to provide the direction for the project in managing safety-related activities; ensuring all safety-related activities are being executed strategically and systematically.

The structured review process and well-defined documentation system should be used as the defence and barriers to minimise any possible systematic human failures (as illustrated in the Swiss cheese model). These activities should be supported and monitored by a suitably qualified and experienced management team.

The components within the Safety Management Plan should consist of all the requirements as stated in IEC61508-1 clause 6 including:

- i. Roles and responsibilities in each phase of the safety lifecycle activities and the approved authority;
- ii. Design review procedures through the different phases of the lifecycle;
- iii. Structured document review scheme and approval procedures (i.e. revised, reviewed and approved – all should be clearly identified with current revision and date of completion).
- iv. Independent technical review and assessment; carried out by an independent subject matter professional and preferably with access to the project information but not part of the design and engineering team.

Fig. 5 shows an illustration of the safety lifecycle with the inclusion of a management procedural system including:

- i. Safety Management Plan
- ii. Human Factor Integration Plan
- iii. Management of Change Procedure

⁶ Dr. Nils Löber, “Coping with (human) errors in organizational and industrial settings” 05.11.2012

The IEC61508 safety lifecycle is the most systematic approach for any safety-related system. The requirements of each phase as stated in IEC61508 should be met to demonstrate the systematic capability of the design. The Human Factor Integration Plan is not a mandatory requirement within IEC61508, however, it would be beneficial to include such a document to raise awareness of the human factor issues at the beginning of the project lifecycle to avoid any over-estimation of human reliability. The Management of Change Procedure is an essential document for all phases of the project lifecycle. Any changes and modifications from the conceptual design to commissioning/decommissioning should be structurally managed and maintained with full traceability. All safety-related documents should be made available to all project members and operational personnel. They should be uniquely identified.

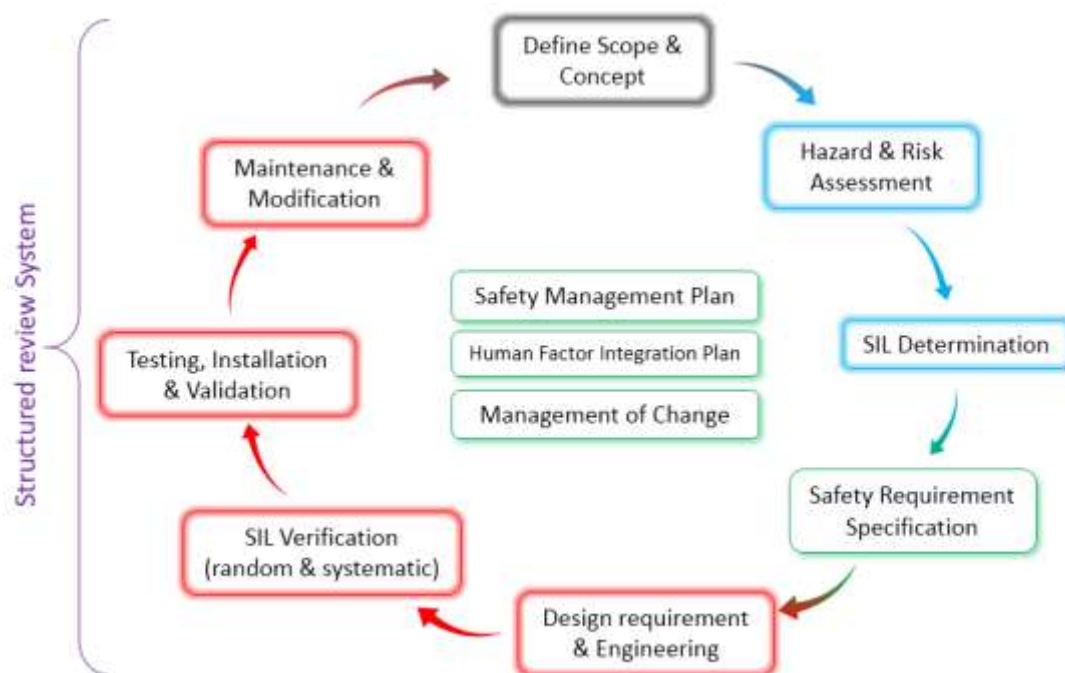


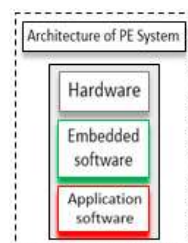
Fig. 5 – Safety Lifecycle Activities

Safety Lifecycle Systematic Approach Example

The following is an example of the systematic approach applied to the design, development and verification process of a Programmable Electronic (PE) system.

A Programmable Electronic system consists of three parts:

- i. Hardware – the physical part of the system;
- ii. Embedded Software – the operating system for the application software;
- iii. Application Software – the software written specifically for the project application.



The random hardware integrity for the Hardware and the systematic capability for the Embedded Software should be verified independently by a third party. They will not be discussed further in this paper.

The systematic capability for Application software should be designed, developed and verified against the software safety lifecycle; i.e. the V-model in IEC61508-3 (see Fig 6). The requirements are different according to the flexibility and complexity of the written language.

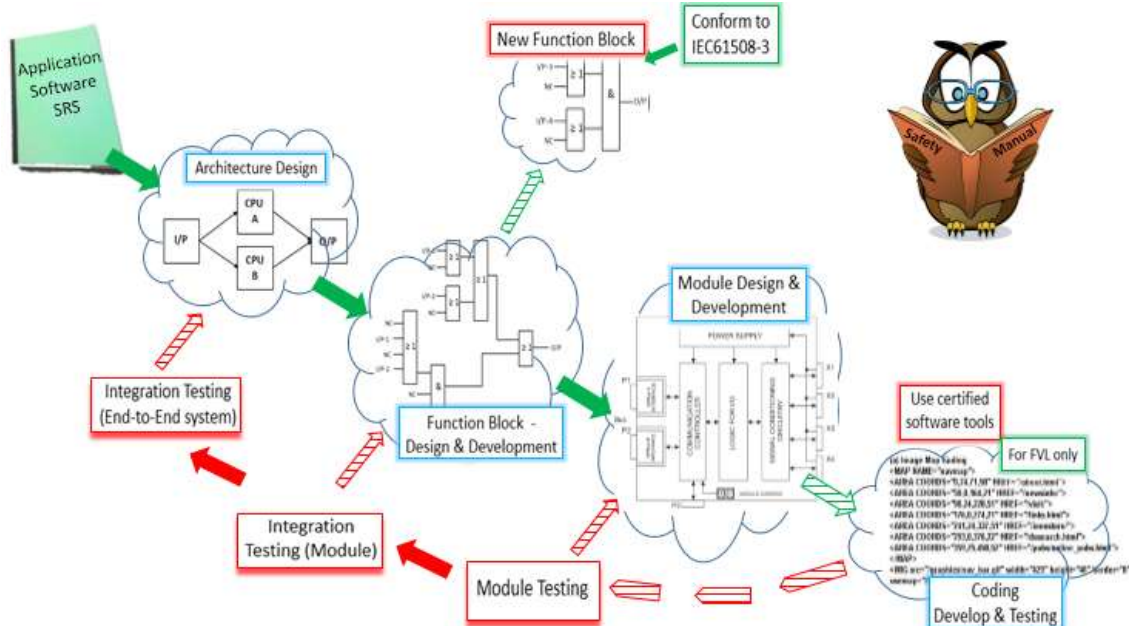


Fig. 6 Illustration of V-Model for Programmable Electronic System

Application Software consists of three different language types:

- i. Fixed programmable language (FPL) – no alteration is available in this programmable language; changes are restricted to parameters of set point and alarm only; the software for the majority of off-the-shelf smart transmitters is written in this type of language. The software is normally verified and certified by the manufacturer's engaged party; there is no mandatory requirement to comply with the V-model.
- ii. Limited Variability Language (LVL) – this programmable language normally consists of pre-defined application library functions that have been verified by a third party certifying body or a subject qualified specialist. Limited changes may be available to specific functions only, provided the supplier's safety manual is followed (any additional functions should be verified against IEC61508-3 to demonstrate the systematic capability). Software such as ladder logic and function blocks are written in this language.
- iii. Full Variability Language (FVL) – this programmable language is more complex and provides for a wide range of functionality and application. The software is normally written in C, C++, and Pascal etc. The software should be verified using certified (utility) software tools and checked by an independent assessor. All documentation including coding, developing and testing must be traceable.

For LVL and FVL, the design, development and verification of the software should follow the recommended structures and procedures as stated in IEC61508 part 3 in order to demonstrate the systematic capability of the system.

Fig 6 illustrates the steps and procedures for the design, development and verification of the software with reference to IEC61508-3. All steps shown should be followed in order to demonstrate the systematic capability of the software. The Safety Requirement Specification (SRS) for application software should be written for the specific project requirement for the software and be designed and developed accordingly. For example, when joining two certified library function blocks into one specific function, the joining procedure should be written in the application software SRS for the specific project. The testing methodology should be written in the Safety Manual.

The PE System supplier should provide a Safety Manual for the programmable software language with full instructions for installation, testing and modification and also state the systematic capability. Any modification or change to an LVL library function block should be confirmed and verified against IEC61508-3. Any new function block should be written according to the instructions in the safety manual.

For FVL, certified software tools (i.e. utility software) should be used for software verification. It should be reviewed and approved by a suitably qualified independent assessor. All steps and procedures for the design and development or any modification during verification and testing should be recorded with systematic traceability.

A Programmable Electronic system has the highest potential for systematic failures compared to Electro-Mechanical systems. They can be caused by widespread factors: environmental influences, human errors, software bugs and data communication error etc. The V-model provides the most effective techniques and measures to demonstrate the systematic capability. All PE system suppliers are required to provide evidence of their compliance to these procedures.

The above procedures demonstrate the importance of using a systematic approach throughout the safety lifecycle and good control documentation system is vital for the process.

Measures of Human Reliability

ISA TR84.00.02-2002 states that systematic failures caused by human error can take place in any phase: design, installation, proof test and operation in by-pass mode. This can be represented mathematically by:

$$P_{\text{sys-human error}} = P_{\text{design error}} + P_{\text{installation}} + P_{\text{proof test error}} + P_{\text{bypassed}}$$

The US Process Improvement Institute (PII) produced a Standardised Plant Analysis Risk Model (SPAR-H) based on work by the US Nuclear Regulatory Commission (NUREG). The model enabled analysis of human reliability which found various reasons for possible human errors in a given task, including: insufficient time, stress, fitness for duty, complexity of the design, experience, training, competence, communication, procedures, work supervision, work environment and the number of personnel.

Typical examples of some of the human errors during installation and testing are:

- i. Mis-calibration of the instrument such as a level/pressure transmitter;
- ii. Forgetting to re-open and lock the block valves under a relief valve after maintenance and before the relief valve is returned to normal service;
- iii. Leaving the transmitter/sensor root valve closed causing an unsafe failure;
- iv. Leaving the entire safety instrumented function in by-pass mode after maintenance or after some other human intervention (such as an unintended error or as a necessity during start-up)

Statistics from the Process Improvement Institute shows that Probability of Human Error (PHE) varies from 0.1 to 0.001 depending on the industry and the control of human factors. For example:

- i. PHE = 0.01 to 0.04 for a relief valve being returned to normal operation after maintenance due to leaving the block valves in the by-pass position;
- ii. PHE = 0.2 while working 30 days of 12 hour shifts during a refinery shut down (In some countries, there are now restrictions for maximum of 12 days shifts)

Below are some of the recommendations for minimising systematic human failures:

For installation and testing:

- i. Include a test override switch as part of the safety instrumented function;
- ii. Include position switch/indicators on the by-pass block valves;
- iii. Consider the use of an alarm to indicate an active by-pass;
- iv. Apply the two man rule for routine tasks and safety critical activities;
- v. Enforce the use of Installation or Testing procedures;
- vi. Where modification takes place, the system should be re-tested to ensure consistency with the requirements;

For Testing Procedures:

- i. Be accurate and complete;
- ii. Be clear and concise with an appropriate level of detail (Too detailed and it may be hard to follow; too little information and it may be difficult to carry out the task correctly);
- iii. Identify any hazards;
- iv. State necessary precautions for hazards;
- v. Reflect how tasks are actually carried out;
- vi. Ensure Procedures are accessible;
- vii. Use consistent terminology;
- viii. Use an appropriate format;
- ix. Use familiar language;
- x. Promote ownership by users;
- xi. Be current and up to date;
- xii. Be supported by training;

Conclusion

There are various reasons for systematic failures; some are inevitable but some may be avoidable. Outcomes from various studies concluded that a large percentage of accidents were contributed to

by systematic human failures. Some of the most recent incidents such as the Buncefield oil storage terminal fire and the Gulf of Mexico oil spill were largely due to systematic human failures.

Although ergonomics is being considered for the location of equipment and the operation of the central control room, it is unusual to integrate human factors in the early stage of a project's safety lifecycle. As concluded from the UK HSE survey, human error occurs throughout all phases of the safety lifecycle and more than 80% of accidents are attributable in some degree to human error.

Understanding human weakness and applying constructive attitudes by using a systematic approach in the early stages of the safety lifecycle could be one of the most effective ways to minimise systematic failures caused by human errors. Last of all, avoid complexity in design and don't over-estimate human reliability.

Minimising Systematic Failures in Safety Instrumented System Design

Cenbee Bullock
Functional Safety Specialist

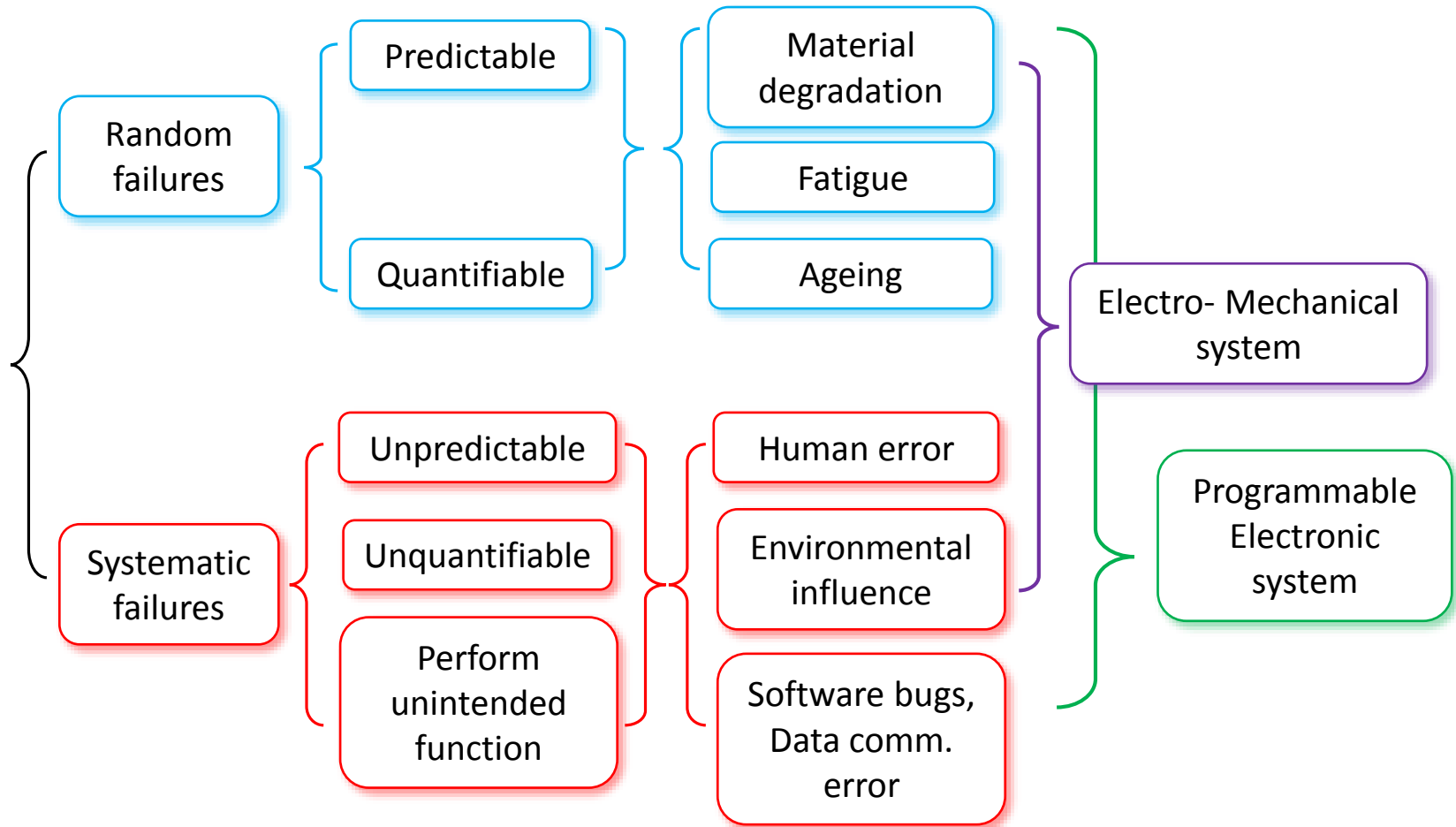
Contents

- Types of Failures
- Safety Integrity
- Why Human Error?
- Human Rationale
- When may Systematic Failures be introduced?
- Swiss Cheese Model (Human Fallibility)
- Safety Lifecycle –Systematic Approach
- Example - Programmable Electronic System
- Software Systematic Capability
- Integrity of Installation and Testing
- Minimising Systematic Failures (Human Errors)
- Summary

Failure



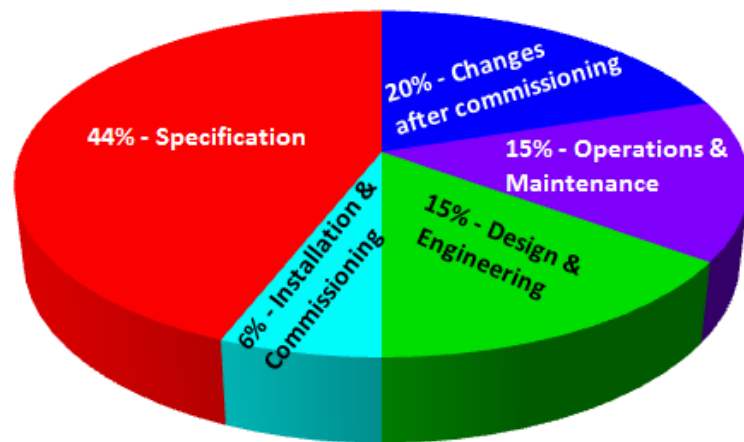
Type of Failures



IEC61508

“In determining safety integrity, all causes of failure (both random hardware failures and systematic failures) that lead to an unsafe state should be included.”

Reference from UK HSE Survey

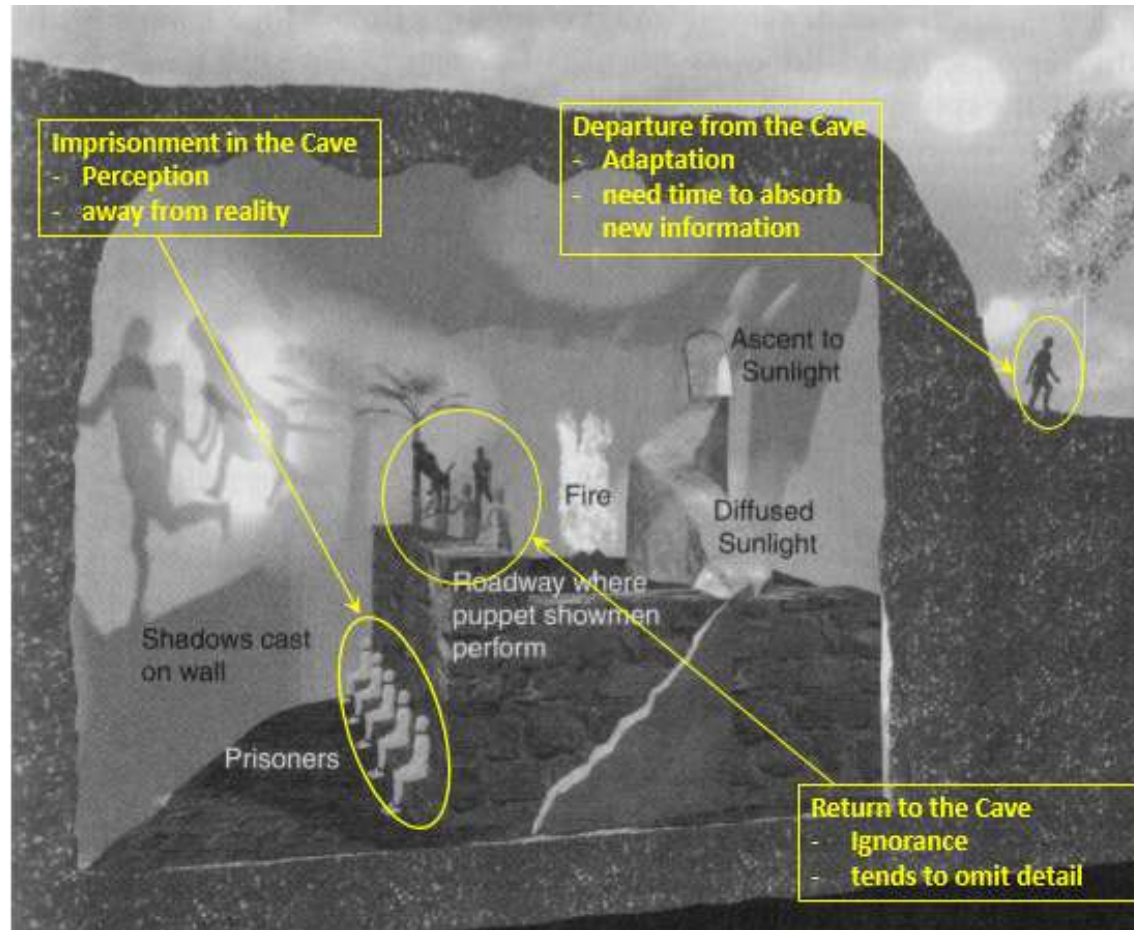


Studies Show



More than 80% of accidents are attributable in some degree to human failures !

Why Human Error? – Allegory of the Cave by Plato



Letter written by G.E. Rawlinson

Aoccdrnig to rscheearch at Cambridge Uinervtisy, it deosn't matter in what order the letters in a word are, the only iprmoetnt thing is that the first and lsat ltteer be at the rghit pclae. The rset can be a toatl mses and you can sitll raed it wouthit porbelm. Tihs is bcuseae the huamn mnid deos not raed ervey lteter by istlef, but the wrod as a wlohe

When may systematic failures be introduced?

ISA-TR84.00.02-2002 Part 2

“Systematic failures may be introduced during the specification, design, implementation, operational and modification phase and affect hardware as well as software.”

Mathematical analysis formulae (TR84.00.02-2):

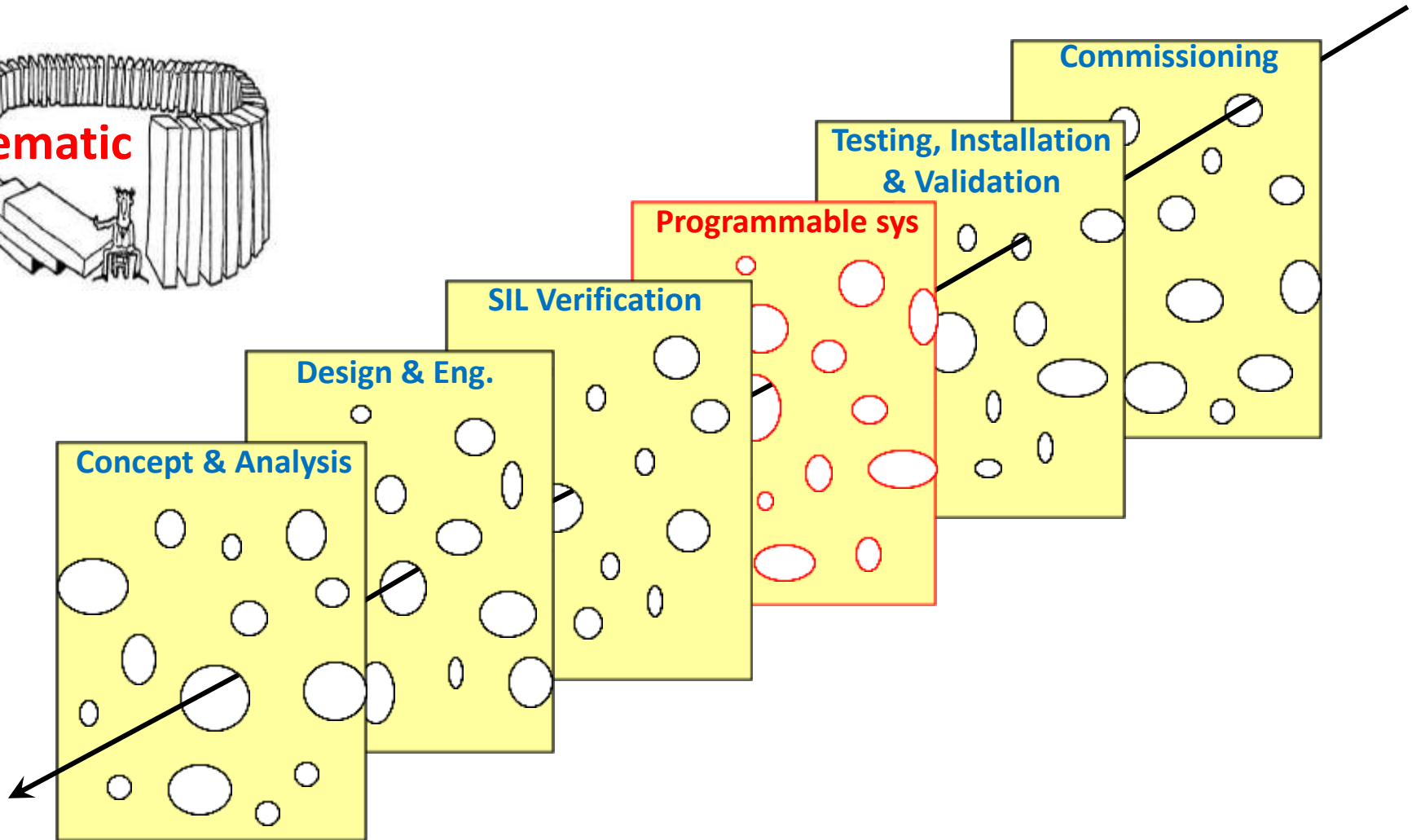
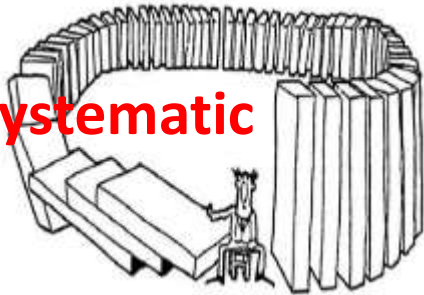
$$PFDSIF = \Sigma PFD_{\text{sensor}} + \Sigma PFD_{\text{logic solver}} + \Sigma PFD_{\text{final element}} + \Sigma PFD_{\text{power supply}} + \Sigma PFD_{\text{systematic failures}}$$

➤ $PFD_{\text{systematic failure}} = PFD_{\text{sys-process plant}} + P_{\text{sys-human error}}$

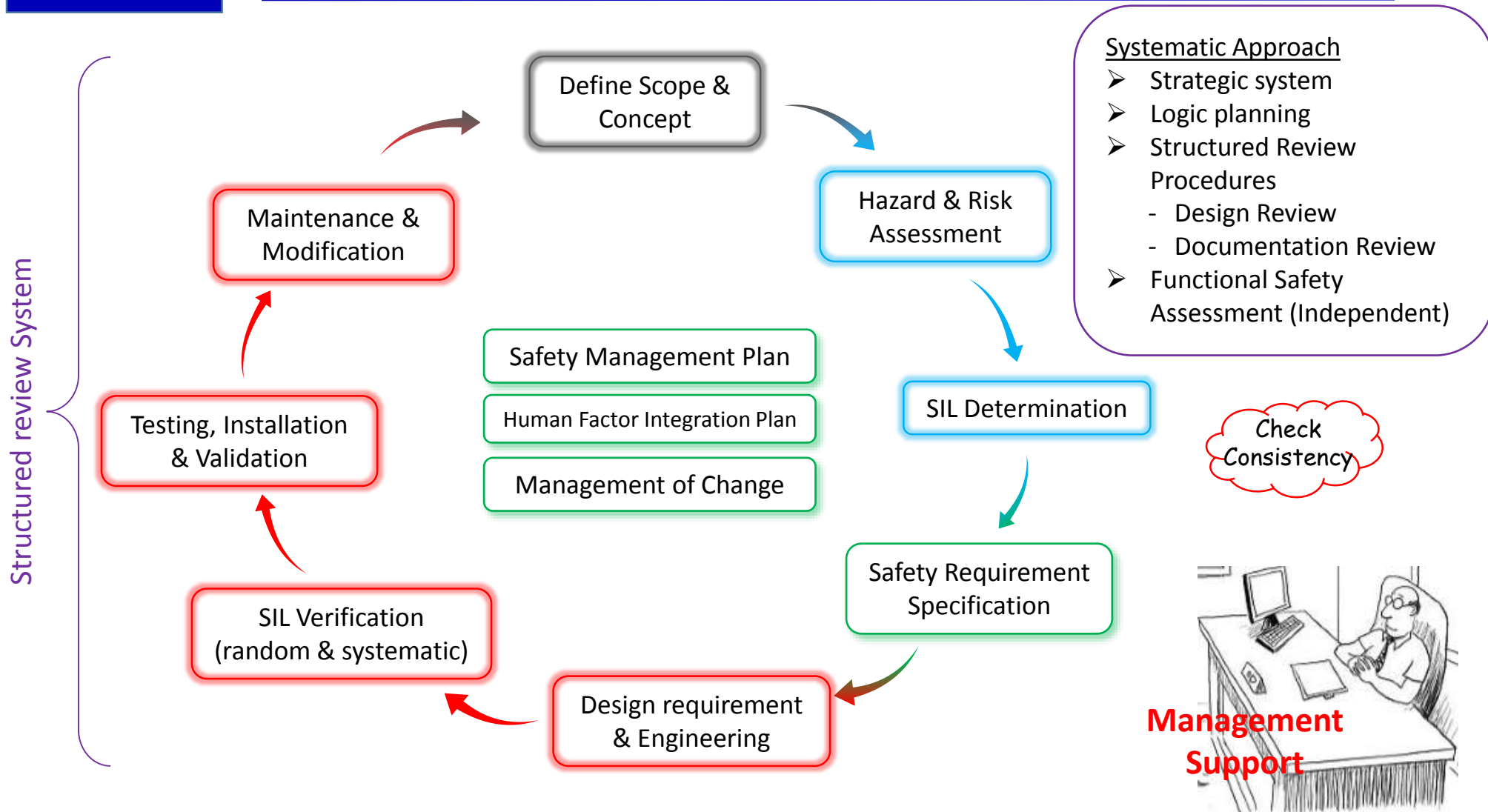
➤ $P_{\text{sys-human error}} = P_{\text{design error}} + P_{\text{installation}} + P_{\text{proof test error}} + P_{\text{bypassed}}$

Swiss Cheese Model (Human Fallibility) – Safety Lifecycle

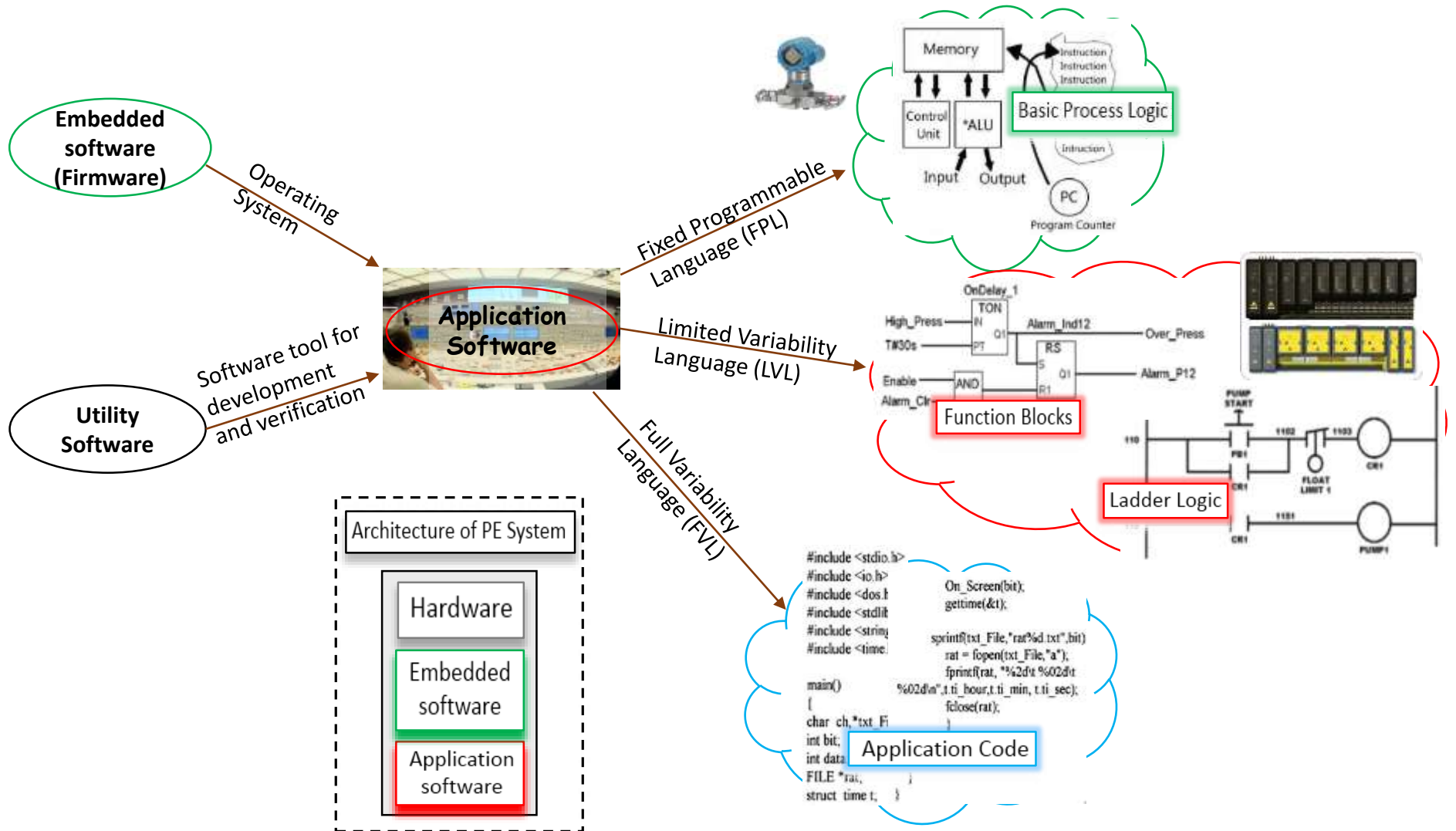
Unsystematic



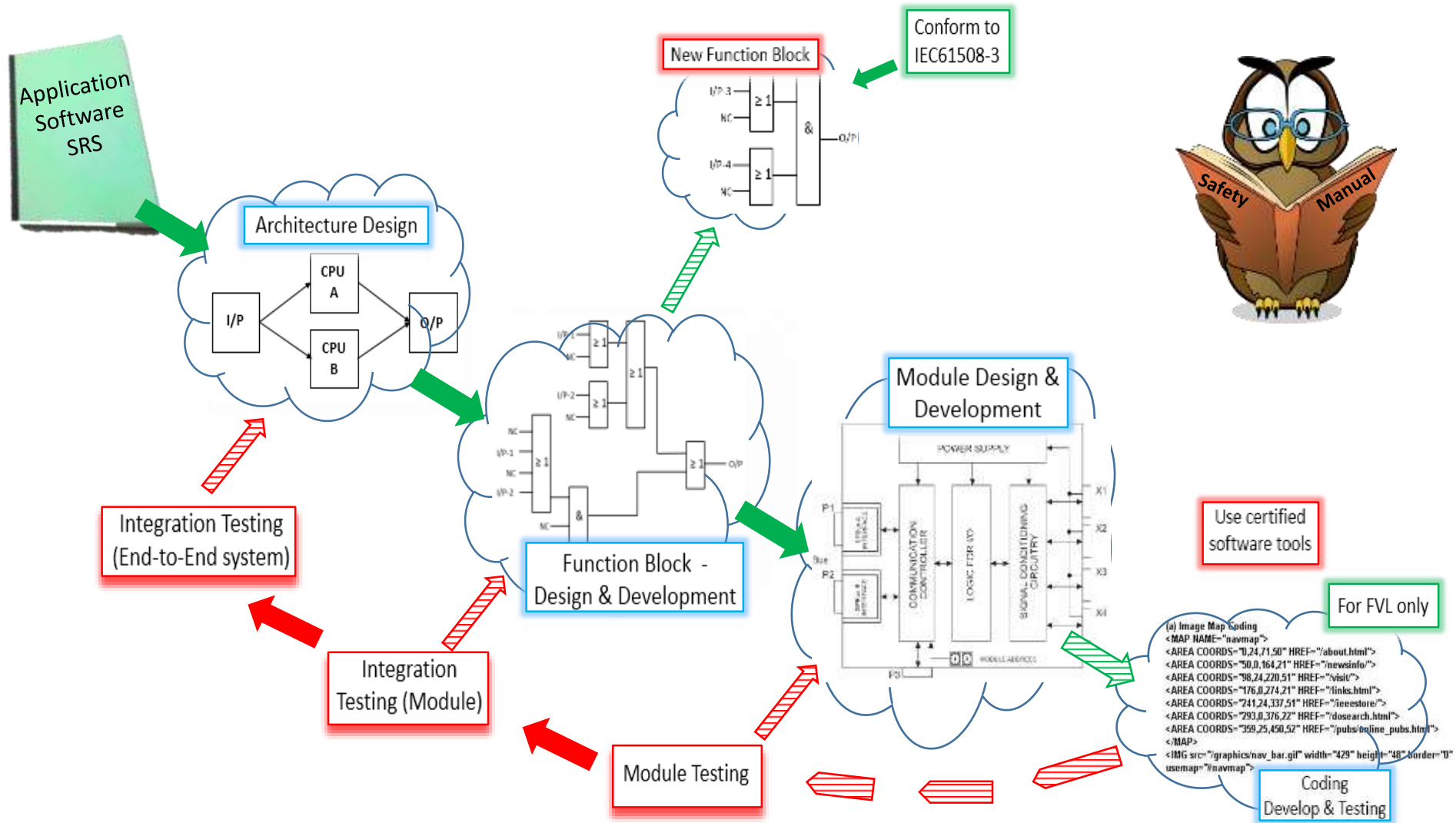
Safety Lifecycle - Systematic Approach



Programmable Electronic System



Software Systematic Capability (V-Model)



Integrity of Installation & Testing

Probability of Systematic Failures due to Human Error

$P_{\text{sys-human error}}$

= $P_{\text{design error}}$ + $P_{\text{installation}}$ + $P_{\text{proof test error}}$ + P_{bypassed}

Human Reliability Analysis

Studies from NUREG & PII in SPAR-H Human Reliability Analysis show that the possible Human Errors in a given task include:

- ❖ Insufficient time
- ❖ Stress
- ❖ Fitness for duty
- ❖ Complexity of the design
- ❖ Experience/ Training
- ❖ Competence
- ❖ Communication
- ❖ Procedures
- ❖ Work supervision
- ❖ Work environment
- ❖ Number of personnel

SPAR – Standardised Plant Analysis Risk Model

NUREG – Nuclear Regulatory Commission, Office of Nuclear
Regulatory Research, Washington DC

PII – Process Improvement Institute, Inc TN 37922

- **Mis-calibration** of the instrument such as level/pressure transmitter
- **Forget to re-open and lock the block valves** under a relief valve after maintenance and before the relief valve is returned to normal service
- **Leaving the transmitter/sensor root valve closed** causing an unsafe failure
- **Leaving the entire SIF in BYPASS** after maintenance or after some other human intervention (such as an unintended error or as necessity during the start-up)

Probability of Human Error (PHE) varies from **0.1 to 0.001** dependent on the industry and the control of Human Factors.

Examples:

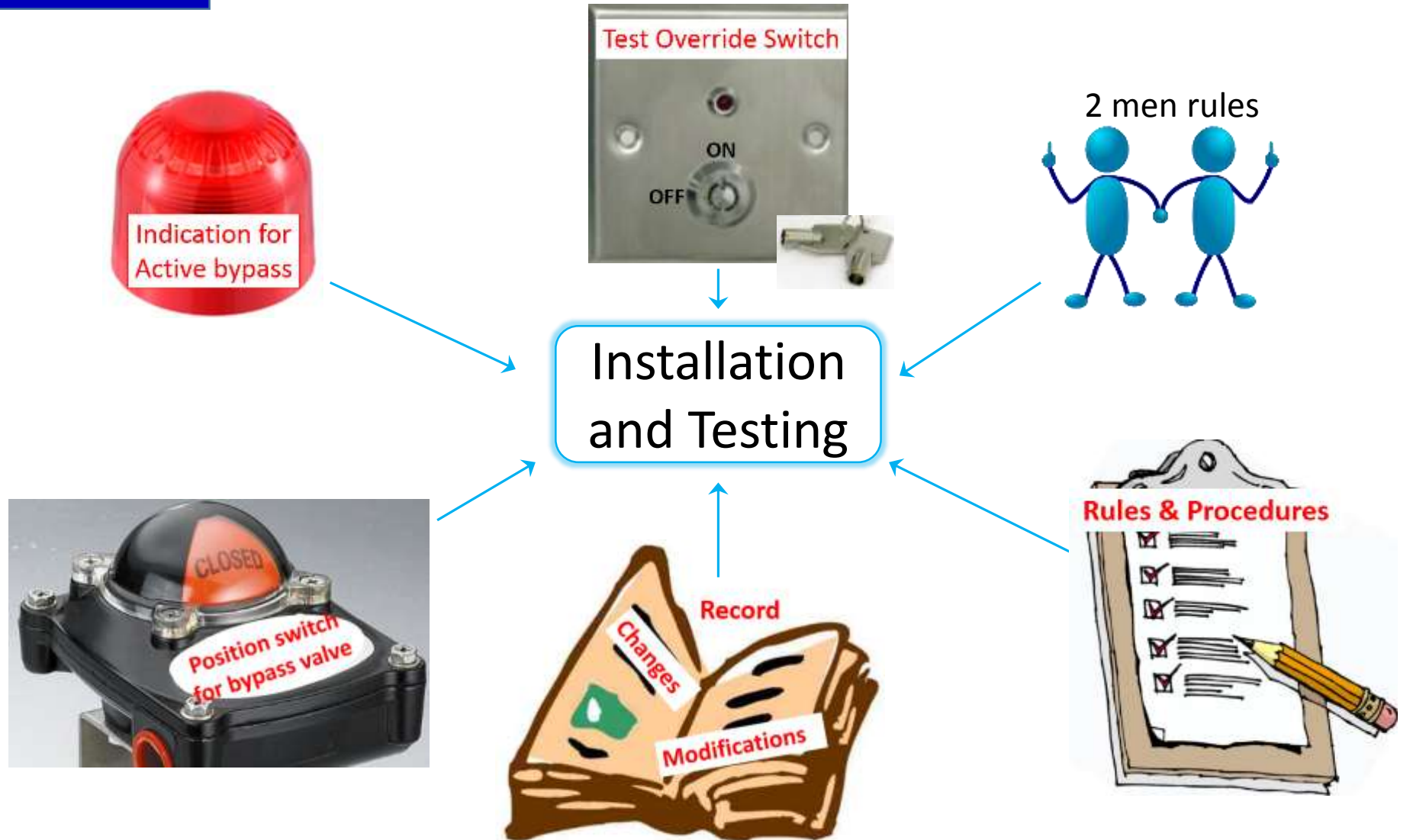
➤ CCPS 2012 – Relief Valve (PRV)

PHE = **0.01 to 0.04** for a Relief Valve being returned to normal operation after maintenance due to leaving the block valves in the bypass position

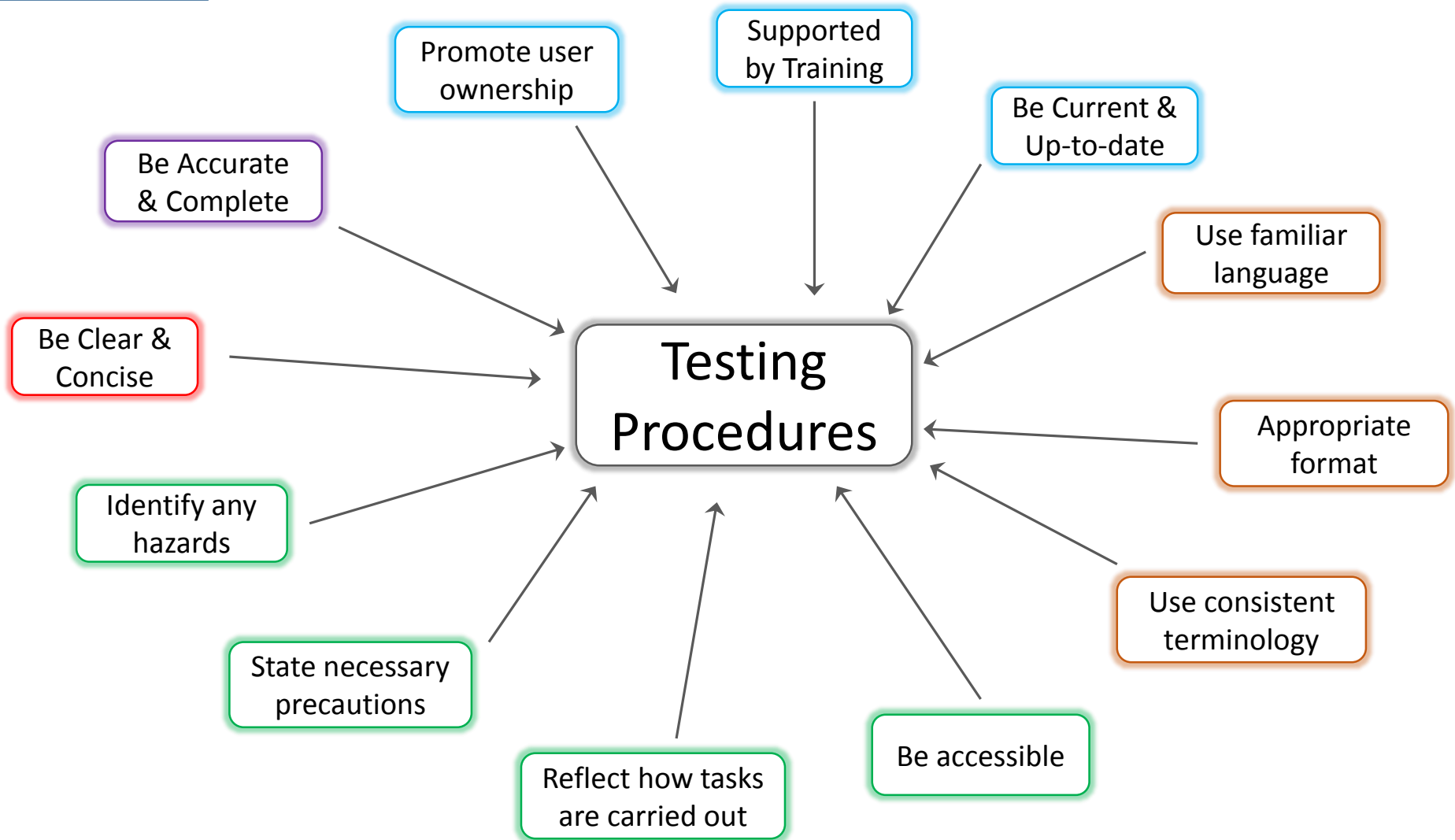
➤ Refinery Shutdown

PHE = **0.2** for Straight 30 working days of 12 hour shift

Minimising Systematic Failures (Human Factors)



Minimising Systematic Failures (Human Factor)



Summary

- Use a systematic approach and apply to safety lifecycle activities
- Integrate Human Factors in the beginning of the safety lifecycle
- Apply a structured review system; design review, independent review
- Use effective document control scheme
- Avoid complexity
- Maintain traceability for all safety lifecycle activities including all changes
- Clear procedures for installation, proof test and maintenance
- Supported by Management

- **Don't** over-estimate human reliability
- **Don't** assume
- **Don't** under-estimate the task

Any queries or for further information, please contact:

Cenbee Bullock

Functional Safety Specialist

PFS Consulting Ltd

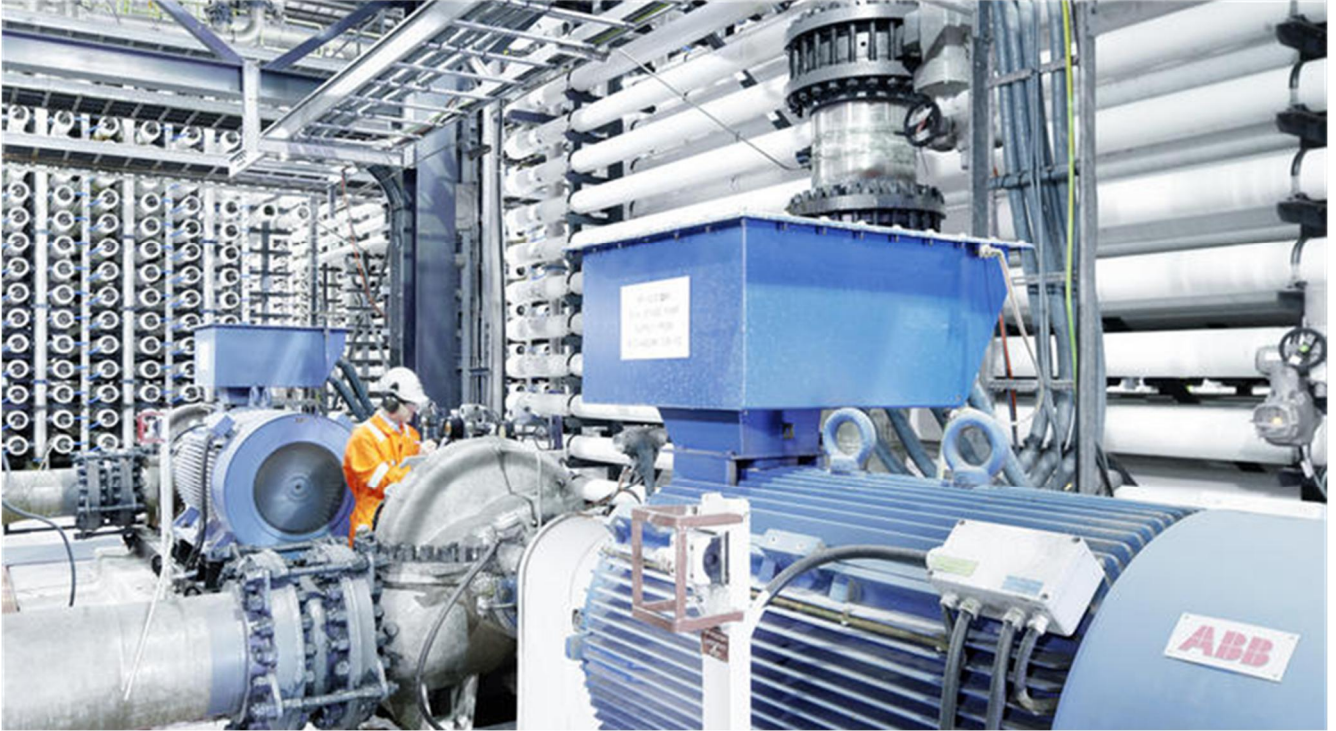
Cenbee.bullock@pfsconsulting.co.uk

+44(0)7733 628 050

ABB

Functional Safety Conference 4/5 November 2014

Pragmatic Compliance Requirement in Offshore Oil & Gas Sector – Challenges & Limitations



Samuel Rajkumar Vincent

Safety Execution Centre Manager

ABB Limited, Aberdeen UK

Abstract

Introduction:

The overall operation, maintenance, repair, modification and retrofit phases of any Safety Instrumented System (SIS) pose significant challenges for process plant operators, particularly for those in the heavily regulated and highly hazardous offshore oil & gas sector. The Operations and Maintenance phase is therefore a key safety lifecycle management requirement for the SIS and is essential from the perspective of the SIS being capable to respond to any demands placed upon it and therefore in support of this requirement; the need for conducting periodic proof tests of the safety instrumented functions (SIF's) and to the monitoring & maintaining of the equipment itself.

Description:

Operating, maintaining and modifying a SIS which is designed and engineered in accordance with minimum industry good practice requirements i.e. compliance with IEC 61508 / IEC 61511 (or those legacy systems installed prior to the release of these functional safety standards) poses both significant challenges and operational/process limitations in the offshore oil & gas sector. One of the fundamental requirements IEC 61511 places upon Operations and Maintenance activities is to maintain the performance of the 'designed-in' functional safety and integrity of the SIS throughout its installed life.

IEC 61511 requires there to be an operations and maintenance planning process and schedule for each SIS. Appropriate maintenance ensures each SIF continues to provide the required functionality with respect to its defined safety integrity level and that consistent operational management ensures that the SIS as a whole provides the required risk reduction.

Following the planning activities closely are the development of appropriate maintenance procedures which are required to define how to maintain and repair the SIS. Essentially this will identify the need for the 'preventative' maintenance (the scheduled activities PM) and the 'corrective' maintenance (the un-planned activities CM). An approach for each requirement will need to be established for the overall planning process including the need for suitable procedures, routines and proforma as the activities differ greatly.

In addition, every aspect of the plans, the procedures and the competency of personnel involved during PM and CM are required to be documented, reviewed, approved and stored accordingly.

Against this background of planning, systems and competency located within a dedicated functional safety management system (FSMS) the End user operations and maintenance teams work under

continuously evolving process pressures and demands in addition to ensuring the installed SIS continues to provide its designed-in functional safety.

In doing so, the operators must fully understand the function the SIS serves as part of the basis of safety for the operation and its relative role in both normal and abnormal operating situations, such as what to do when it initiates a shutdown; and how to react to diagnostic alarms from SIS Components.

The plant maintenance team plays a pivotal role to provide operators with an SIS that performs to its targeted function and integrity and thus ensures safe operation of the plant. Management therefore have a critical role to play in balancing the profit vs. safety equation. Everyone will appreciate that good safety is good business for maintaining profitable and sustainable business operations.

This paper will discuss and review the challenges that are presently in place when operating, maintaining and modifying the SIS in a pragmatic way and in accordance with the overall O&M phases of the Safety Lifecycle as defined by IEC 61508 & IEC 61511.

1. The Operational Challenge

1.1. Introduction

The North Sea offshore sector is a vibrant business area with major reserves of liquid oil and natural gas. The UK oil and gas industry benefits our lives in many ways. Its products underpin modern society, supplying energy to power industry and heat homes, fuel for transport etc. Since first production in the 1960s, the UK offshore oil and gas industry has continuously grown and remains the country's largest industrial investor, paying more tax into Exchequer than any other corporate sector.

In terms of scale, the UK upstream oil & gas supply chain generated turnover of more than £35 billion in 2012. Many companies operate within the sector including, but not limited to, the following major business entities:

- Nexen
- BP
- Total
- BG
- ConocoPhillips
- Talisman
- Shell
- Maersk
- TAQA
- Centrica

To support the sector, many supply chain partners seek to continue to expand their industrial solutions for the hydrocarbon supply chain, encompassing production, processing, transportation, storage and distribution.

There are over 100 offshore oil and gas installations in the North Sea which are in UK waters ranging from smaller structures in the Southern North Sea to very large and heavier structures in the Northern North Sea.

It is estimated that about 80% of the Electrical, Electronic Programmable Electronics Systems (EEPES) for Emergency Shutdown, Process Shutdown and Fire & Gas applications (1st Generation systems such as TMR) currently running in the process industry are in classic lifetime phase, and were installed before the publication of current industry good practice safety standards such as – IEC 61508 / IEC 61511. Note also that these systems were not originally subject to the present demands placed onto the operators to run the assets longer than first envisaged. This demonstrates the challenge we face in not just operating and maintaining new projects using the current 2nd generation SIS which have high availability and reliability through diverse technology (e.g. the ABB AC800M HI Safety system) but also the legacy systems as identified above.

In essence, and to address the challenge of continued operations using a mix of technology systems, many operating companies require operations and maintenance services that encompass the following requirements:

- Integrated automation and electrical products and systems for optimised manufacturing
- Engineering, procurement and construction services that meet manufacturing requirements and cost
- Operations and maintenance services that provide a platform for continued operational success

1.2. Background

High hazard manufacturing and facilities operations and maintenance encompasses a broad spectrum of technical activities that are required to assure the manufacturing environment will safely perform at the optimised profitability level for continuous time periods for which the facility was designed and constructed.

Operations and maintenance activities typically includes the day-to-day activities necessary for the process plant and its supporting utilities systems and equipment to perform their intended function within the notional technical design limits.

According to the EASHW, *'regular maintenance is essential to keep equipment, machines and the work environment safe and reliable. Lack of maintenance or inadequate maintenance can lead to dangerous situations, accidents and health problems. Maintenance is a high-risk activity with some of the hazards resulting from the nature of the work. Maintenance is carried out in all sectors and all workplaces'*.

In the context of the IEC 61508 and IEC 61511 standards, it is essential that all hardware and/or software modifications related to any SIS, which are in operation, are properly planned, reviewed and approved prior to the execution of these activities.

Operations and maintenance activities are therefore managed as a combined entity because a processing facility cannot operate at peak efficiency and corresponding profitability without being maintained; therefore the two are planned and as managed as one. This will therefore be implemented as either PM or CM which are both further defined as:-

- Preventative maintenance is a series of routine and planned operations to ensure the functional safety performance of the SIS is maintained throughout its operational life
- Corrective maintenance is a process implemented in response to failures and anomalies of the SIS to restore the functional safety performance of the SIS throughout its operational life

Recent high profile incidents and accidents within the process Industries has brought into sharp focus the need for Asset Operators to effectively maintain, operate and seek ways to continually improve their basis of safety whilst managing the heavily regulated and stakeholder expectations of this sector.

Operationally, the process dynamics are changing rapidly on an increasing frequency as process pressure and temperatures now widely differ across many different assets. With increasing interconnectivity of the operational platforms with respect to the basis of safe operation, this brings further challenges for the sustainable management of the asset base.

In addition competitive pressures are such that the industry continues to face greater financial, resource capture (deep water recovery) and competence issues in meeting the challenge of change. This in itself has meant that asset management programmes continue to prolong the longevity of the existing asset base that is already well past the original design life and so the ever increasing impact of delivering successful O&M.

Today, the use of programmable control systems to implement safety functions is now a common practice within the Process Industries and Functional Safety Management is achieved by established IEC 61508 and IEC 61511 Standards. However, for over 30 years, protection and mitigation systems have been installed on high hazard facilities comprising and including Emergency Shutdown Systems, Fire & Gas Systems, Boiler Management Systems, etc. These safety related (legacy) systems provide an essential layer of protection when the plant and equipment experience operational disturbances which can potentially go out of control leading to an incident.

It therefore follows that the advent of an SIS onto a manufacturing facility is a critical protection system. During the design and engineering phase, the individual SIF theoretical Safety Integrity Level is achieved based on certain design assumptions in order to predict the performance of the SIF.

As such, the intended operating conditions will affect these baseline design assumptions and therefore the eventual SIF safety integrity. Periodic maintenance and proof testing is required to be implemented as a key specification requirement so as to ensure the continued and demonstrable integrity of each SIF post commissioning. Therefore competent persons, organizations and supporting management procedures are necessary to ensure that the system complies with industry good practices and local/international standards.

The IEC 61511 safety lifecycle approach requires, that appropriate competency is applied in each phases of the safety lifecycle and this need to be consistently applied using an auditable functional safety management system. So within the O&M safety lifecycle phases, how can an operator who is challenged with maintaining process safety and maintaining aggressive production targets actually implement and monitor a verification and proof testing program? Not performing Functional Safety maintenance and individual SIF proof testing is simply not an option.

1.3. Effective O&M Practices and what is important for success?

For those safety related systems that have been well managed and maintained (or conversely those that have not) and thus performed as expected with either good or poor reliability and availability over

many years, the ability to maintain functional safety performance will be inextricably linked to the O&M practices delivered within the facility.

Having discussed the implication for safety lifecycle compliance to the safety standards in this area, the author believes that effective O&M practices will need to have considered the following key attributes:

List of Authorised Personnel

SIS operational anomalies should be dealt with in an organised way from within the end user organisation and the requirements replicated into any supply chain provider perspectives. In doing so any work activities related to SIS should only be undertaken by authorised and competent personnel. It is a mandatory requirement for compliance with the safety standards that personnel both from the end user and any service provider organisations, have the correct authorisation, knowledge and experience to be able to deal with and evaluate O&M activities onto SIS, the impact of required actions, the risks associated with certain actions and the delivery of such work requests.

Operations/system constraints

Note that any SIS scheduled maintenance or fault diagnosis may result in a system with limited capabilities to perform its risk reduction functions, for example due to being taken off line for routine maintenance, or loss of I/O-module(s), loss of redundancy of communications, redundancy of central processor, or power supply, etc. Therefore on occasion, it may be necessary to stop operation of part of the process during the period of scheduled maintenance or system diagnosis and repair. This operational constraint should be considered as part of the O&M impact assessment process.

It should also be noted that the time between occurrence/detection of the SIS error/fault and resolution of the error/fault may be restricted as the system is allowed to function in a “degraded mode” for a limited period of time before a complete shutdown is required and in doing so additional risk reduction measures may have to be implemented by the operations team to compensate for this event.

Referring back to the importance of O&M innovation at the development of the SIS safety requirements specification (SRS), the MTTR requirements may also need to identify issues with automatic shutdown of the system depending on how the diagnostics for the safety system controller have been configured to react to system faults i.e. the shutdown timer may have been running well before the maintenance request has been acknowledged i.e. avoidance of unnecessary spurious trips due to the lack of communication and response between the plant operators and the maintenance team.

Getting the job done

Before any work starts, a method statement and impact assessment should be developed and included within any preventative maintenance routine documentation. Separately, a similar system should exist for corrective maintenance activities which will need to develop a bespoke method statement which will be dependent on the nature of the faults identified. In addition an impact analysis shall always be produced with respect to corrective action where functional safety performance could be affected by direct intervention with the SIS hardware and software.

Accordingly, any on site requirement, or remote investigative/diagnostic assessments of a running SIS will require the end user approval via a suitable permit to work and that no work should commence on the SIS unless a valid permit to work is issued by the responsible permit authority.

Note again that it is the responsibility of the end user issuing the permit to work to clearly state the conditions under which the O&M activity is to be allowed to happen. This will include the operations which are allowed by the maintenance engineer (e.g. change hardware modules, download software, change configuration settings, block/deblock functions/modules, etc) and specifically state those which are not allowed.

The O&M Engineer with respect to competency requirements will always need to be aware of the nature of the system application (i.e. a safety integrated system which may accidentally shutdown the process when incorrectly operated). This and other considerations shall be included in the O&M method statement and work impact risk assessment mentioned earlier.

System Documentation

The end user will be required to ensure that the O&M Engineer will have access to all system documentation. It is the responsibility of the end user to ensure that supporting system documentation is made readily available, current and valid for use. Examples of system documentation may include but not be limited to

- P& ID's
- Cause & Effect Diagram
- Wiring Schedule
- System Performance logs
- End user historical O&M performance/maintenance reports
- etc.

Failure to supply up to date valid documentation could mean that a sufficient and adequate risk assessment cannot be undertaken for the required work activities and that additional measures may have to be taken by the end user to rectify any concerns prior to the work proceeding via the PTW.

Diagnosis as opposed to maintenance

Consideration needs to be made here, after access to the SIS has been granted and approved by the end user (either direct or remote and has been duly authorised), that the O&M Engineer should then be allowed to perform a system diagnosis as applicable. It will be important that the O&M Engineer should pay special attention to recent maintenance and service activities for example including but not limited to hardware and/or firmware and/or application software modifications, etc. It is usual that the diagnosis will take place covering:

- Direct access – where an end user technical authority presence provides the added possibility to discuss the system behaviour with operations teams in addition to the system diagnosis.
- Remote access – which may require a constant telephone connection with the end user on the other end to be able to discuss matters while performing the diagnosis.

However it will be imperative that during this phase the O&M Engineer should not change any information which resides in the system until the impact assessment has been completed based on this initial non-intrusive diagnostic exercise. Note the diagnosis activities should be limited to reading information (opening and closing displays, logs, files etc.) without changing any information in the system and in accordance with the appropriate techniques and methods as found in Table B.4 of IEC 61508 Part 2.

Implications for SIS Modification

During the system analysis activities outlined above, if the work request/problem is agreed to be rectified via a modification to the SIS, then the O&M Engineer should inform the responsible technical authority within the end user organisation that a formal change request (management of change MOC) is to be made and as a minimum an impact assessment will be required to be undertaken under the necessary MOC processes.

Note that this activity is a mandatory requirement that any SIS modifications are to be managed in full accordance with IEC 61508 Ed 2 and IEC 61511 requirements. Modifications can only proceed with the full approval of the end users Technical Authority (TA). The responsibility for this modification is owned solely by the end user and should be managed accordingly utilising their compliant functional safety management system.

It should also be noted that the change impact assessment should be rigorously reviewed by all authorised parties concerned. The impact assessment states the implications of the proposed change and should be documented accordingly to identify as a minimum:

- The repair or replacement activity affecting SIS performance
- How does the intended repair / replacement proposed solution impact on determining if the change on a component or function; has an effect on other components or functions within the SIS under review; or other systems connected to it?
- Define any degradation of the SIS whilst repair or replacement is performed and ensure the Client understands the impact of the degradation so that they can apply additional safety measures whilst the work is carried out
- Once the impact assessment form is completed, it shall be reviewed and agreed with the technical authority or their representative (as an independent reviewer) and approved along with the Job Method Statement

The risk assessment states the risks which are associated with the implementation of the solution. Although the probability of the risk may be very small, the effect on the SIS and any potential outcome could be high. The risk assessment can be prepared with the contribution of a number of parties in close cooperation with the end user, however the end user has overall responsibilities to determine how the planned changes may affect the process and plant given their knowledge of the application of the system.

This experience is to be combined with the O&M Engineer's experience and knowledge of the SIS technology platform and the application of the safety elements used within the system. This assessment should result in a better balanced risk assessment acceptable for the end user. In addition the end user shall take appropriate "operational" actions if necessary to mitigate the risks.

A risk assessment shall always be completed regardless of whether the task is initial investigative work or planned maintenance, independent of the required actions, such as exchange of a faulty hardware module, inspection of application software, update of firmware, etc.

1.4. One Approach to Support Effective O&M

Responsible O&M supply chain partners such as ABB provide the necessary commitment and traceability to demonstrate and ensure that all safety applications are implemented and maintained in accordance with the international safety standards IEC 61508 / IEC 61511 and to be recognized as preferred suppliers of service, engineering and systems with professional functional safety solutions and competent resources.

In particular the end user organisations operating in the high hazard sectors recognise the additional assurance that functional safety management systems provide in underpinning systematic capabilities for relevant lifecycle phase requirements.

When it comes to the O&M phases in particular, such leading service organisations will utilise a TUV accredited FSMS for the operations, maintenance and modifications of a SIS on behalf of their client's commitments to maintain and improve functional safety performance for the asset.

For example, ABB Service Aberdeen started this procedural evolution in 2012, this was in response to our own internal ABB mandate for continued FS excellence and to ensure that our customer recognized the benefits of the ABB SIS design and operation & maintenance service provision in compliance with relevant safety standards.

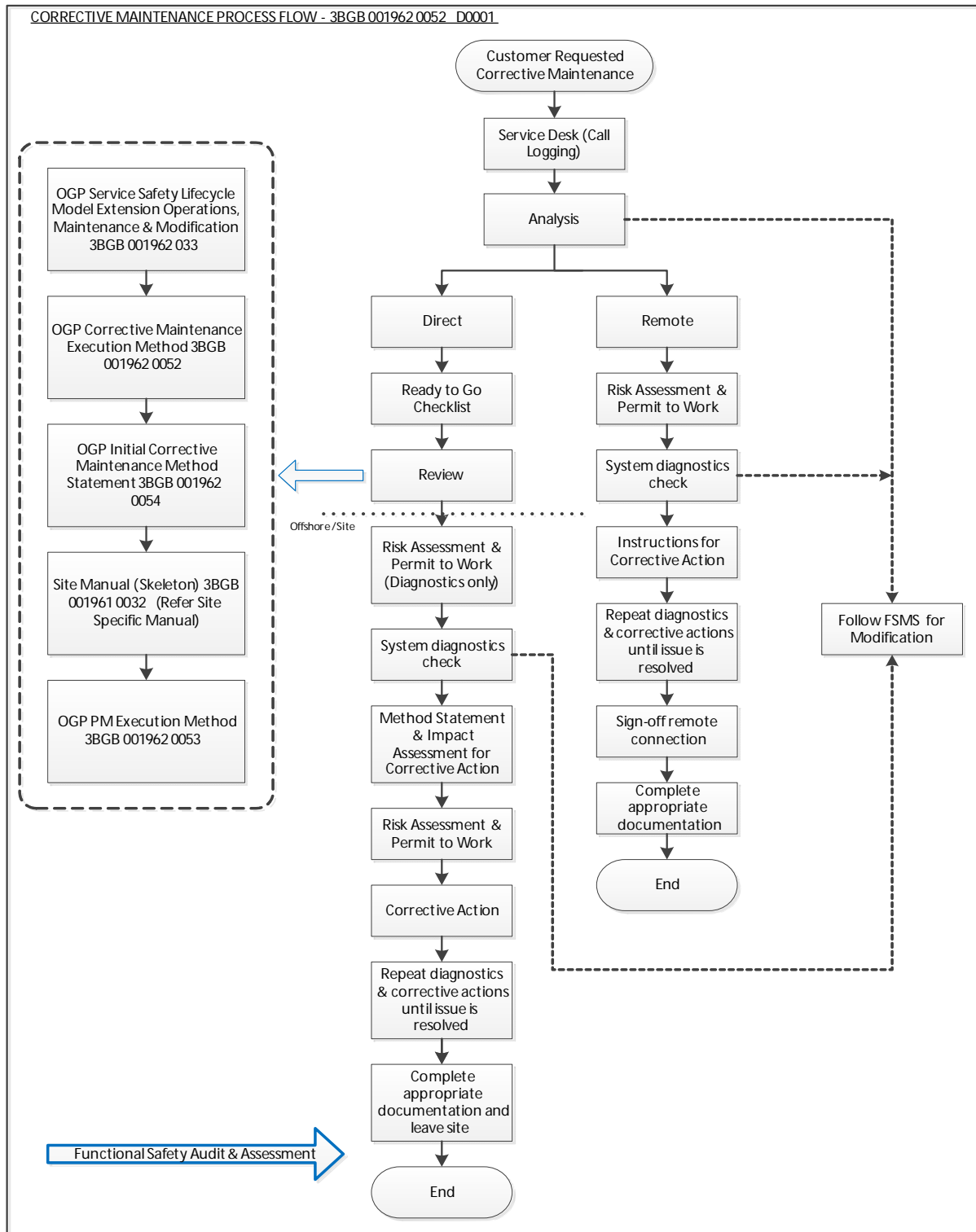
This overall 18 months journey required full commitment and empowerment from local senior management, support for the initiative from our key clients and the parallel activities of working with these clients to build on our successful relationships and for integrating their FSMS processes with ours to streamline the overall supply chain interfaces etc. The effort for developing the FSMS to cover phases 4 to 7 within IEC 61511 has resulted in a market leading accredited certification regarding our SIL 3 systematic capabilities as endorsed by TUV SUD as detailed in section 1.4.1 and 1.4.2.

Such certified procedures will need to be aligned directly with the IEC 61508: Ed2 21010, and equivalent IEC 61511 O&M lifecycle model requirements for maintenance and modification covering;

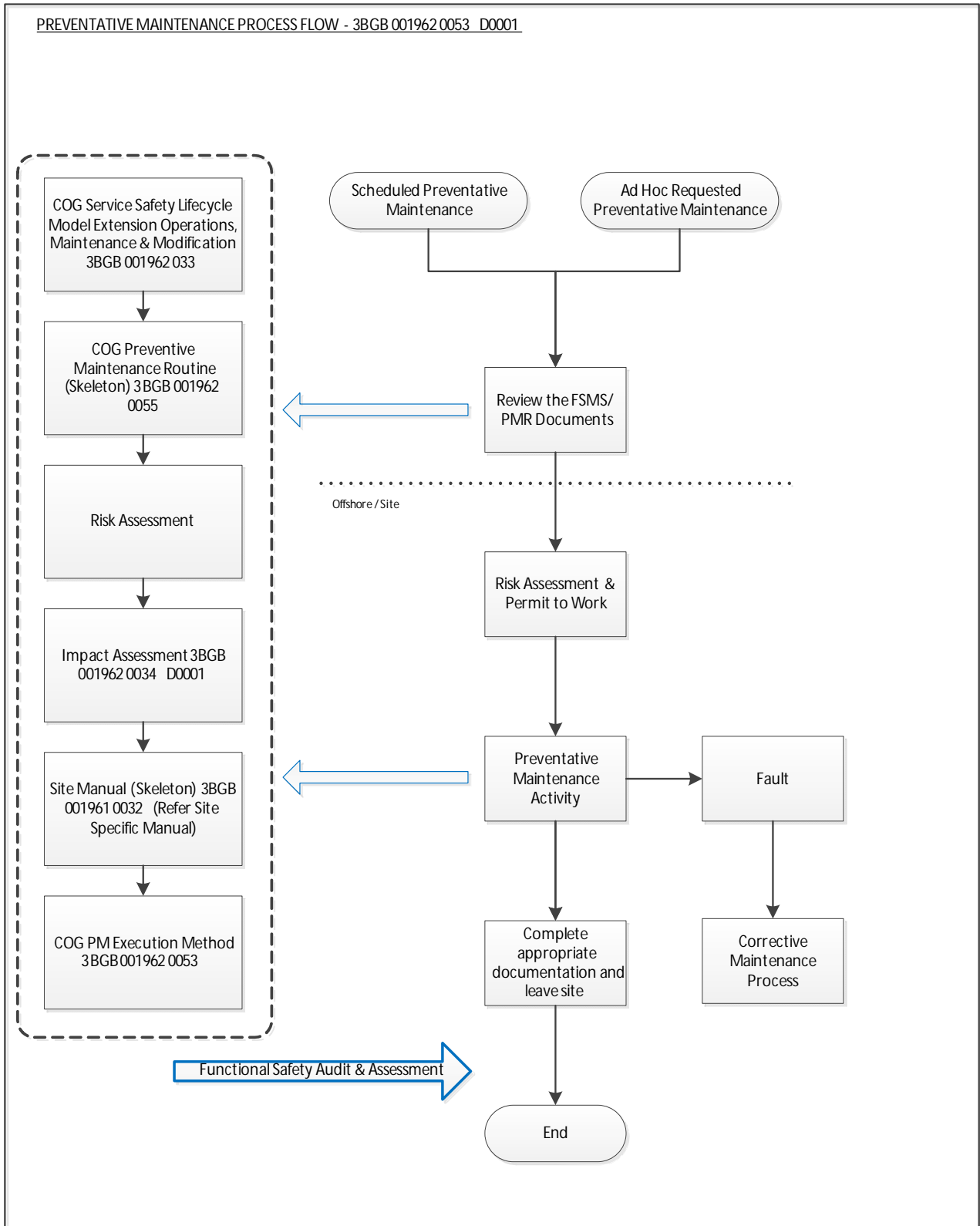
- Corrective maintenance procedures, checklists and method statements
- Preventative maintenance procedures, checklists, method statements and routines
- Management of change and impact assessment
- Gap analysis and modification safety requirements specification

- Modification change design and engineering realisation
- Demonstrable documentation and traceability to industry good practice

1.4.1 Corrective Maintenance Process Flow



1.4.2 Preventative Maintenance Process Flow



1.5. How is a compliant O&M FSMS developed within the End User and Supply Chain?

A Functional Safety Management System (FSMS) is usually developed as a result of a gap analysis performed against the existing in-house company ISO9001 Quality Management System (QMS), and the requirements of the relevant clauses of the good practice safety related standards; IEC 61508, IEC 61511 and ISA84 and also any supporting standards dependent on SIS scope i.e. IEC 62061 and IEC 61800-5 for machinery. Most organisations will purport to have the QMS certification as the baseline of a structured procedural approach to try and manage functional safety within them; however experience suggests that the process of a detailed gap analysis of these 'Hybrid' systems usually identifies that many of the recommended techniques and measures required by the standards are generally missing, or are inadequate.

For the Asset Operator, it will be important to assess the capabilities of both the internal O&M systems as well as the supply chain to deliver a comprehensive documented solution to meet industry and regulatory good practice expectations.

From experience of assessing many FSMS over time, the inclusion of simple high level 'additions' to QMS systems that have little substance behind them does not provide adherence to the normative requirements of the safety standards. In particular, the procedures become weaker in detail and competency requirements when greater levels of risk reduction are required to be engineered e.g. SIL 2 and above.

Responsible suppliers who embrace the 'best in class' requirement of their clients, will go to great lengths to both interpret and provide terminology understanding of the relevant safety related standards (and how this relates to the existing QMS process) for the development of an additional FSMS procedural set which results on the existing QMS being extended and improved.

Such commitment to FSMS development by the supplier requires extensive internal resource and funding and requires continual effort to maintain its relevance once developed. Similarly the SIS design engineering, operations and maintenance documentation and verification and validation activities delivered by these best in class organisations will differ to that of a typical non-safety related project.

It therefore follows that Asset Operators seeking to partner with a responsible supplier will expect to see the provision of FSMS compliance activities within any proposals received against a safety related bid enquiry.

This attainment of a robust methodology to demonstrate that functional safety is being managed correctly should be a key recognition factor for Asset Owners and EPC's as a means to underpin their own FSMS requirements. By doing so this provides increasing confidence and assurance that SIS solutions that are being developed on their behalf are satisfactory.

Such supplier FSMS commitment ultimately demonstrates to the Asset Owner that the supplier:-

- Provides documented and traceable compliance to the Industry good practice safety standards
- In use and continuous improvement of the FSMS, allows the supplier to work closely with the Asset Owner/EPC to ensure that functional safety management is executed to provide safe and reliable solutions drawing on the combined experience of the Asset Owner/EPC and supplier project teams

- Ensures that the FSMS is fit for purpose and withstands detailed stakeholder scrutiny / audit and is underpinned further by appropriate third party assessment
- Ensures that the safety elements engineered for the solution meet the requirements of the standards in terms of functionality and reliability e.g. ABB's 800xA Hi SIL 3 capable safety controller

1.6. So are all FSMS Procedures the Same?

As with all supplier claims to competency and procedure / systems that are deployed to design and engineer SIS solutions, the depth and rigour for key compliance requirements can vary greatly.

There is a stark difference between a self-declaration of conformity to IEC 61508 / IEC 61511 and an accredited third party certificate from a leading Industry certification body such as TÜV. The effectiveness of any O&M FSMS can only be measured on the basis of the third party certification audit to ensure it complies with the requirements of the safety standards. When it comes to the Asset Owner/EPC making a selection on a supplier to design, engineer and verify the adequacy of a SIS solution it follows that suppliers who have gone the extra mile effectively differentiate themselves from the competition.

As the ultimate responsibility for functional safety management (FSMS) resides with the Asset Owner, then clearly a professional and compliant approach to the development of the system utilising an accredited FSMS methodology represents 'best in class' management of the functional safety requirements. This allows traceability and transparency for FS requirements to be audited and assessed by both in-company and regulatory stakeholders alike.

Likewise, the reciprocal to this approach for a solution developed by a less robust FSMS could lead to the potential for:-

- Misinterpretation of ITT technical solution responses by the project owners commercial team during cost comparison analysis of response content
- Project schedule slippages, due to time spent in clarifying TQs & PQs, performing impact analysis and in-depth verification and validation for every change in the specification i.e. design by TQ
- Potential for expensive re-engineering of the solution at factory acceptance testing (FAT) based on misinterpretation of requirements and poor functional safety management practices regarding baseline assumptions and technical application, which invariably impacts on resources and costs
- The potential that a safety system that does not meet the necessary risk reduction could be installed at site
- Lack of demonstrable traceability to Industry good practice standards
- Potential exposure to liabilities both corporately and professionally
- Failure to recognise the asset management 'inherent benefits' of the technology solution offered i.e. use of ABB 800xA asset management diagnostics features

For all involved in functional safety management throughout the entire safety lifecycle, there should be inclusion within the inherent FSMS processes for a robust competency assessment process with acceptance criteria for the key roles in the design, engineering and independent verification activities required of the project deliverables based on knowledge, experience, training and qualifications.

Each of these criteria should be reviewed against the technology selected for the project, the industry into which the project would be delivered, and the standards themselves. Any shortcomings in competency are mitigated by peer review, or additional training. Again visibility of this process and the procedures to be followed should be a cornerstone of a compliant FSMS process.

As the Asset Operator ultimately responsible for the end result, are you confident that the people making the decisions on your behalf are competent to do so?

Note also that while some organisations claim certification for design and engineering of SIS, ABB has already gone one better and included the O&M phase activities within their TuV accreditation.

1.7. Conclusion

Compliance to industry good practice standards via the demonstration of third party accredited FSMS certification should be viewed as a significant strength and desirable requirement by Asset Owners. Implementing good safety practices should not be viewed as a cost impediment when correctly priced proposals are returned with FSMS deliverables included (regardless of project physical size and expected duration).

If Asset Owner/EPC teams can understand the benefits of a FSMS, they will be more likely to request and specify certificated FSMS requirements in practice and provide a common approach for project implementation and operations and maintenance excellence so that those responsible for the management of FSMS within the Asset Owner/EPC project structure ensure that:

- There is no ambiguity in what needs to be delivered and to ensure procedures and processes have a clearly defined function
- Ensure project teams within the entire safety lifecycle have a clear definition of how the project should be executed with respect to O&M innovation/requirements
- Ensure everyone within the entire safety lifecycle understand the differentiation and benefits of accredited FSMS certification to their business
- FSMS expectations on SIS deliverables, operations & maintenance, auditing and assessment become second nature
- For increasing levels of SIS assurance, the O&M documentation, competencies and deliverables should be in alignment with any internal/external stakeholder expectations e.g. in-company auditing technical specialists and regulatory authorities

1.8. Reference

- IEC 61508 Edition 2 (International Standard of rules applied in industry, titled Functional Safety of Electrical/Electronic/Programmable/Programmable Electronic Safety-related Systems)
- IEC 61511 (International Standard of rules applied in process industry, titled Functional Safety – Safety Instrumented Systems for the Process Industry Sector)
- EASHW (European Agency for Safety and Health at Work)



Samuel Rajkumar Vincent Functional Safety Conference 4/5 Nov 2014

Pragmatic Compliance Requirements Operations and Maintenance in accordance with IEC 61511 – Challenges & Limitations

Abstract Agenda

- Discuss the requirements for the overall operation, maintenance, repair, modification and retrofit phases of any Safety Instrumented System (SIS)
- Identify the significant challenges for process plant operators
- Focus on the operations and maintenance lifecycle phases for maintaining SIS functional safety performance
- Summary and conclusions



The Operational Challenge

Introduction

- The North Sea offshore sector is a vibrant business area with major reserves of liquid oil and natural gas.
- To support the sector, many supply chain partners seek to continue to expand their industrial solutions.
- It is estimated that around 80% of the E/E/PES (1st & early 2nd Generation systems) currently running in the process industries are in 'Classic' lifetime phase
- This demonstrates the challenge we face in not just operating and maintaining new projects using modern SIS; but also the mix of legacy systems as identified above.

Industry Focus

Supply Chain Services

- Many operating companies require operations and maintenance services that encompass the following requirements:
 - Integrated automation and electrical products and systems for optimised manufacturing
 - Engineering, procurement and construction services that meet manufacturing requirements and cost
 - Operations and maintenance services that provide a platform for continued operational success



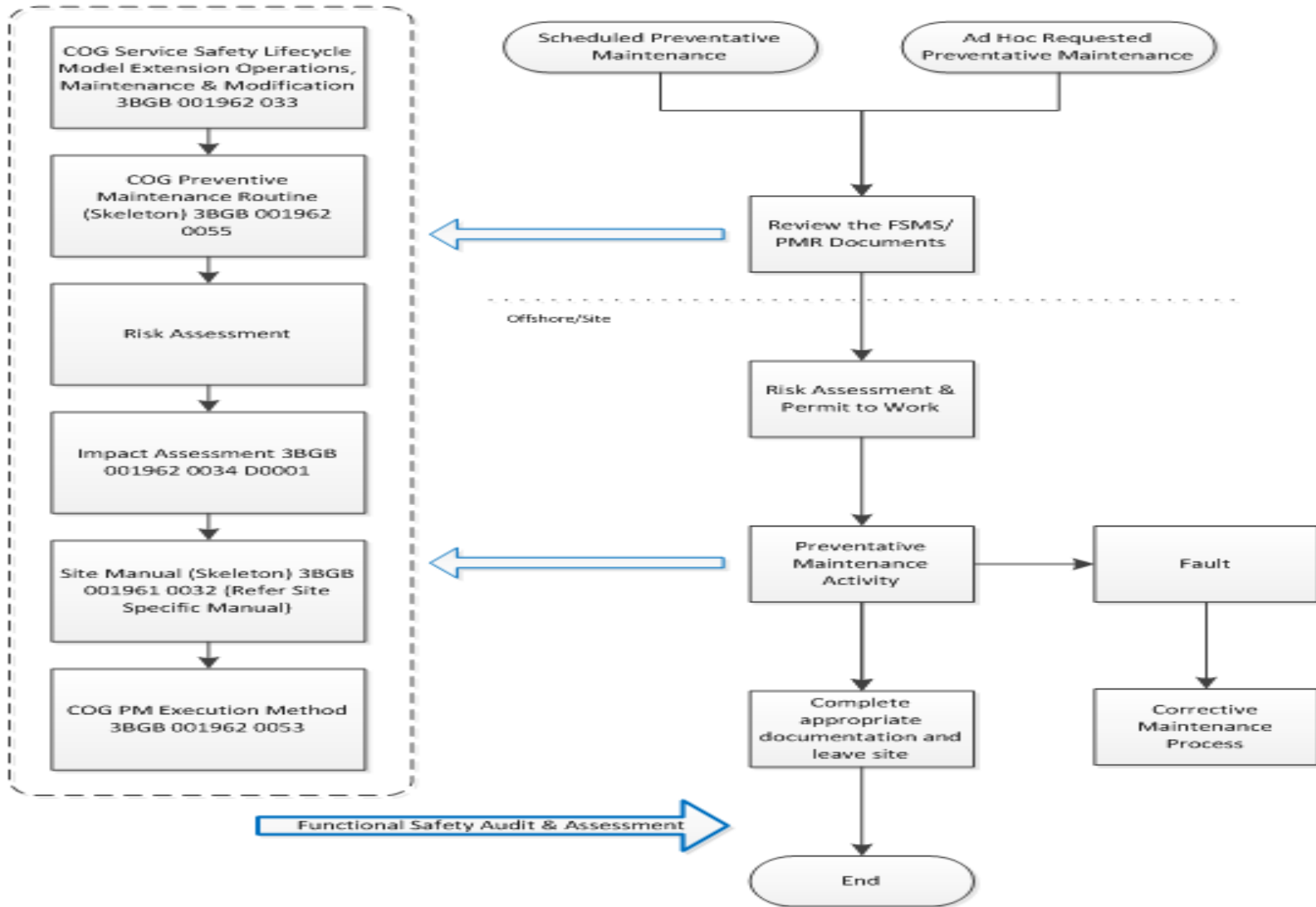
O&M Requirements

- Operations and maintenance activities typically include the day-to-day activities necessary for the process plant and its supporting utilities systems
- Regular maintenance is essential to keep equipment, machines and the work environment safe and reliable.
- It is essential that all hardware and/or software modifications related to any SIS are properly planned, reviewed and approved prior to the execution of these activities.

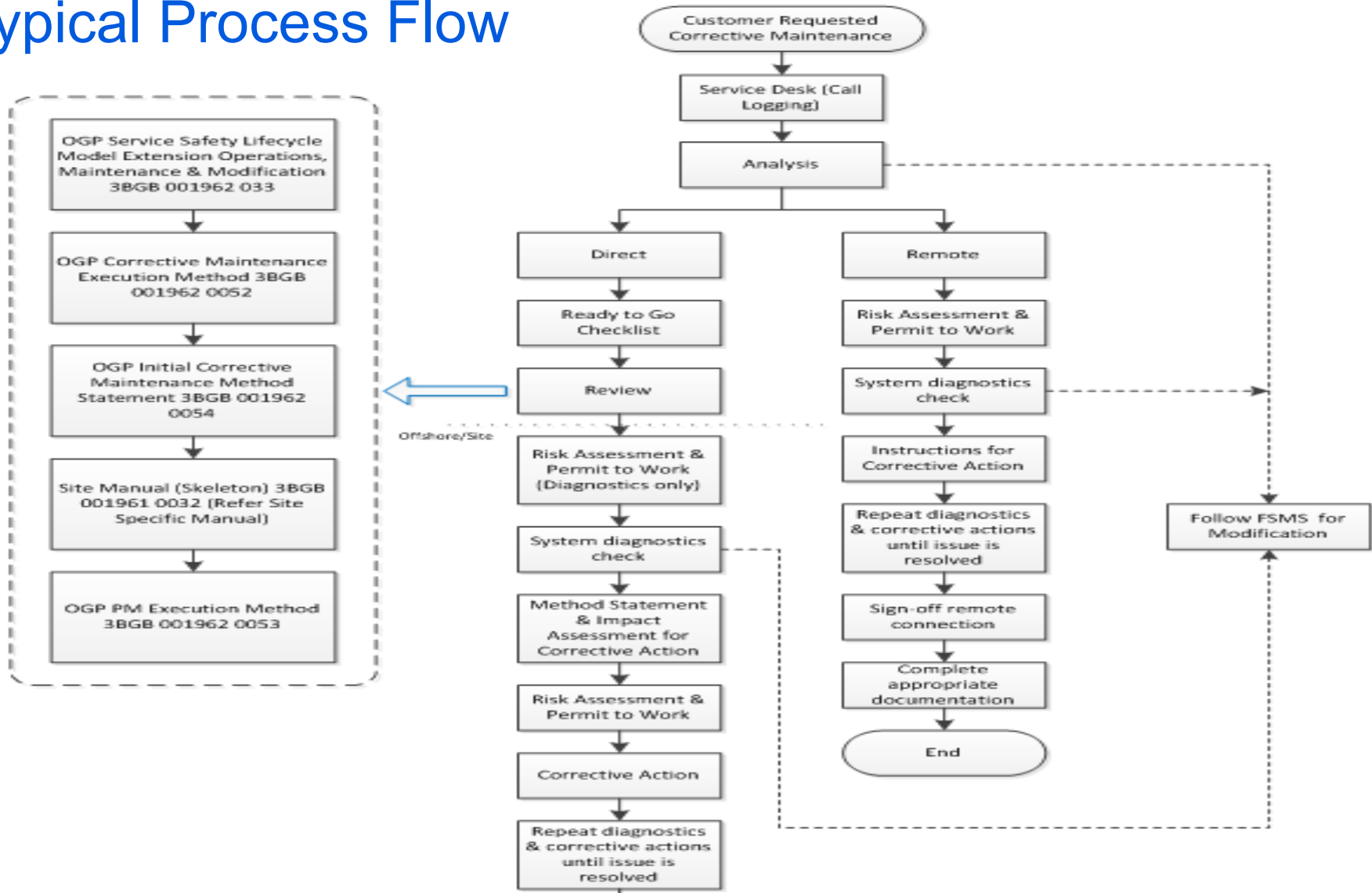


- Operations and maintenance activities should be managed as a combined entity
- A processing facility cannot operate at peak efficiency and corresponding profitability without being maintained; therefore the two are planned and as managed as one.
- Efficiency and profitability can be achieved by active maintenance, applying either PM or CM which are both further defined as:-
 - Preventative maintenance is a series of routine and planned operations to ensure the functional safety performance of the SIS is maintained throughout its operational life
 - Corrective maintenance is a process implemented in response to failures and anomalies of the SIS to restore the functional safety performance of the SIS throughout its operational life

Preventative Maintenance Typical Process Flow



Corrective Maintenance Typical Process Flow



Operating conditions

- The Safety Integrity Level achieved during design and engineering is as per the required target SIL
- The on-going safety performance – i.e., SIL may be affected by the operating conditions
- Periodic maintenance and proof testing is required to be implemented so as to ensure the continued and demonstrable integrity of each SIF post commissioning.
- The IEC 61511 safety lifecycle approach requires, that appropriate competency is applied
- *How can an operator who is challenged with maintaining process safety and maintaining aggressive production targets actually implement and monitor a verification and proof testing program?*



- The ability to maintain functional safety performance will be inextricably linked to the O&M practices delivered within the facility.
- Operations & Maintenance practices will need to have considered the following key attributes:
 - List of authorised personnel
 - Operations/system constraints
 - Method statement and impact assessment for PM & CM activity
 - Access to system documentation
 - Diagnosis as opposed to maintenance
 - Implication of SIS Modification



One Approach to Support Effective O&M

- Responsible O&M supply chain partners need to demonstrate that all safety applications meet the requirements of IEC 61508/61511;
 - This covers commitment, engineering and system with professional functional safety solutions, traceability, competent resources etc.
- High hazard sectors recognise the additional assurance that functional safety management systems provide
- When it comes to the O&M phases in particular, such leading service organisations will utilise a TUV certified FSMS for the operations, maintenance and modifications of a SIS



One Approach to Support Effective O&M

- Such certified FS procedures will need to be aligned directly with the IEC61508: Ed2 2010, and equivalent IEC 61511 O&M lifecycle model requirements for maintenance and modification covering;
 - Corrective maintenance procedures, checklists and method statements
 - Preventative maintenance procedures, checklists, method statements and routines
 - Management of change and impact assessment
 - Gap analysis and modification safety requirements specification
 - Modification change design and engineering realisation
 - Demonstrable documentation and traceability to industry good practice

How is a compliant O&M FSMS developed

- A Functional Safety Management System (FSMS) is usually developed as a result of a gap analysis performed against the management of FS clauses in the standards
- For the Asset Operator, it will be important to assess the capabilities of both the internal O&M systems as well as the supply chain
- This attainment should be a key recognition factor for Asset Owners and EPC's as a means to underpin their own FSMS requirements.
- By doing so this provides increasing confidence and assurance that SIS solutions that are being developed to achieve the necessary risk reduction.



How is a compliant O&M FSMS developed

Benefits

- Such supplier FSMS commitment ultimately demonstrates to the Asset Owner that the supplier:-
 - Provides documented and traceable compliance to the Industry good practice safety standards
 - Allows the supplier to work closely with the Asset Owner/EPC to ensure that functional safety management is executed to provide safe and reliable solutions
 - Ensures that the FSMS is fit for purpose and withstands detailed stakeholder scrutiny / audit
 - Ensures that the safety elements engineered for the solution meet the requirements of the standards in terms of functionality and reliability



So are all FSMS Procedures the same?

- As with all supplier claims to competency and procedure / systems the depth and rigour for key IEC 61511 compliance requirements can vary greatly.
- There is a stark difference between a self-declaration of conformity and an accredited third party certificate from a leading Industry certification body such as TÜV.
- Ultimate responsibility for functional safety management (FSMS) resides with the Asset Owner
- A professional and compliant approach to the development of the system utilising an certified FSMS methodology represents 'best in class' management of the functional safety requirements.
- This allows traceability and transparency for FS requirements to be audited and assessed by both in-company and regulatory stakeholders alike.

FSMS

Potential problems?

- A less robust FSMS could lead to the potential for:-
 - Project schedule slippages, due to time spent in clarifying TQs & PQs, i.e. design by TQ
 - Potential for expensive re-engineering of the solution based on misinterpretation of requirements
 - The potential that a new or modified safety system that does not meet the necessary risk reduction could be installed at site
 - Lack of demonstrable traceability to Industry good practice standards
 - Potential exposure to liabilities both corporately and professionally
 - Failure to recognise the asset management ‘inherent benefits’ of the technology solution offered i.e. use of asset management diagnostics features

- Compliance to industry good practice standards via the demonstration of third party accredited FSMS certification should be viewed as a significant strength and desirable requirement by Asset Owners.
 - There is no ambiguity in what needs to be delivered and to ensure procedures and processes have a clearly defined function
 - Ensure project teams within the entire safety lifecycle have a clear definition of how the project should be executed with respect to O&M innovation/requirements
 - FSMS expectations on SIS deliverables, operations & maintenance, auditing and assessment become second nature
 - For increasing levels of SIS assurance, the O&M documentation, competencies and deliverables should be in alignment with any internal/external stakeholder expectations e.g. in-company auditing technical specialists and regulatory authorities

Power and productivity
for a better world™





Proof Testing

www.risknowlogy.com

or contact

rgb@risknowlogy.com

Risknowlogy

- ▶ Experts in Risk, Reliability and Safety
- ▶ Founded 2002
- ▶ UK office 2013
- ▶ Functional Safety Services
 - ▶ Consultancy - Functional Safety Management
 - ▶ Consultancy - Functional Safety Product Design
 - ▶ Consultancy - HAZOP Chair, LOPA, SIL Determination, SIL Verification
 - ▶ Certification - people, systems, organisations, products
 - ▶ Training - TUV Functional Safety Engineer / Professional
 - ▶ CPD at Engineer level - Workshops (e.g. SIL Verification and Calculation)
 - ▶ Instrument Technician Training - **SILComp**

Our Topics for today ...

- ▶ What is a Proof Test
- ▶ Why Proof Test?
- ▶ Ideal Proof Testing
- ▶ Lessons from a real world review
- ▶ Issues for practical Proof Testing
- ▶ Future of Proof Testing

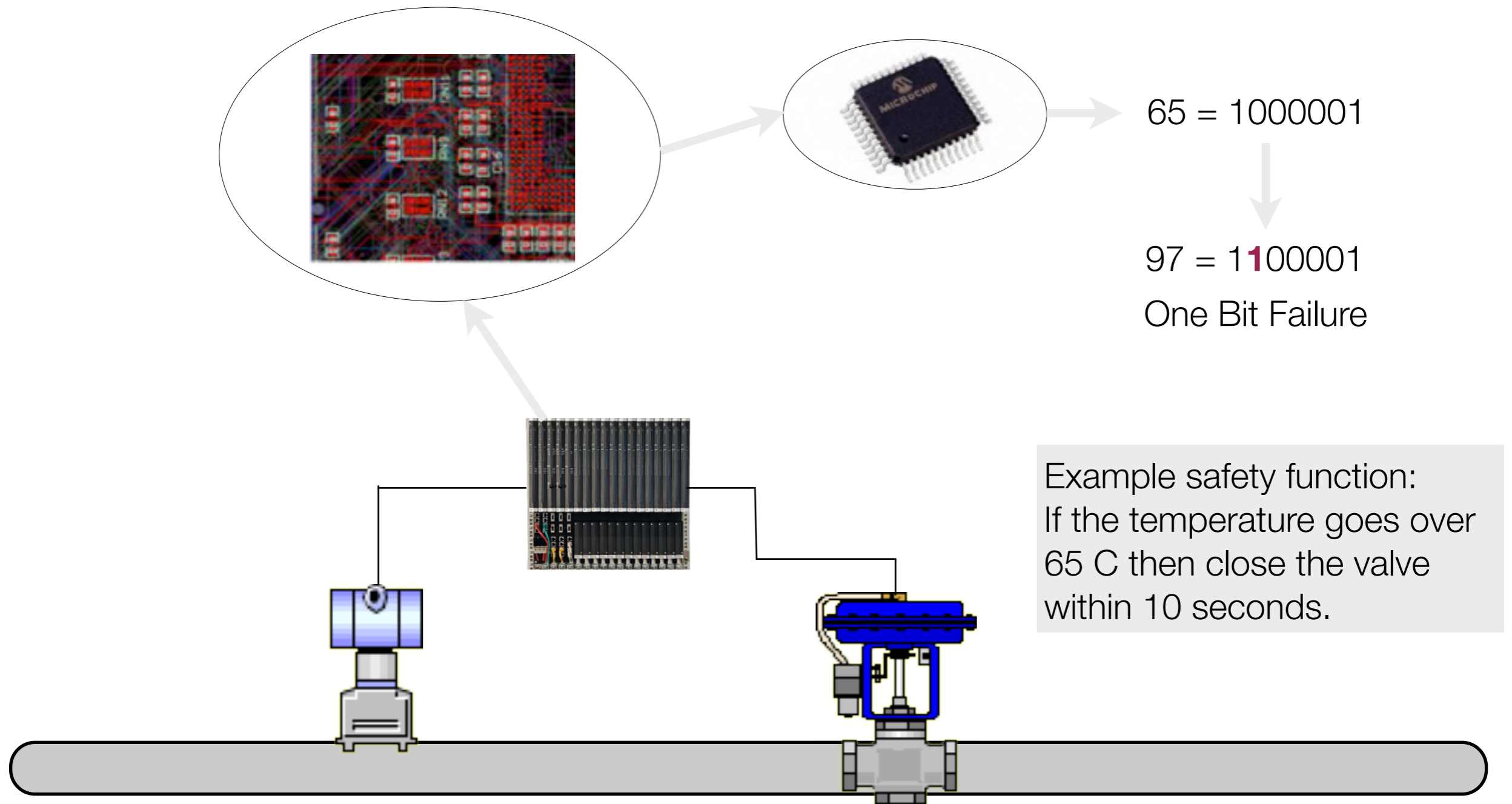
What is a Proof Test

- ▶ A way of finding undetected, dangerous failures
- ▶ With “demand” mode systems
 - ▶ you can run all day with a dangerous fault
 - ▶ you don't know it
 - ▶ until the day you needed it to work
- ▶ As near as you can, simulate a demand
- ▶ Which means you need to know what it is supposed to do
- ▶ Frequency of Proof Testing is decided by your dangerous undetected failure rate

Safety Instrumented System Failures

- ▶ Safety instrumented systems can fail because of...
 - ▶ Random hardware failures
 - ▶ Common cause hardware failures
 - ▶ Systematic failures

Random Hardware Failures - Safe or Dangerous?



Random Hardware Failure

▶ Picture to follow

Common Cause Failures

- ▶ Complete plant flooded because of heavy rainfall, bad drainage and dike failure
- ▶ Below: lightning strike



PFD and SIL

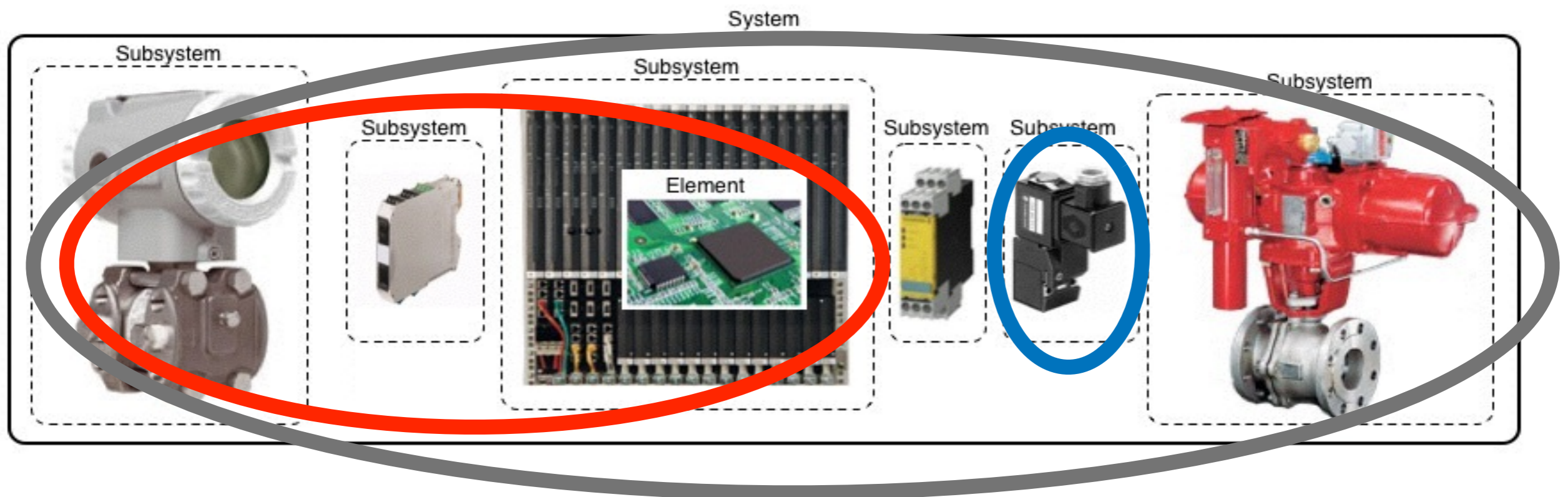
- ▶ PFD from the Dangerous Undetected Failure rate, Beta Factor, Proof Test Interval and MTTR

SIL	PFDavg	Risk Reduction
4	0.0001 - 0.000001	10000 - 100000
3	0.001 - 0.0001	1000 - 10000
2	0.01 - 0.001	100 - 1000
1	0.1 - 0.01	10 - 100

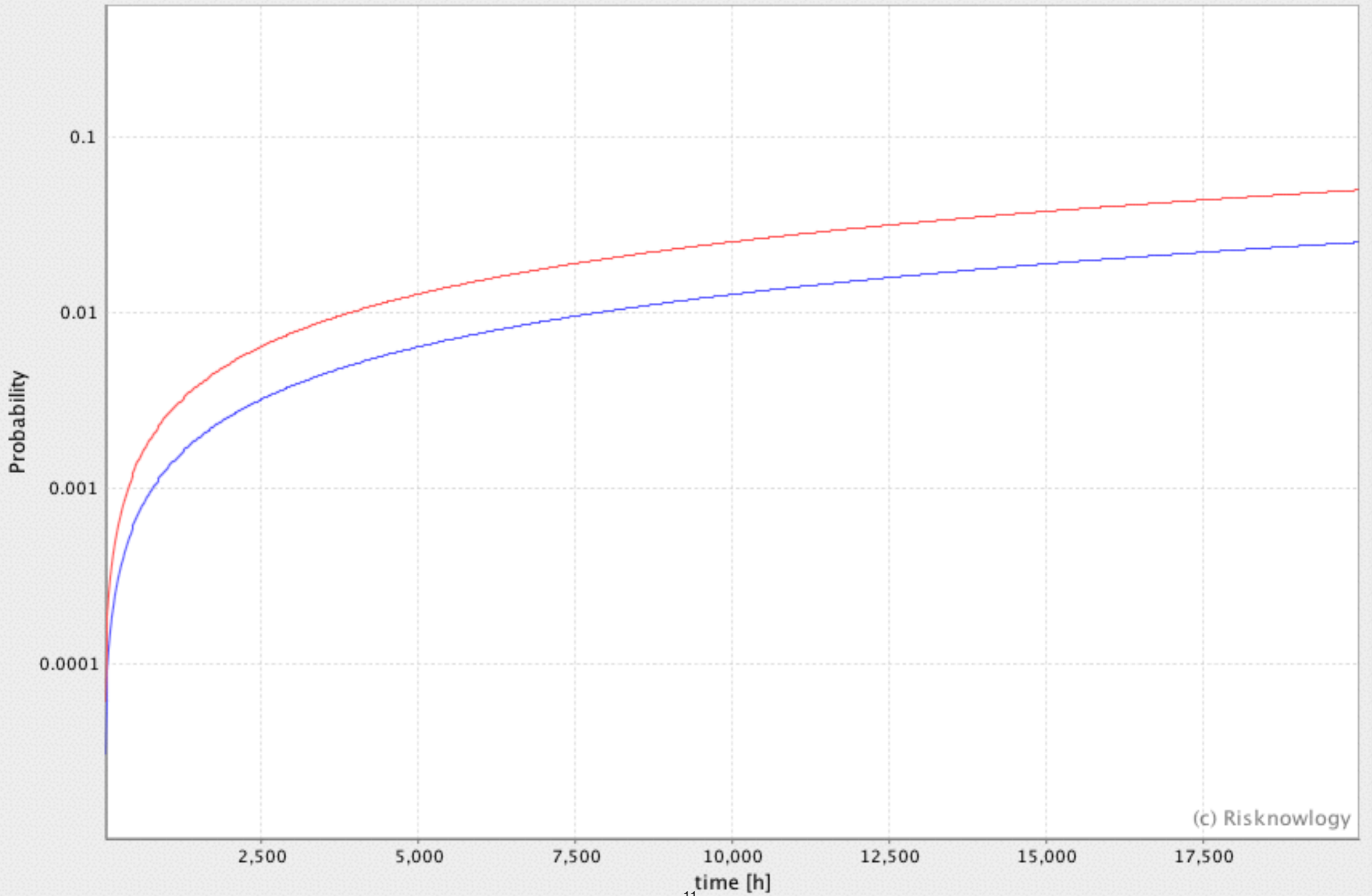
Don't forget the other SIL requirements - 1000 of them!

Proof Test - 100% or Partial

- ▶ We can carry out a proof test on
 - ▶ One individual device
 - ▶ On a combination of devices
 - ▶ On the complete safety loop

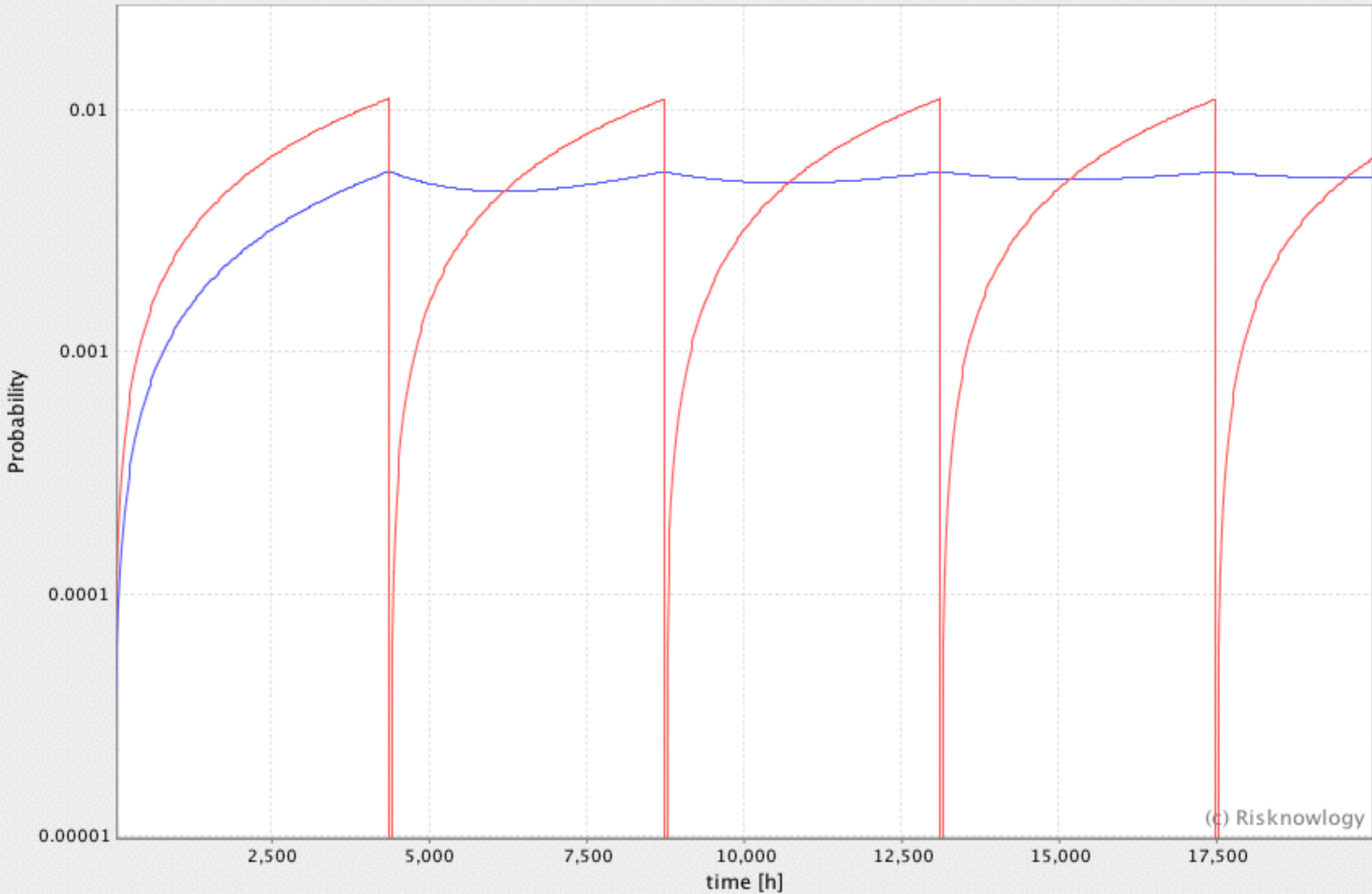


Fail Dangerous - No Proof Test



(c) Risknowlogy

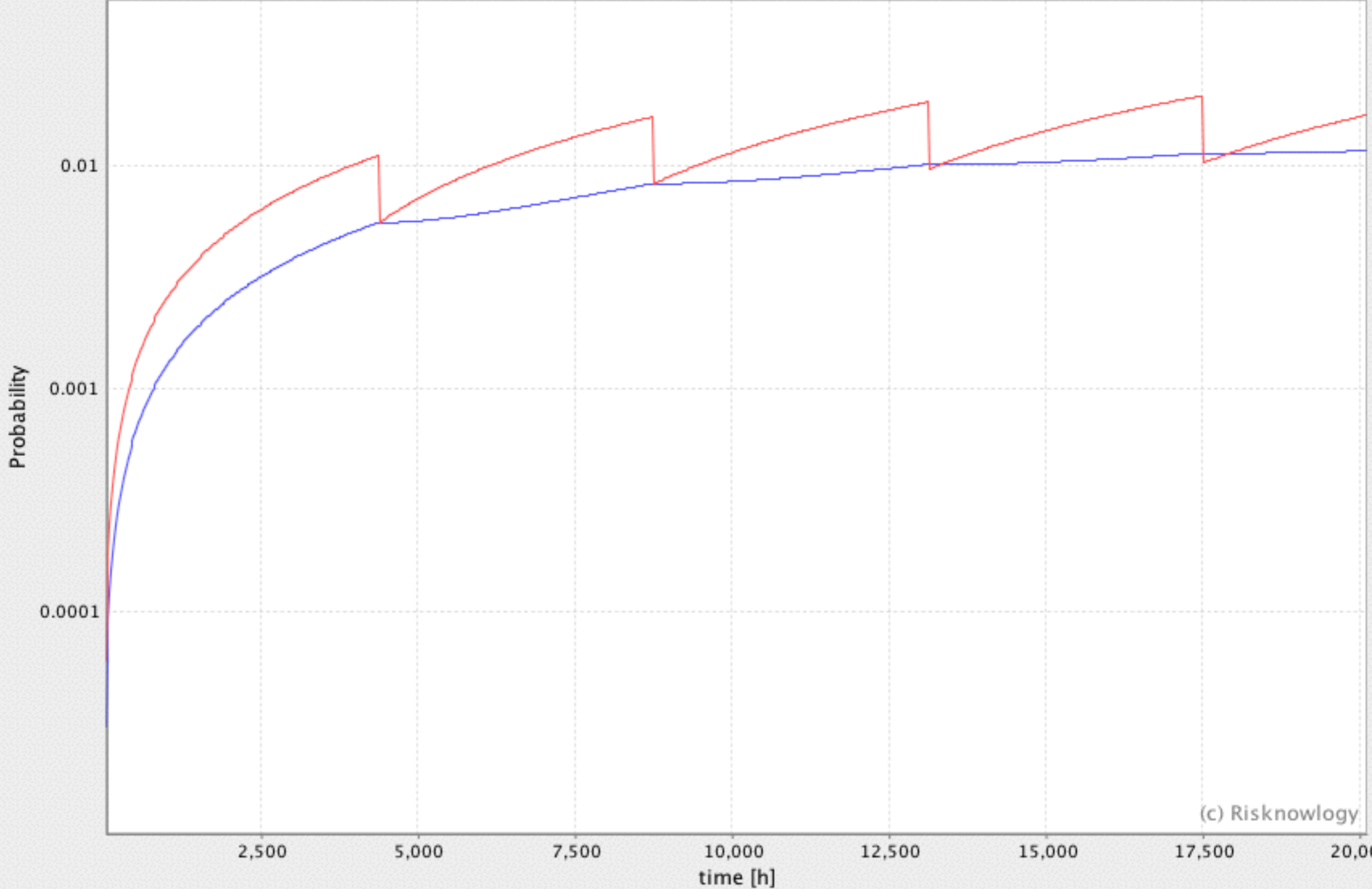
Fail Dangerous - 100% Proof Test - 6 Months



(c) Risknowlogy

Fail_Dangerous ¹²AVG(Fail_Dangerous)

Fail Dangerous – 50% Proof Test – 6 Months



(c) Risknowlogy

— Fail_Dangerous —¹³AVG(Fail_Dangerous)

Examples of “Simplified” Equations

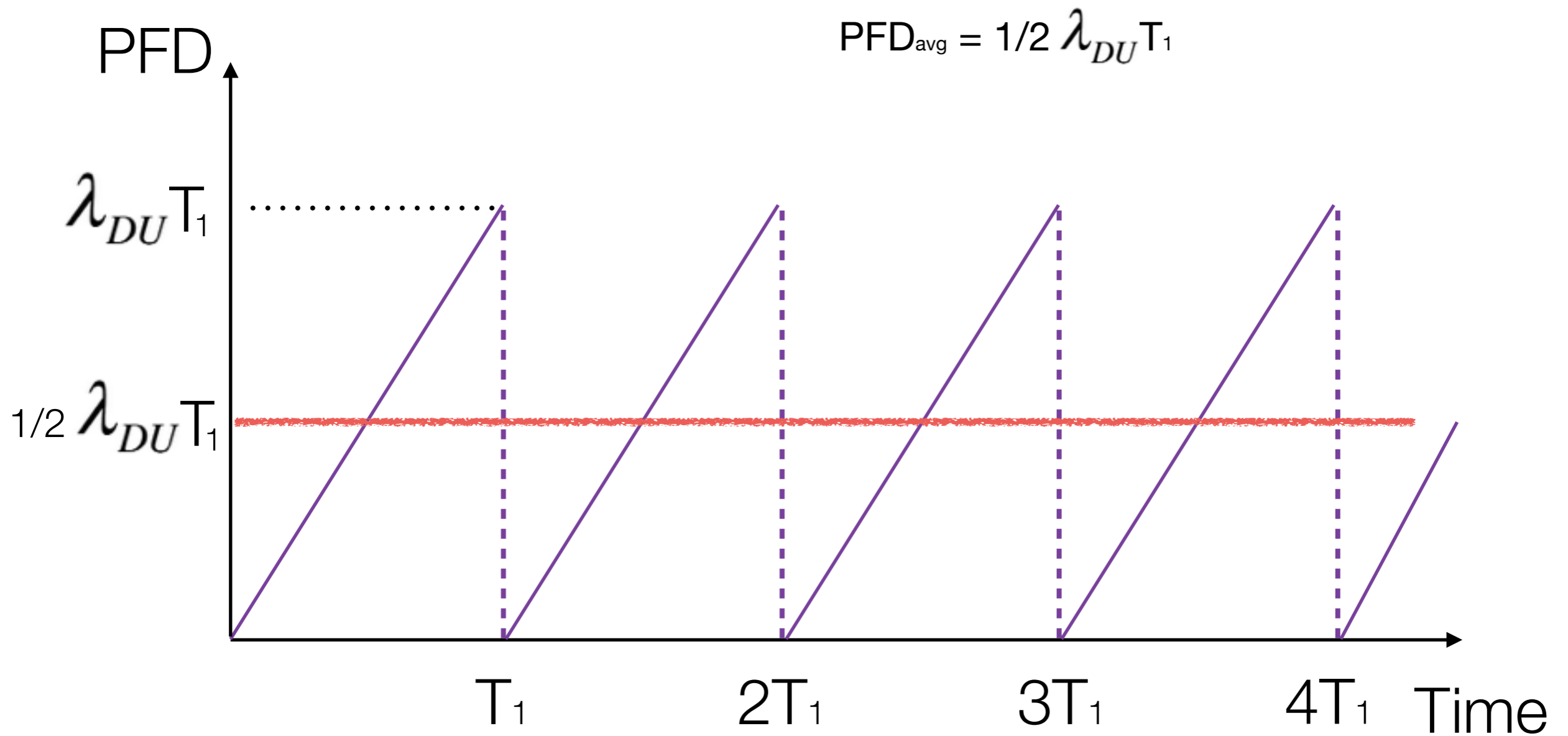
▶ 1001

$$PFD_{avg} = (\lambda_{du} + \lambda_{dd}) \cdot t_{CE}$$

▶ 1002

$$PFD_{avg} = 2 \left((1 - \beta_D) \lambda_{dd} + (1 - \beta) \lambda_{du} \right)^2 t_{CE} t_{GE} + \beta_D \lambda_{dd} MTTR + \beta \lambda_{du} \left(\frac{T_1}{2} + MTTR \right)$$

PFD simplified



Another look at the “Simplified” Equations

▶ 1001

$$PFD_{avg} = (\lambda_{du} + \lambda_{dd}) \cdot t_{CE}$$

$$PFD_{avg} = 1/2 \lambda_{DU} T_1 + \lambda_{DD} MTTR$$

$$\approx PFD_{avg} = 1/2 \lambda_{DU} T_1$$

▶ 1002

$$PFD_{avg} = 2 \left((1 - \beta_D) \lambda_{dd} + (1 - \beta) \lambda_{du} \right)^2 t_{CE} t_{GE} + \beta_D \lambda_{dd} MTTR + \beta \lambda_{du} \left(\frac{T_1}{2} + MTTR \right)$$

$$\approx PFD_{avg} = 1/2 \beta \lambda_{DU} T_1$$

Revealing Failures By Diagnostics

- ▶ A test is called a Diagnostic Test when that test
 - ▶ Is carried out automatically, AND
 - ▶ Is carried out frequently, AND
 - ▶ Is used to reveal failures that could jeopardise the safety function, AND
 - ▶ Results in an automated safe response
- ▶ Usually a diagnostic test is a “built-in” feature
 - ▶ For example a memory test, CPU test, watchdog, ...
 - ▶ Example analogue input module
- ▶ Normally designed according to 61508-2 and 61508-3



Safe Failure Fraction (SFF)

- ▶ A measure of the effectiveness of the **fail safe** design and **built-in diagnostic tests**
- ▶ It is calculated as follows:

$$SFF = \frac{\lambda_S + \lambda_{DD}}{\lambda_S + \lambda_{DD} + \lambda_{DU}}$$

- ▶ It is a design parameter, not an operational parameter
- ▶ It's not relevant to Proof Testing (except being based on some common data)

Through Normal Process Operation

- ▶ Revealing failures through normal process operations means that
 - ▶ The **process behaviour** on its own **reveals** the failure of the subsystem, for example
 - ▶ The factory shuts down due to a safe failure in the pressure transmitter, or
 - ▶ The vessel cannot be emptied due to a dangerous stuck close of the drain valve
- ▶ This way of revealing failures is not useful
 - ▶ Not from a safety point of view
 - ▶ Not from a process availability point of view

Revealing Failures By Proof Tests

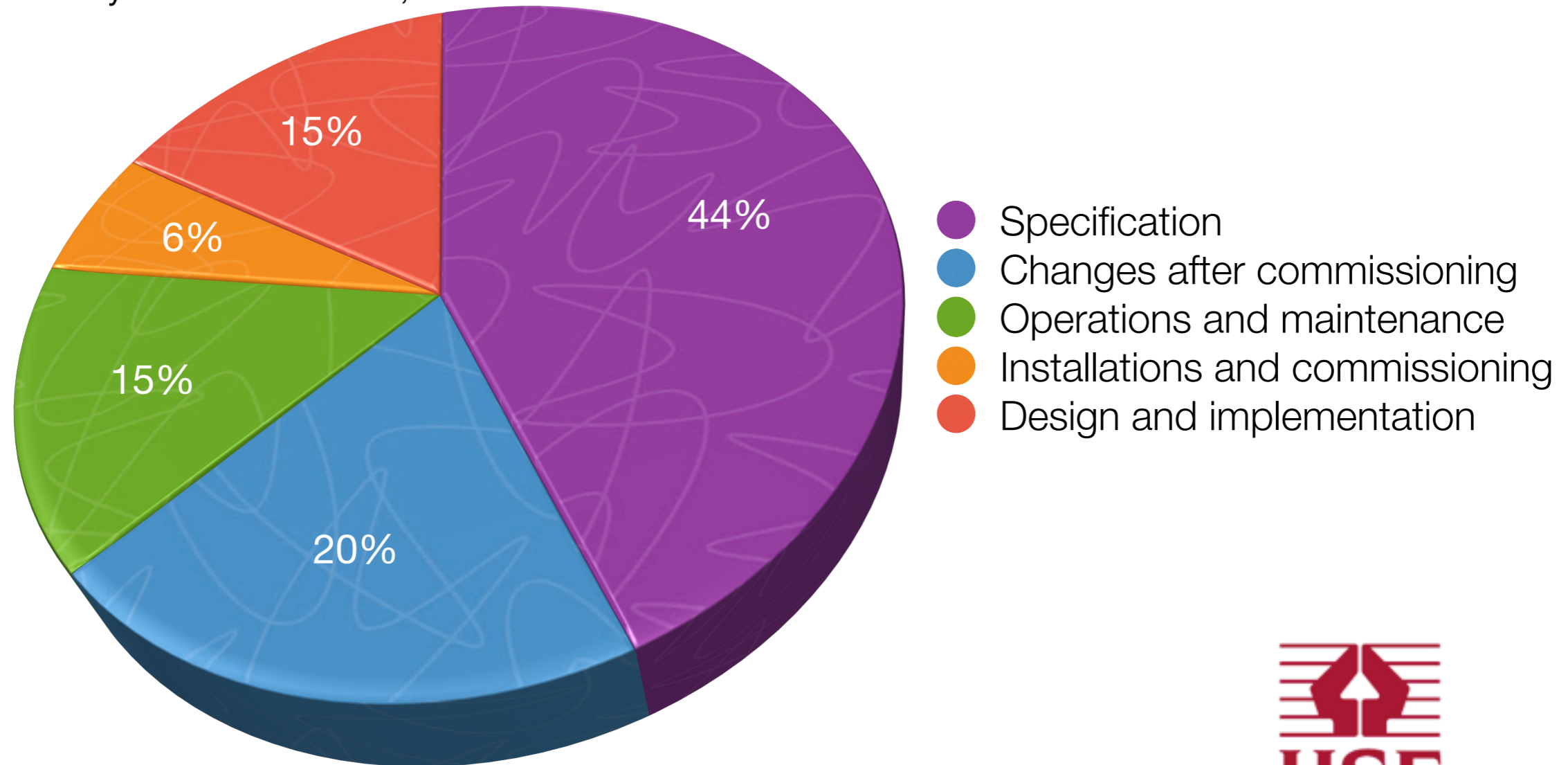
- ▶ All other tests are called Proof Tests.
- ▶ They are
 - ▶ Not automatic, OR
 - ▶ Their frequency is too low
- ▶ A proof test is
 - ▶ Initiated by human action
 - ▶ Usually not “built-in”, additional equipment is necessary to carry out the test
- ▶ For example an operator performs a Partial Stroke Test (PST) on a safety valve
- ▶ Note: not subject to the rules in IEC 61508 for development of H/W and S/W

Systematic failure example



Origin of failures

Analysis Of 34 Incidents, based on 56 causes identified



Out of control: Why control systems go wrong and how to prevent failure?
(2nd edition, source: © Health & Safety Executive HSE – UK)



Purpose of Proof Testing

- ▶ Finds Dangerous Undetected failures due to random hardware failures and common cause issues
- ▶ Random hardware failure rate measure is λ_{DU}
- ▶ But Proof Testing also finds
 - ▶ Early signs of common cause failure (like corrosion)
 - ▶ Actual common cause failure
 - ▶ Systematic failures
 - ▶ Safe undetected failures

Ideal Proof Testing

- ▶ Starts with the SRS
 - ▶ What does the Safety Function do?
 - ▶ How can you test it?
 - ▶ What is the test?
 - ▶ How will you by-pass valves?
 - ▶ How will you test multiple inputs?
 - ▶ How will you test multiple outputs?
 - ▶ How will you proof test without stopping the plant?
 - ▶ How will you provide “alternative means” of protection when testing a live plant?

If you don't ask (in the SRS), you won't get

Ideal Proof Testing Design

- ▶ Starts with the SRS - what is the safety function supposed to do?
- ▶ FAT and SAT should deliver basis of proof test
- ▶ On commissioning, have the instrument technicians write the proof test
- ▶ Have the instrument engineer verify it
- ▶ Or vice-versa, but peer review it as much as you can
- ▶ Carry out Human Factors Analysis
- ▶ Lots of pictures in the work instruction!
- ▶ Don't forget competence

How to Proof Test

- ▶ Permission to start a Proof Test from the Operator
 - ▶ Is this a good time?
 - ▶ Are you competent to do this?
 - ▶ Complete bypass log
- ▶ When proof testing, if you find a fault ...
 - ▶ Remember, you already have “alternative means” in place
 - ▶ You fix it, but fast
- ▶ Monitor the number of bypasses you have in place (weekly?)
- ▶ At company level record, analyse and periodically review all failures
 - ▶ Look for repeats, trends, patterns

Real plant data

- ▶ Very large plant
- ▶ 2 years of data
- ▶ A good example of good proof testing done well
- ▶ On “SHE” critical loops (mitigation and protection)
 - ▶ 87 failures
 - ▶ 34 dangerous detected, 55 dangerous undetected (until proof tested)
 - ▶ Of the 55
 - ▶ 30 Random Hardware Failures
 - ▶ 11 Common Cause (Environmental) Failures
 - ▶ 10 Systematic

Learning points from real plant data

- ▶ The undetected failure rate is similar to the spurious trip / detected failure rate
 - ▶ For every fault you know about, there's one you don't
 - ▶ And it means your Safety Function will never work
- ▶ Beta factor = 25%
 - ▶ Probably not, as could be Systematic, but it's not 1%
- ▶ Proof testing interval is set by PFD (Random + Common Cause)
 - ▶ But it catches Systematic too
 - ▶ Here Systematic was 20% of all failures
 - ▶ And maybe higher if Common Cause failures actually Systematic

Proof Test Interval

- ▶ Proof test interval selection
 - ▶ Any laws?
 - ▶ Manufacturer data / safety manual
 - ▶ interval might be very short (never mind what SIL it is)
 - ▶ power cycle a logic solver (only way to test diagnostics?)
 - ▶ Proof test interval by calculation (you have to anyway)

Proof Test Design

- ▶ Proof test design
 - ▶ I wouldn't start from here if I was you
 - ▶ Look at how you can implement partial proof testing
 - ▶ Be skeptical about any claims of diagnostic coverage
 - ▶ The manufacturer's data is unlikely to help with % figures
 - ▶ Don't be afraid of estimating coverage yourself
 - ▶ Just be conservative

Is a Demand a Proof Test?

- ▶ If you have a demand
 - ▶ Did the safety function work correctly?
 - ▶ Was it a functional test or a proof test (multiple inputs)
 - ▶ If it was only a functional test, can you analyse it to prove it was a proof test
 - ▶ And document it, or it doesn't count

The Future of Proof Testing

- ▶ More and more automated
- ▶ Designed in
 - ▶ so (probably) compliant with 61508-2 and 61508-3
 - ▶ or part of the application programme - compliant with 61511
- ▶ If it runs fast enough and acts automatically
 - ▶ it's diagnostics
 - ▶ so λ_{DU} is lower
 - ▶ which means longer proof test intervals
- ▶ But what about the systematic and common cause failures?
- ▶ Document what you want in the SRS
- ▶ Train Instrument Technicians for SIL like we do for ATEX

Future tasks

- ▶ How you calculate PFD (and proof test intervals) with partial proof testing
- ▶ How you calculate Beta factor
- ▶ Develop Instrument Technician Competence training (**SILComp**)
- ▶ For articles on these topics and others www.risknowlogy.com
- ▶ To ask your own questions rgb@risknowlogy.com



Proof Testing

www.risknowlogy.com

or contact

rgb@risknowlogy.com

Functional Safety 2014

Title: Functional safety – Team of individuals of Individual team?

Abstract

The paper will look at the bigger picture where functional safety covers the various boundaries in organizations, and responsibilities for functional safety. It will show that it is not a team of individuals but an individual team.

Introduction

The title of this paper is like that of a football team. The best success comes from all players knowing their role and boundaries, when to pass, and having the spatial awareness to react when they receive the ball.

The football manager may have the capability, but if one or more in the team does not have the required skill set and motivation then the ball may be lost. In Functional Safety it is also key to have people who understand and can apply the right skills and practices throughout the organization, as not having these may lead to incorrect or dangerous situations.

In a football game the worst result is losing a match, which is likely to have a cost and reputational impact. In Functional safety the consequences may and are most likely to be more severe, including harm to people.

In football a well meant intention may impact on the consequences. For example David Luiz's headed clearance that resulted in The Netherlands second goal. If he could repeat the situation do you think we would take the same course of action? In this instance, although Brazil was beaten David Luiz had the rest of the game to redeem himself.

In Functional safety a well meant intention may be followed by a stronger punishment or consequence without the opportunity to amend the wrong.

The purpose of this paper is to show that "well meant intentions" may not deliver the intent of the IEC Standards, or even Company Standards. However, the correct implementation of IEC 61508 / 11 at each phase will.

The paper will highlight the positions and levels of competences required by the different parts within the functional safety processes. Functional safety processes consist of the life-cycle from customer identification of a requirement, through the supply chain in delivering this requirement for safety functions, to the life-cycle management of functional safety when in service, and through later life modifications or decommissioning.

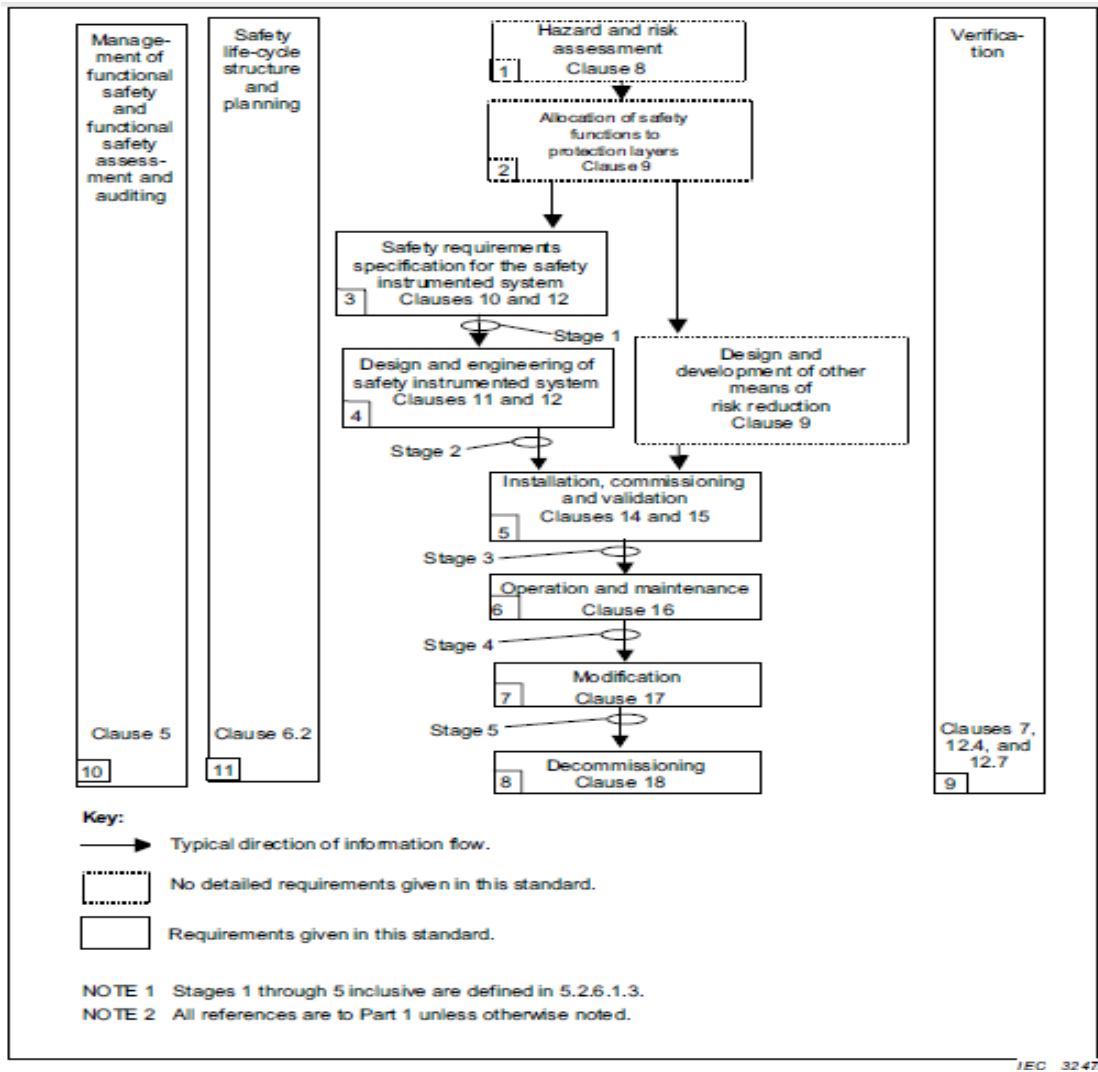
The “supply chain” is the parties involved in delivering and not just supplying safety systems. That is; the customer, the design house, the equipment manufacturer, the installer, the commissioner, the operator.

IEC 61511 Part 1 Clause 4 “Conformance to this International Standard” states;

“To conform to this International Standard, it shall be shown that each of the requirements outlined in Clauses 5 through 19 has been satisfied to the defined criteria and therefore the clause objective(s) has (have) been met.”

Figure 1 (copy of IEC-61511 Figure 8 – SIS safety life-cycle phases and functional safety assessment stages) shows the Safety Instrument System (SIS) safety life-cycle phases and functional safety assessment stages, which highlight the connectivity of the various parts in the process.

Figure 1: SIS safety life-cycle phases and functional safety assessment stages



Disclaimer: The content in this paper is loosely based on experiences, and have been embellished to bring out the salient points against the objectives of this paper.

As an end user does your company have or employ the organizations, processes and competences that directly maps to Figure 1? Or as an end user does your company have or employ the organizations, processes and competences that may map those in Figure 1?

Note the question did not focus on projects as Figure 1 covers all stages and life-cycle. For projects only a few of the clauses are covered, typically clauses 5 through 15, but can include clauses 17 and 18. For end users all clauses apply.

As an end user are all the clauses applicable to you?

Discussion

For Greenfield (e.g. a new site) the clauses 5 through 15 usually have more than one company, organization or disciplines involved. That is the end user identifies the project requirement and may contract out to an EPC (Engineering Procurement contractor) for the design and maybe another contractor for the construction. As SIS is part of Functional Safety there are multi-disciplines involved in these companies. There is also the equipment manufacturers' who must meet the requirement specification.

There are international standards such as IEC 61511, and others, and possibly end user company standards.

All this provides multiple interfaces and information transfer that require to be managed. Back to the football analogy, if the ball is not under your control and you try to pass it then it may not go where you intended.

Whilst there are multiple interfaces and complexity for Greenfield projects these generally can be easily managed for delivering Functional safety.

Modifications and decommissioning brings other challenges. Modifications can be from small changes to Greenfield projects adding to Brownfield processes. It can also include elements of decommissioning where the equipment for decommissioned functions is re-used with changed functionality.

Modifications has similar multiple interfaces, standards etc. as for Greenfield, but with added interfaces and complexities with connections to the Brownfield equipment and from operational constraints.

The intent of the following case studies is to show where things can go wrong, and where it could be said it was a team of individuals and not an individual team.

Case 1: Loss of containment detection from low pressure detection

Some international standards suggest the use of low pressure detection for the identification of loss of containment from leaks.

Project that are being engineered may include this detection to be installed, such as to meet the requirements of these standards. The SIL determination analysis identifies when low pressure detection is not appropriate for leak detection, and projects either change designs, or if too far into design continue and accept the ineffective functions.

It provokes the question is leak detection activated by low pressure common sense or fallacy?

Extracts from one standard for pressure vessels and for pipelines are:

Pressure Vessels

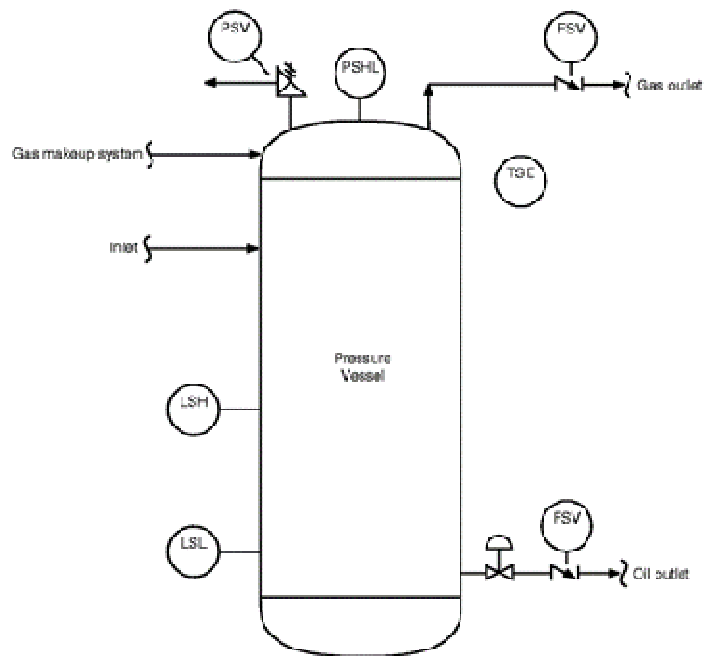
A pressure vessel should be provided with a PSL sensor to shut off inflow to the vessel when leaks large enough to reduce pressure occur, unless PSL sensors on other components will provide necessary protection and the PSL sensor cannot be isolated from the vessel when in service.

Undesirable Event

= Leak

Detectable Abnormal Condition at Component

= Low pressure



Pipelines

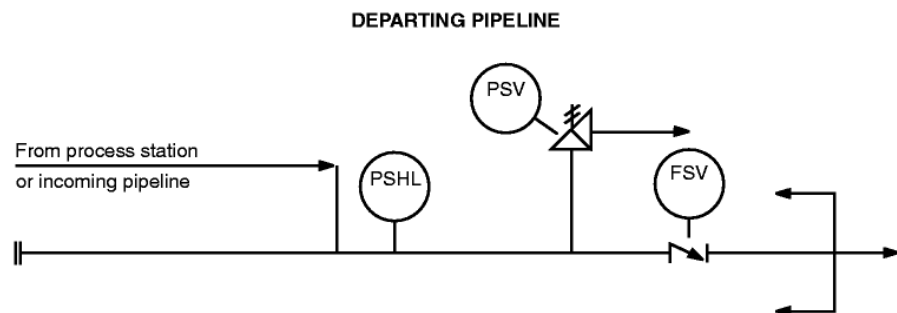
PSH and PSL sensors are required on departing pipelines to shut off all input sources.

Undesirable Event

= Leak

Detectable Abnormal Condition at Component

= Low pressure



For these two examples of using low pressure as leak detection how many HAZARDOUS states would be detected?

Low pressure detection is unlikely to detect fugitive or small releases, and also may not detect reasonably large releases.

Disclaimer: The content in this paper is loosely based on experiences, and have been embellished to bring out the salient points against the objectives of this paper.

If the HAZARD is toxic gas such as H₂S and the concentration in the process stream is high, then even small releases may have severe consequences.

If release is liquid and non-toxic or hazardous (e.g. water), then smaller releases may be acceptable and only significant leak rates that trip or upset the process are to be considered for detection.

If the release is liquid and hydrocarbon, then what release size could be tolerated before leading to a hazardous event? This should be analysed, and maybe even modelled, to determine acceptable limits.

If the release is flammable gas, then what events would low pressure detect? For a pipeline even a catastrophic release close to the feed source may not be detected by low pressure detection located at the feed source.

Low pressure detection may have a role to play in process safety, but each application should be based on the hazard and the ability to detect the hazard.

Standards that provide guidance that is towards prescriptive methods may miss the real hazard, and as such may give the end user a false sense of safety.

The summary of this case study is that:

1. Know your hazard, and always carry out Hazard and Risk assessment.
2. When leak detection is required the allocation of the safety function should consider:
 - a. the best detection method
 - b. the detection time, and
 - c. the response action
3. Use Standards wisely. Do not always blindly follow!

Case 2: Installed and commissioned functions that impacted integrity

This case covers a couple of examples where installed functions impacted integrity.

Project 1: Greenfield added to Brownfield

A new outlet facility was added to a site to transfer fluids to another location. This is a Greenfield (new facility) that required shut down interfaces with Brownfield (existing facilities).

The new facilities have Emergency Shutdown (ESD) isolation valves to box in the inventory, a depressurization blow down valve, high wattage pumps, and local manual ESD stations.

The Brownfield installation used dual trip circuits that each used an energized to trip solenoid valve for tripping closed the ESD shutdown isolation valves, and the depressurization via blow down valves. This requirement was due to relief systems inventory limits which meant the whole plant could not be depressurized at same time, and staggered blow down required.

The new facilities were designed and engineered by an Engineering Procurement Contractor and installed as per the design. This included quality control and checks at various stages, including FAT, and commissioning before handing over to site for operations.

What is missing?

Two years later another Greenfield/Brownfield project was to change out the existing ESD logic system with a newer ESD logic system, including expanded for additional processes.

During the changeover of the ESD logic system a requirement was to review and check out all interfaces, such that a smooth and uneventful change-over could be implemented without shutting down the process. The system being energise to trip the outputs (ESD valves etc.), and via two separate routes, enabled the project to plan changing over one channel at a time. There would be a limited period when the ESD system would have only one channel to trip the ESD valves etc., hence the rigor required in the execution planning and on validating output actions.

During the development works for the change-over method the investigation into existing functionality it was identified that some ESD functions would never have worked, as they had field wiring into the termination cabinet but no internal wiring to the ESD system.

Oops what went wrong with first project?

All Greenfield functions had been tested, including FATs, and proven to work from the new cabinets and new equipment.

It appears that the ESD functions were not tested from the existing ESD system. An obvious statement based on what was found.

IEC 61511 Part 1: 14 SIS Installation and Commissioning

14.1 Objectives

14.1.1 The objectives of the requirements of this clause are to

- Install the safety instrumented system according to the specifications and drawings;
- Commission the safety instrumented system so that it is ready for final system validation.
- etc.

14.2.3 The safety instrumented system shall be commissioned in accordance with planning in preparation for the final system validation. Commissioning activities shall include, but not be limited to, confirmation of the following:

- Earthing (grounding) has been properly connected;
- Energy sources have been properly connected and are operational;
- Transportation stops and packing materials have been removed;
- No physical damage is present;
- All instruments have been properly calibrated;

Disclaimer: The content in this paper is loosely based on experiences, and have been embellished to bring out the salient points against the objectives of this paper.

- All field devices are operational;
- Logic solver and input/outputs are operational;
- The interfaces to other systems and peripherals are operational.

The summary of this case study is that Greenfield / Brownfield:

1. Design must include Functional safety assessment of designs to review all interfaces with Brownfield systems.
2. Installation, commissioning, and validation testing must include testing all interfaces with the Brownfield systems, with activation of relevant shutdown levels.

Project 2: Modifications/ Decommissioning

During a routine process shutdown test only a small proportion of the process had shut down. The process had to be manually shut down. The process was shut down for circa 3 days before the cause was identified and rectified, which had a direct cost of in excess of £3M.

One year earlier the shutdown system had operated as required.

The initial site investigation identified modifications had been carried out on the system. All of which had been installed and their functionality tested, and brought into service, and functionally operated as per design.

Thus it appeared that cause of failure in the shutdown system was not from modification, and further investigation into components started.

The further investigation added the technical authority and the system vendor to the team. The team revisited each of the modification packs including the as built drawings.

One of the designed modification had to be changed during the implementation as the design assigned input module had been used by another change. The installation used another input module that had been previously decommissioned. This change to the design had been tested and the designed function for this change had functioned as per design with the correct effects. No issues were found or evident, however as was seen later this modification had a massive effect on the capabilities of the shutdown system.

IEC 61511 Part 1 clauses 17 (Modifications) and 18 (Decommissioning) are very small in relationship to the rest of the standard, but have clear messages about **approvals** and **safety integrity of the SIS is maintained despite of any changes made to the SIS**.

The investigation identified that the decommissioned module had not been fully decommissioned as wires had been left on the backplane. The modification for the new design that now used this module added a 24V feed to one of the backplane pin, which in course tied the shutdown rail to a permanent

Disclaimer: The content in this paper is loosely based on experiences, and have been embellished to bring out the salient points against the objectives of this paper.

power source. The modification installed had been fully tested and operated as a stand-alone function as it did not require the shutdown line as part of the function, and hence the fault introduced to the shutdown system was not picked up.

The summary of this case study is that:

1. No on-site changes to a design should be undertaken without a full review of the proposed change.
2. When decommissioned components are used a physical review of the as built/left state must be ascertained before adding these components to a design.

This case shows that a well meant intention during the installation by using another decommissioned module added a hazard into the safety system.

Case 3: Experience vs Competence

A small site did not have an Instrument Engineer. A change was being implemented on part of their shutdown system with some new sensors and associated shutdown logic. This change had been designed by a large engineering procurement contractor, who produced installation and site acceptance testing documentation to be used.

The implementation of this change was through a local based company. The end user did not have an instrument engineer but also had a project engineer. The end user project engineer was reliant on the very experienced contractor supervisor, who overseen the installation and commissioning.

What could go wrong?

An independent functional safety assessment stage 3 post commissioning identified that the installation and commissioned systems had gaps against the designed requirements. There were gaps in management, documentation and on SIF capabilities. Typical findings were:

1. The developed Site Acceptance Testing (SAT) and Commissioning procedures were not used by the installation contractor.
2. There was no evidence of full quality procedures used for installations and commissioning, and thus no completion or commissioning dossier available.
3. The test documentation available was sparse and did not provide evidence of testing of all installed equipment. Such as; no installation quality assurance inspection certificates, some of the continuity and earth test certificates for the instrument cable not dated, no continuity and earth test certificates for the power cable, no installation inspection certificates, etc.
4. There were no drawings (e.g. red lined or as-built) available on site.
5. There were calibration issues for the new radar level sensors, with different ranges and zero datum points for same tank.
6. The tank has a voted 1oo2 level sensors, but the level trip settings on each sensor was different.

The following extract from IEC 61511 part 1 indicated minimum requirements.

IEC 61511 Part 1: 5.2.2 Organization and resources

5.2.2.1 Persons, departments, organizations or other units which are responsible for carrying out and reviewing each of the safety life-cycle phases shall be identified and be informed of the responsibilities assigned to them (including where relevant, licensing authorities or safety regulatory bodies).

5.2.2.2 Persons, departments or organizations involved in safety life-cycle activities shall be competent to carry out the activities for which they are accountable.

NOTE As a minimum, the following items should be addressed when considering the competence of persons, departments, organizations or other units involved in safety life-cycle activities:

- a) Engineering knowledge, training and experience appropriate to the process application;
- b) Engineering knowledge, training and experience appropriate to the applicable technology used (for example, electrical, electronic or programmable electronic);
- c) Engineering knowledge, training and experience appropriate to the sensors and final elements;
- d) Safety engineering knowledge (for example, process safety analysis);
- e) Knowledge of the legal and safety regulatory requirements;
- f) Adequate management and leadership skills appropriate to their role in safety life-cycle activities;
- g) Understanding of the potential consequence of an event;
- h) The safety integrity level of the safety instrumented functions;
- i) The novelty and complexity of the application and the technology.

The summary of this case study is that:

1. Experience may not make one competent.
2. Competence is required for all life-cycle parts, disciplines and companies.
3. Have and follow the quality plan, without exception.

Overall Summary

This paper through a few examples shows that:

1. Functional safety covers various boundaries in organizations, and responsibilities that require managing such that interfaces are seamless and robust.
2. For success it should not be a team of individuals but an individual team.

References

IEC 61511 International Standard, Functional safety – Safety instrumented systems for the process industry sector – Part 1, 2 and 3, International Electrotechnical Commission

API Recommended Practice 14C, Recommended Practice for Analysis, Design, Installation, and Testing of Basic Surface Safety Systems for Offshore Production Platforms, American Petroleum Institute

Author

Robert (Bob) Nicol

Nicol Instrument Engineering Limited

Bob has been in the process industry, mainly oil and gas, for over 46 years. He has held roles with design engineering contractors and end users at engineering or senior engineering roles, consultant, technical authority and subject matter expert.

Whilst IEC 61508 and IEC 61511 are relatively new standards and now considered good practice, all career roles have has some form of Functional safety to some standard.

List of companies worked for includes; BP, Shell, Crawford and Russell Inc., Ralph M Parsons, Borg Warner, Smith and Taylor, South Scotland Electricity board.

Functional Safety *2014*

Team of individuals or
Individual team?

Nov 2014

Robert (Bob) Nicol
Nicol Instrument Engineering Limited

Topics

- * **IEC 61511 requirements**
- * **Team of individuals or Individual team?**
 - * *Case 1: Loss of containment detection from low pressure detection*
 - * *Case 2: Installed and commissioned functions that would never work*
 - * Project 1: Greenfield added to Brownfield
 - * Project 2: Modifications/ Decommissioning
 - * *Case 3: Experience vs Competence*
- * **Summary**

Disclaimer

The content in this paper is loosely based on experiences, and have been embellished to bring out the salient points against the objectives of this presentation.

IEC 61511 requirements

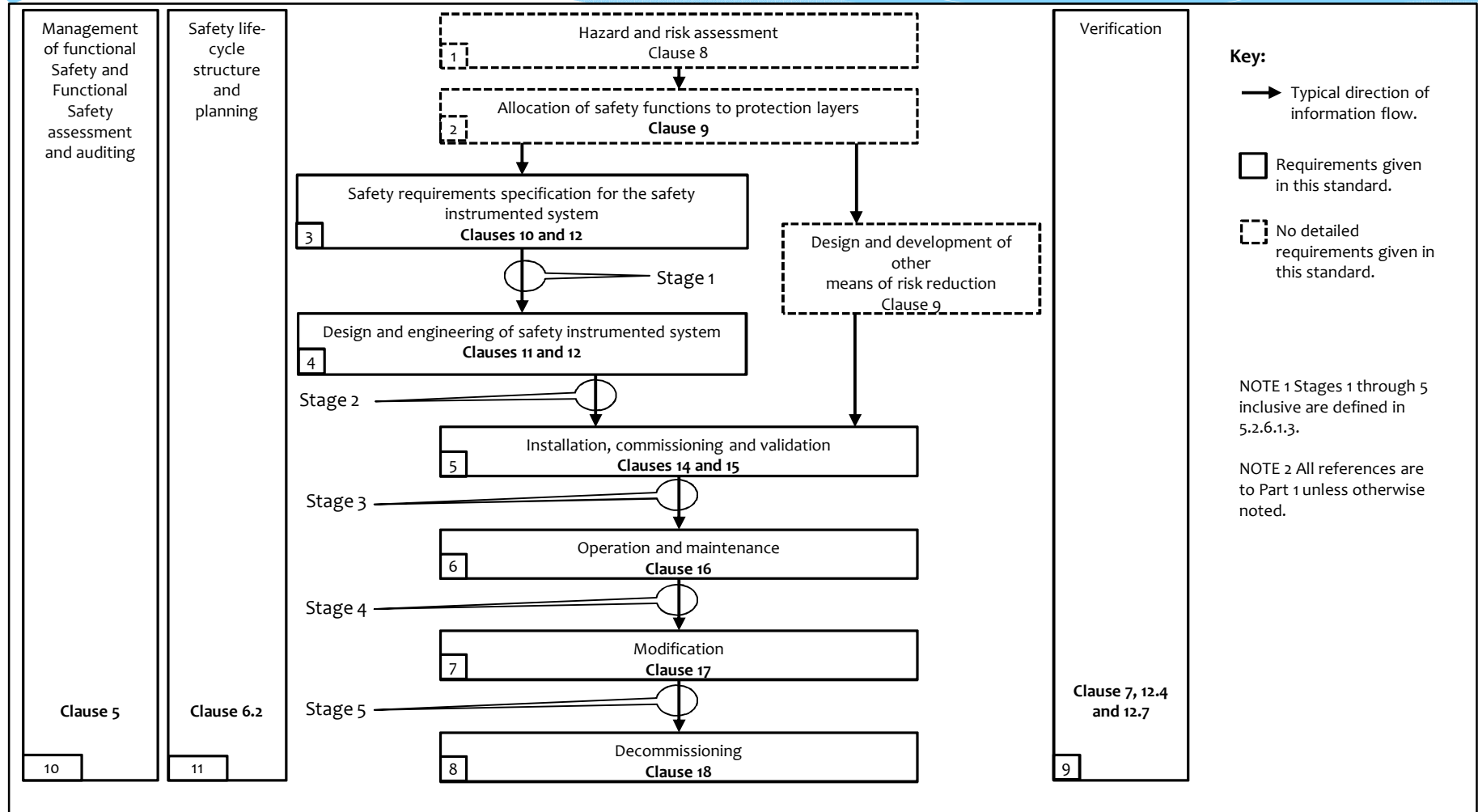


IEC 61511

To conform to this International Standard , it shall be shown that each of the requirements outlined in **Part 1** Clauses 5 through 19 has been satisfied to the defined criteria and therefore the clause objective(s) has(have) been met.

IEC 61511 Part 1

Figure 8 – SIS safety life-cycle phases and functional safety assessment stages



Poll

- * Does your company have a Functional Safety Plan?
- * Does your company's organisation and processes map with IEC61511 Figure 8?

**Team of individuals or
Individual team?**

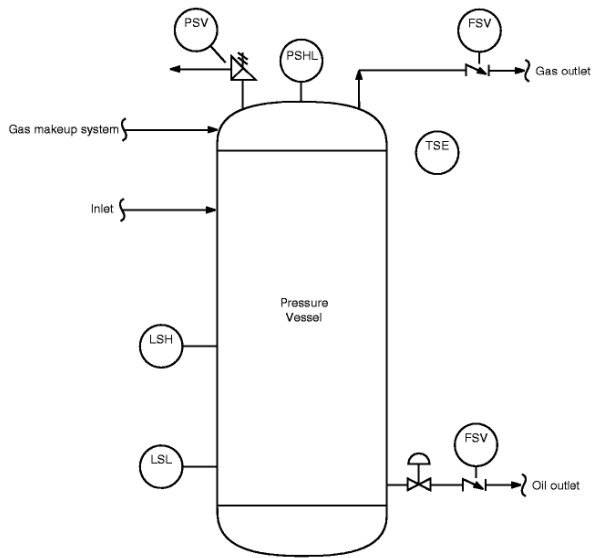
Case 1:

*Loss of containment detection
from low pressure detection*

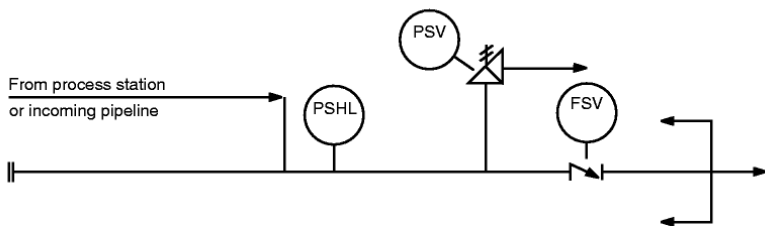
Poll

- * How many use low pressure detection for identifying leaks?

API 14C typically in SAT tables



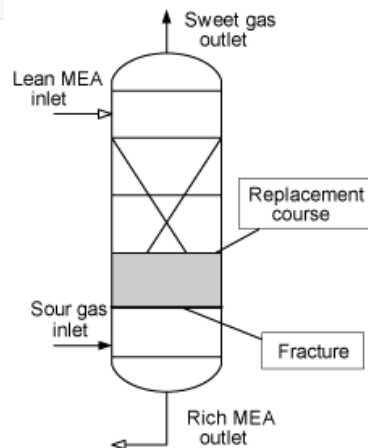
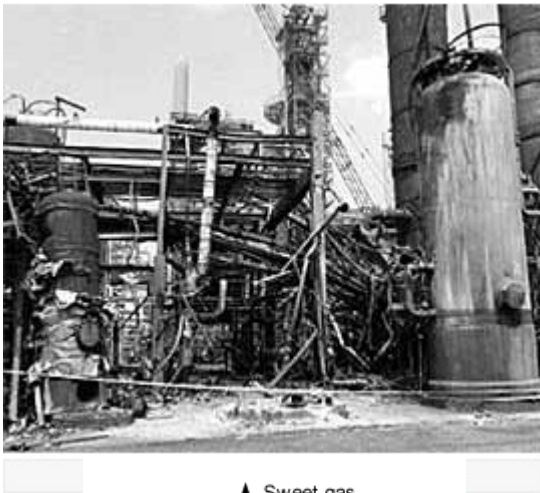
DEPARTING PIPELINE



Undesirable Event	Cause	Detectable Abnormal Condition at Component
Leak	Deterioration Erosion Corrosion Impact damage Vibration	Low Pressure

Pressure vessel example

Amine absorber column failure



- * 23 July 1984, an Oil refinery, Illinois, suffered an explosion and a fire.
- * Seventeen people were killed.
- * Damage was estimated to be over \$100 million.
- * Explosion caused by the ignition of a propane and butane cloud that had leaked from the vessel.
- * Prior to the explosion an operator noticed gas escaping from a horizontal crack near the bottom of the vessel.
- * The crack grew and he initiated evacuation of the area.
- * As the fire fighters arrived, the column cracked further and a large amount of gas was released.
- * The gas ignited and the explosion sent the upper part of the tower into the air, landing over a mile away.
- * **How effective would low pressure detection have been ??**

Pressure vessel example



RUPTURE HAZARD OF PRESSURE VESSELS

- * In a 1996 accident, three workers were killed and a number of others were injured.
- * Vessel containing air and water.
- * After a number of years of service, the vessel developed a pin-hole leak. The leak was repaired but not in adherence with recognized codes.
- * A month later, the vessel failed catastrophically at the weld area. The vessel ripped apart and rocketed through the roof.
- * **How effective would low pressure detection have been ??**

Pipeline example

1988: Oilfields crippled after storage ship drifts

North Sea oil production has been dealt another blow just five months after the Piper Alpha disaster.

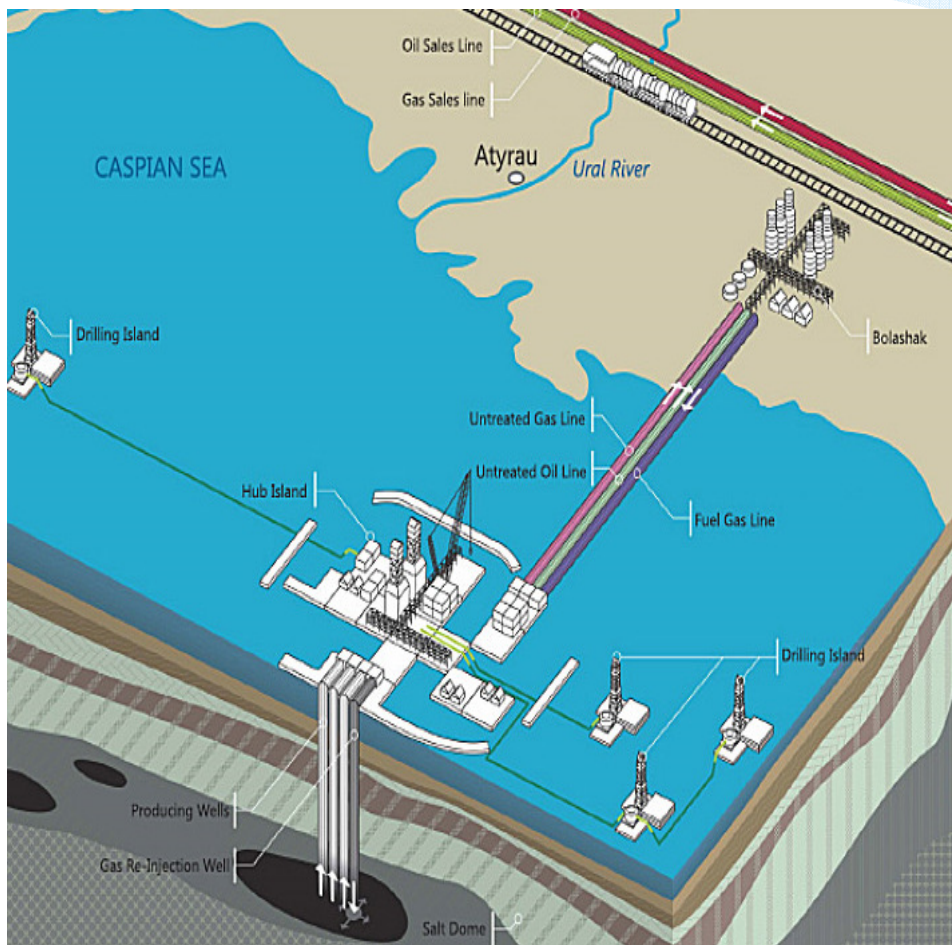
Three North Sea oil fields have been shut down after a giant floating storage vessel, the Medora, broke free of its moorings in gale-force winds.



- * 25 December 1988 the Fulmar FSU (Floating Storage Unit) broke loose from its moorings.
- * Approximately 1,300 tons of oil were spilled following the incident.
- * Transfer line had pressure detection with low pressure trip – this did not trip the product transfer.
- * **How effective was the low pressure leak detection ??**

High pressure – High H₂S

Low pressure leak detection ???



Case 2:

*Installed and commissioned
functions that impacted
integrity*

Project 1: Greenfield added to Brownfield

Project 2: Modifications/ Decommissioning

Project 1: Greenfield added to Brownfield

- * A new outlet facility was added to a site to transfer fluids to another location.
- * Brownfield installation used dual trip circuits that each used an energized to trip.
- * New facilities were installed as per the design, had quality control and checks at various stages, including FAT, and commissioning before handing over to site for operations.
- * **What could go wrong ??**

Project 1: Findings

- * The new Greenfield functions, tested in isolation of Brownfield, accepted as functioned as designed.
- * Full function test of Brownfield to Greenfield not carried out.
- * New facilities ESD functions were not connected to the ESD shutdown system.
- * Result was the ESD functions would never have worked on demand.

Project 2: Modifications/ Decommissioning

- * Annual routine testing of shutdown ESD system.
- * **What could go wrong ??**
- * Only part of process shut down.
- * Plant had to be manually shut down.
- * Investigation took 3 days, and production lost during this time.
- * If a real demand then massive failure of ESD system.

Project 2: Findings

- * A small project design was changed on site.
- * Site change used a decommissioned module.
- * The modification was tested and worked.
- * ESD functionality was not tested as not part of the small project modifications.
- * The decommissioned module had a connection to ESD rail, which was not identified on drawings or during wiring changes.
- * Result was that the change prevented the ESD system from functioning.

Poll

- * Does your company practices for Greenfield /Brownfield include review of interfaces ??
- * Does your company have full function testing including Brownfield to Greenfield ??

Case 3:
Experience vs Competence

Project outline

- * Small site with no Instrument Engineer.
- * Change being implemented on part of their shutdown system.
- * The design by a large engineering procurement contractor (EPC).
- * EPC supplied installation, commissioning and site acceptance testing (SAT) documentation.
- * Installation and implementation through a local based company.
- * Local based company had very experienced supervisor, who overseen the installation and commissioning.
- * **What could go wrong?**

Findings

- * The EPC supplied documentation for installation, commissioning and site acceptance testing (SAT) not used.
- * Full installation quality control, testing and commissioning dossier not available. Such as:
 - * Documentation available was sparse and did not provide sufficient evidence of testing of all installed equipment;
 - * No installation quality assurance inspection certificates;
 - * Some continuity and earth test certificates for the instrument cable not dated;
 - * No continuity and earth test certificates for the power cable;
 - * No as-built drawings (e.g. red lined or as-built available on site).
- * The level voting was 1002 sensors, but the level trip settings on each sensor was different and at wrong settings.
- * There were calibration issues for the new radar level sensors, with different ranges and zero datum points used for same tank.

Summaries

Case study Summaries

- * Case study 1: Leak detection:
 - It is not always possible with low pressure detection.
 - Know the hazards.
 - Select most appropriate detection method.
- * Case study 2: Project 1
 - Design must include Functional safety assessment of designs to review all interfaces with Brownfield systems
 - Installation, commissioning, and validation testing must include testing all interfaces with the Brownfield systems, with activation of relevant shutdown levels.

Case study Summaries

- * Case study 2: Project 2
 - No on-site changes to a design should be undertaken without a full review of the proposed change.
 - When decommissioned components are used a physical review of the as built/left state must be ascertained before adding these components to a design.
- Case study 3:
 - Experience may not make one competent.
 - Competence is required for all life-cycle parts, disciplines and companies.
 - Have and follow the quality plan, without exception.

Overall summary

- * Functional safety covers various boundaries in organizations, and responsibilities that require managing such that interfaces are seamless and robust.
- * For success it should not be a team of individuals but an individual team.

Thank you

Application software integrity: is your logic solver as reliable as you think?

Neil Wakeling BA MA CEng FInstMC MIET (CFSE),
Group Technical Authority for Functional Safety and ICSS, SBM Offshore, Monaco

Abstract

The logic solver is generally by far the most reliable part of a Safety Instrumented Function in terms of random hardware failures. However, the largest source of failures is likely to be systematic factors, often dormant errors, discrepancies or forces in the application software not detected during the safety system validation, or introduced during the start-up or operations phases. Whilst IEC61511 addresses application software in some detail, including via the implementation of a code review performed prior to plant start-up, it's certainly not correct to say that once validated, the logic solver needs no further attention. The challenges of maintaining the integrity of safety application software is a point not lost on some national regulators and major oil companies who prohibit software-based systems for certain high integrity protection systems.

This paper draws on the experience of safety logic code reviews conducted across the world's largest fleet of FPSOs, covering Process Safety, but also Fire and Gas and Emergency Shutdown systems where particular considerations apply. It focuses on methods for eliminating errors before plant start-up, and how to maintain the integrity of application software during the longest phase of the safety lifecycle: operation. A comprehensive set of procedures throughout the project execution, operation and indeed brownfield modification stages of the lifecycle is needed to reduce the chances of safety reliability being impacted. Without such measures, your logic solver might not be as reliable as you first thought.

1. Introduction

Over the past five years, SBM Offshore has undertaken a comprehensive code review and offline test of all safety application software across the world's largest fleet of leased hydrocarbon production facilities. This exercise has been conducted for over 15000 Process Shutdown I/O, and for more than 18000 Fire and Gas and Emergency Shutdown I/O. The review process spans brand new to 10 year old production facilities, and has been embedded in the company's Group Technical Standards as a requirement for all new facilities. This paper presents some of the key conclusions, challenges and lessons to be learnt from this process, which has enabled residual errors to be rectified, making oil and gas production facilities safer.

Process Shutdown systems on many hydrocarbon facilities are designed to the American Petroleum Institute's Recommended Practice 14C, essentially a prescriptive rather than a risk-based approach to safety, which results in large shutdown systems. Maintaining the integrity of such systems, which may consist of over 1000 I/O, poses significant challenges. Fire and Gas and Emergency Shutdown systems are yet larger, with 1500 or more inputs and outputs, and are subject to their own unique issues.

The extension of IEC61511 code reviews to large safety systems not designed to IEC61511 is a useful means of eliminating residual application software errors. By analysing the recurring errors found in such code reviews, weaknesses in design, commissioning and operations processes and systems can be identified and counter measures put in place.

For facilities designed to IEC61511, the mandatory independent code review (IEC61511-1 section 12.7.2.3) should ensure that errors are removed before plant start-up, while

functional safety management processes are relied upon to protect against errors being introduced during perhaps 20 years of operation. Proof testing during operation should reveal software errors that could be introduced, but as we will see later, most of the errors found in code reviews would not be revealed by testing.

This paper discusses some of the counter measures that can be put in place to reduce the likelihood of application software errors being introduced or remaining undetected, and contrasts these measures with those required by IEC61511. In many cases, the software anomalies found simply serve to highlight the benefits of applying Functional Safety Management principles described in IEC61511 to all safety systems.

1.1 What is an FPSO?

A Floating Production Storage and Offloading vessel is usually a ship either purpose built or converted from an oil tanker. FPSOs are typically around 300m long, and are moored in offshore locations where they perform the same functions as offshore production platforms. These include the separation and treatment of produced hydrocarbons and the injection of treated seawater and gas into the reservoir. Unlike fixed platforms which generally pump produced oil into a pipeline or to a remote loading terminal, the FPSO can store crude oil on board, periodically offloading it directly to a shuttle tanker.

FPSOs are well suited to deep water applications, while their large storage capacity makes them particularly effective as early production systems, where there is no oil pipeline. Currently there are over 200 FPSOs operating worldwide.



Figure 1: SBM Offshore's FPSO Cidade de Paraty, sailing away from the shipyard

1.2 Terminology

On an FPSO there are typically three main safety instrumented systems. The following terminology is used throughout this paper:

- Process Shutdown System (PSS) – the hazard prevention system which detects potentially dangerous conditions and executes process shutdowns, also known as the Safety Instrumented System.

- Fire and Gas System (FGS) – a hazard mitigation system which detects gas release, fire, heat or smoke, and executes fire fighting and other mitigation actions such as water deluge.
- Emergency Shutdown System (ESD) – a hazard mitigation system, generally triggered by Fire or Gas detection, which executes process depressurisation, electrical isolations and other global shutdown functions including those associated with platform abandonment.

The following terms are used in this paper:

- Override or bypass refers to facilities designed into the logic solver to enable operators to defeat shutdown functions for maintenance or operational reasons, usually in a controlled and self-revealing way.
- Software forces refer to changes to the logic solver application software made by a control system technician to defeat a shutdown function.

2 Code Reviews

2.1 Methodology and timing

IEC61511-1 section 12.7.2.3 describes the requirement for application software code reviews. SBM Offshore have taken these principles and supplemented them with a full offline test of safety application software on a safety logic solver platform, running on the same hardware as the target project. A scope of work has been developed, including specific checks to be made to ensure that the persons executing such code reviews perform consistent checks. Furthermore, known recurring errors are highlighted as specific points to check. As required by IEC61511 for SIL3 functions, an independent company has been used for such reviews.

The timing of code reviews can be particularly tricky – they should be performed on the final version of the safety application software having undergone validation testing. The code review also requires final as-built design documents to which the software is programmed. But the code review also needs to be complete early enough to allow errors found to be corrected before the plant is started up. For this reason, and especially when applied to large safety systems, it's recommended to ensure that code reviews are conducted in phases – within a hydrocarbon facility this could mean that the fire and gas system code review is conducted separately to the Process Shutdown System. Critical errors identified must be rectified before plant start-up by a competent engineer, with shutdown functions re-tested.

2.2 Basic software structure of a safety instrumented function

Let's first examine what a basic safety instrumented function looks like, programmed using a Function Block language.

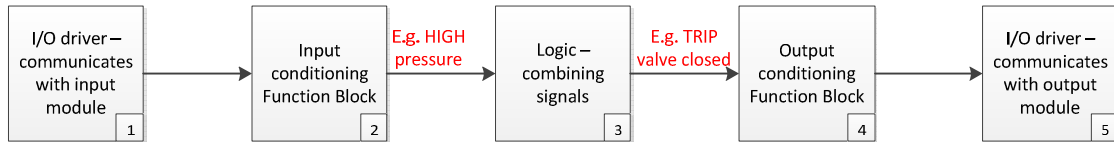


Figure 2: basic software structure of a simple instrumented function

- The first block, block 1 interfaces with the input module connected to the field sensor
- Block 2 provides interface to the HMI system for the sensor element, reporting the measured value. It subjects the measurement to signal conditioning, and generates a trip output if the measurement exceeds the trip set point. It may also incorporate latch and override facilities.
- Block 3 represents logic where one signal may be combined with others. This could consist of voting logic, or a logical AND/OR operation, and time delays.
- Block 4 provides interface to the HMI system for the output element, such as a shutdown valve. It may also incorporate latch or possibly override facilities.
- Block 5 interfaces with the output module, translating a boolean 0 or 1 into typically 0V or 24V outputs.

2.3 Analysis of Code Review results

It's useful to review the types of errors, flaws and anomalies found in application software. In the following sections, the errors are broken down into 8 categories, starting with the most serious.

Apart from the most serious errors, many of the anomalies described below would not be detected by simple proof testing, or even by rigorous stress testing.

i) Safety function will not work at all

This category of anomalies, clearly the most serious, is fortunately one of the rarest. For a safety instrumented function to not work at all, a serious breakdown in processes must have occurred – implying that design verification, testing and/or validation have completely failed at some point. Many of the errors in this category point to commissioning or brownfield changes where logic is forced or disabled, probably post validation, to prevent unwanted shutdowns. Examples of software forces include:

- Software force applied to I/O driver or communications blocks.
- Trip function switched off on the software function block.
- Temporary logic inserted into the application software to defeat logic.

Self-revealing bypasses (such as Maintenance Override switches) should always be preferred, and any forces, no matter how temporary, must be logged in order to ensure they are removed. It has to be recognised that during testing or plant start-up phases, maintenance override switches may not provide sufficient bypass facilities. For this reason it's essential that design, commissioning, operations and modification procedures incorporate auditable procedures for the implementation of software forces, enabling such forces to be removed later.

The anomalies found however also indicate common techniques used, when parts of the plant are running during late commissioning stages, to modify software avoiding spurious trips. That is, a trip function is disabled to prevent an unwanted trip, modified on-line, but not fully restored. Particular vigilance is needed for changes made once parts of the plant are running.

Techniques can be applied to standard library function blocks to ensure that some forces are self-revealing, via alarms. Other forces applied to fail-safe signals communicated between logic solvers can be more difficult to make self-revealing, and specific test procedures may be required to ensure such forces are removed.

ii) Safety function seriously flawed: will only partly work or work too late

This group of anomalies in particular highlights the challenges in managing changes post logic-solver FAT. Whether due to revisions in design documentation, or due to commissioning changes, each phase of change brings with it an increased risk of introducing errors. Examples of this group of serious anomalies include:

- Part of logic missing – particularly a risk for complex logic with multiple inputs or outputs.
- Trip settings incorrect.
- Timer periods incorrect.
- Incorrect instrument range – usually introduced due to changes.

Strong management of change and verification procedures can prevent such errors being introduced. Furthermore, the management of safety logic solver vendor competence becomes a further challenge through multiple revisions of design documents where different software engineers modify the original logic. It's recommended to test each change made post-FAT, rather than relying solely on the final validation testing to reveal errors.

iii) Wrong signal connected / tag number discrepancy

Using the wrong signal in a safety function could have serious consequences. However, experience has shown that tag number discrepancies revealed by code reviews are rarely due to the wrong signal being connected. Rather, this highlights errors in the design documents not corrected in as-built documentation. Such discrepancies go to the heart of management of change procedures. Changing any tag number at any time during a project can lead to this problem, and the importance of keeping design documents updated in line with commissioning red-line mark-ups is evident. Global time differences between the design authority and the commissioning team, along with 7 day working on site, can slow the speed of response to site queries, leading to changes being made without master documents being corrected, or worse, the wrong signal being connected.

iv) Safety function will not work in certain circumstances

This rather general group of anomalies highlights the importance of considering wider logic issues:

- A maintenance override has been configured, when not permitted. Connecting the override enable software parameter to an "override prohibited" tag is a technique to explicitly prohibit overrides and avoid accidental re-enabling of overrides.
- The precedence of two sets of competing logic incorrect.

- Spurious setting of overrides or modes on logic solver start-up.
- The second pulsed output to generate a general plant alarm will not work; a common problem that can be easily solved with a standard software function block.
- Fire zone inhibits defeating the wrong signals. Fire zone inhibits are a particular challenge in fire and gas systems and should wherever possible be programmed in a self-revealing way.

v) Safety function will not work in a specific error state

Techniques are used in safety systems to ensure that the fail-safe state is defined, and that shutdowns are executed using fail-safe techniques. When these techniques are not fully applied, the overall reliability of the function will be reduced. Specific anomalies in this group include:

- Normally open field contacts used instead of normally closed.
- Use of energise to trip circuits when fail-safe circuits are required.
- Communications between logic solvers not set to fail-safe on loss of communications.
- Wrong voting logic used, affecting the logic degrading on sensor failure.
- Revealed sensor error not programmed as required to automatically generate a trip.

vi) Possible dangerous implications

Incorrect software techniques, especially the selection of the wrong standard software function block, or incorrect implementation, can lead to inconsistencies that could have dangerous implications. Examples include:

- High-high trip programmed using the high alarm output. This error can mean that there is no latch and no override facility.
- Incorrect programming of energise to trip circuits – leading to spurious operation on logic solver power-up or loss of communications.
- Tripping of equipment not required to be tripped; typically resulting from changes not fully implemented.

vii) Works but too often, too quickly or too early, causing spurious trips

Aside from the loss of production, spurious trips increase risk since the most dangerous plant states often occur during plant shutdown and start-up. This category of anomalies, though less significant than those described earlier, are caused by the same breakdowns in procedures already described. Errors include incorrect timers, trip settings, function block implementation or software techniques.

viii) Degraded integrity

The final category of anomalies is one that also reveals poor practices, particularly by the logic solver vendor. Not fully following the requirements of the safety manual for logic solver integrity may not normally prevent an instrumented function from working, but will reduce the integrity and reliability of such functions, especially when considering failure states. An example is the use of a non-safe signal, or non-safe software blocks, as part of a safety function.

3 Preventative Measures

A clear learning from conducting code reviews is that each recurring error reveals a weakness somewhere in a procedure that could be addressed. The demarcation of responsibility and the interfaces between the engineering company and the logic solver vendor are particularly important considerations. There are benefits in using the same logic solver platform project after project, with the same software library, as this enables more standardisation and familiarity with error modes. This enables stronger control to be taken of FAT and validation test procedures to feed past experience from code reviews into test procedures. Above all, it is observed that most errors are introduced post-FAT through changes, which require the strongest management of change procedures to be in place. Auditing of logic solver vendor commissioning procedures, especially with regard to change management and temporary force logging, can be beneficial. As can introducing processes for the export of software parameters such as range and trip settings for remote review by the design authority. Education and training around the importance of procedures, and raising awareness of past errors have been observed to be an effective means of preventing mistakes from being repeated.

3.1 Measures during different project phases

Errors can be introduced during any project phase:

- Design and logic solver FAT
- Post FAT changes – implementation of revisions to design documents
- Commissioning and validation
- Operation
- Minor modifications and brownfield changes

Responsible parties during each phase may be different departments or companies, but many of the same controls should apply. Competence management and the control of software forces are two examples that span all phases. An integrated view of procedures across the project phases can be beneficial, and must address the transfer of responsibility at the end of each phase. The boundaries between the phases and responsibilities are often blurred, for example with sub-systems being handed over from commissioning to the operation company while other subsystems are still undergoing design changes.

Rather than leaving the software code review for post-validation, an independent review of software techniques employed, for example post FAT, is a useful strategy to reveal errors early. This allows corrective measures to be made before errors are repeated, including additional training and awareness for the logic solver vendor.

3.2 Standardise and build in self-revealing features

A robust application software library, incorporating features designed to reveal errors, is an effective way of improving software quality. A number of techniques are described in the above sections and indeed in IEC61511, but again, analysis of code review reports assists in developing new strategies to reveal hidden software errors or anomalies. These can include

the development of standard software solutions (e.g. a new function block) for logic requirements prone to error in implementation.

Application software design must take into account the required testing regimes and possible phases of plant modes during operation. Otherwise, the operating company may need to apply software forces, rather than use a more controlled method of bypassing shutdowns during certain operations. Prohibiting overrides may necessitate software forces during commissioning phases, and even to re-start the plant after a shutdown during operation.

3.3 The benefits of simplicity

A fundamental principle of IEC61511 is the limiting of size and complexity in safety systems, concentrating effort on hazards where risk reduction is actually needed. As described earlier, small, manageable safety systems designed to IEC61511 are often made larger and more complex through the addition of asset/financial protection functions. It's common in many oil and gas facilities to retain prescriptive API RP 14C shutdown functions, even when IEC61511 is applied in full.

A typical hydrocarbon production facility designed to IEC61511 may have between 30-50 safety and environment SIL functions which will be subject to the rigours of functional safety management. By comparison, Process Shutdown Systems designed to API RP 14C may consist of 300-400 shutdown functions.

Most shutdown functions are relatively simple, but many are made more complex via the inclusion of multiple "convenience shutdown" actions, whereby the plant is aligned ready for re-start. More complex shutdown functions require a very clear design description to ensure correct implementation and testing.

The larger and more complex the overall safety system, and the more it is subjected to change, the more opportunities exist for errors to be introduced. Small well defined safety systems can be more easily locked down, with software signatures taken to ensure no change is made post-validation. Where Safety systems are not designed to IEC61511, or where SIL functions are mixed with other shutdown functions, there are benefits in identifying and segregating critical functions for additional rigour. This can include the segregation of the highest SIL functions into a dedicated logic solver, subject to yet more rigorous controls.

3.4 Non-software based solutions

One solution to prevent software errors is to use non-programmable systems for the highest integrity functions. This approach is encouraged by the UK HSE (see reference [4]) for the protection of pipelines and risers from oil well pressure. Many international oil companies indeed employ solid state logic solvers for such functions, where the safety instrumented function may be the only layer of protection. Whilst the riser overpressure safety function is the most high profile, other high SIL hazards may exist where the instrumented function is either the only or the last layer of protection, which may merit similar precautions.

4 Conclusions

This paper describes error or weaknesses that can be found in safety application software and preventative measures to avert reoccurrence. Like proof testing, the objective is to identify residual errors before an instrumented function fails to perform its function in a real demand situation, and to allow corrective action to be taken.

This paper advocates that IEC61511 code reviews should be repeated periodically during the operation phase; starting after the first year of operation, where the risk of introducing errors is highest. Theoretically the pre-start-up code review removes the risk of residual software errors, while functional safety management procedures (such as the prohibiting of all software forces during operation) reduce the risk of the introduction of errors. However, reality may be different, not least in IEC61511 designs where large numbers of asset and convenience trips are not fully segregated from personnel safety and environmental protective functions.

In Fire & Gas and ESD systems, and also Process Shutdown Systems designed to API RP 14C, end-to-end testing of large numbers of safety instrumented function is neither always practical nor required by some regulators. In such applications, periodic offline testing is essential, providing a low-cost solution to eliminate errors with minimal disruption caused to operations.

Application software code reviews, whether conducted pre-start-up, or during the operations phase, tell you how effective functional safety management and verification procedures have been in preventing the introduction of errors. This provides a valuable tool to pinpoint where those procedures need strengthening for subsequent projects.

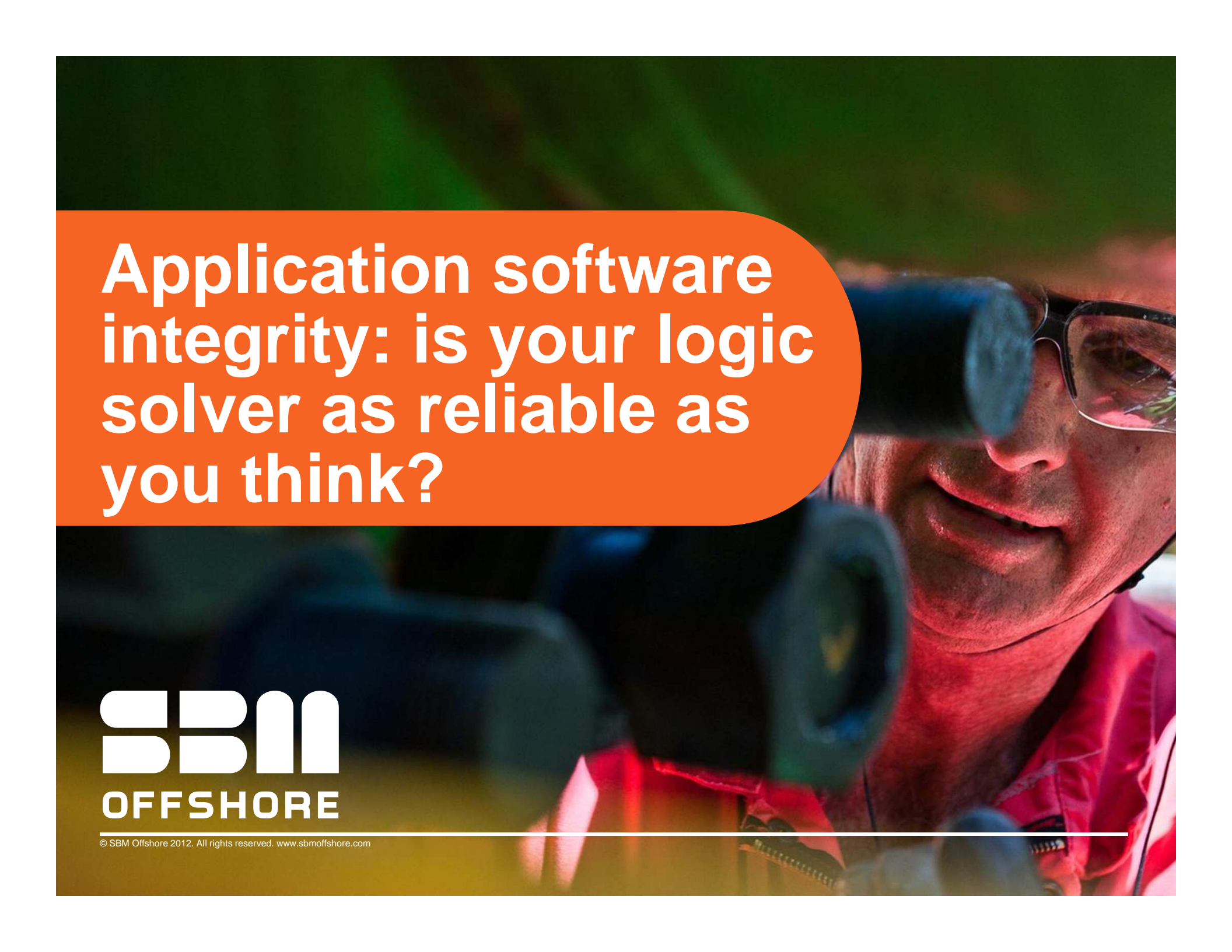
5 References

- [1] IEC61508 Functional safety of electrical / electronic / programmable electronic safety-related systems
- [2] IEC61511 Functional Safety – Safety instrumented systems for the process industry sector
- [3] API RP14C Recommended Practice for Analysis, Design, Installation, and Testing of Basic Surface Safety Systems for Offshore Production Platforms
- [4] SPC/TECH/OSD/31 UK HSE: Safety instrumented systems for the overpressure protection of pipeline risers

The image features a background of a technical drawing or blueprint, showing various lines, grids, and some faint text. Overlaid on this background is the SBM Offshore logo and name. The logo consists of the letters 'SBM' in a large, white, sans-serif font. The 'S' and 'B' are connected, and the 'M' is composed of two vertical bars. Below the logo, the word 'OFFSHORE' is written in a smaller, white, sans-serif font.

SBM OFFSHORE

Application software integrity: is your logic solver as reliable as you think?



**Application software
integrity: is your logic
solver as reliable as
you think?**

SBM
OFFSHORE

© SBM Offshore 2012. All rights reserved. www.sbmoffshore.com

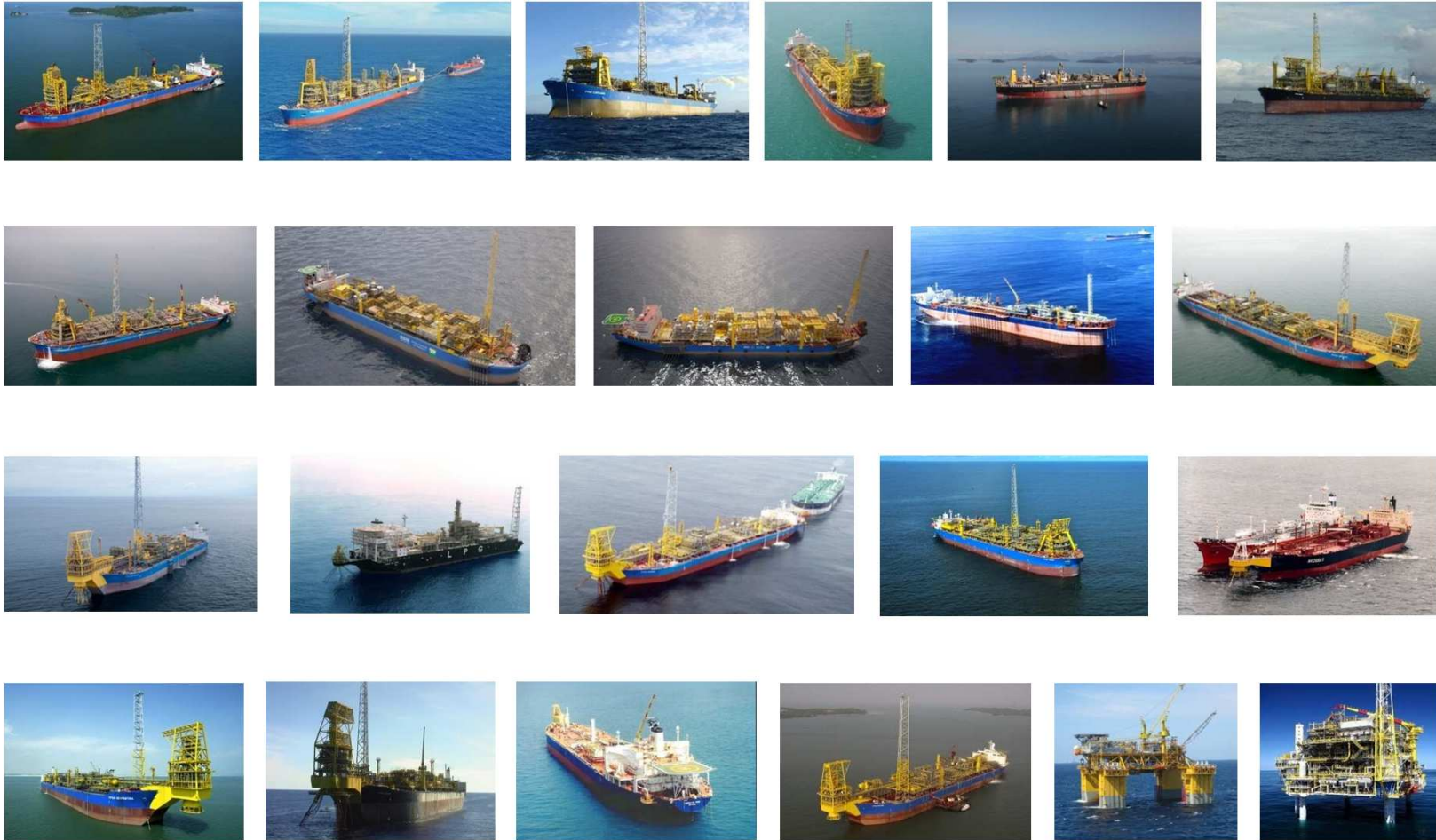
Agenda

- Introduction
- Code review methodology
- Analysis of results
- Preventative measures
- Conclusions

Introduction

- Code reviews of 15000 Process Shutdown and 18000 Fire and Gas I/O
- 16 FPSOs + 1 platform
- 12 were conducted on existing FPSOs, and 5 as part of project execution
- Now embedded in company's Group Technical Standards

Our World: Floating Production



What is an FPSO?

- An FPSO is a Floating Production Storage and Offloading vessel
- A ship either purpose built or converted from an oil tanker
- Typically around 300m long
- Moored in offshore locations where they perform the same functions as offshore production platforms
- Well suited to deep water applications and early production systems
- Currently there are approximately 200 FPSOs operating worldwide

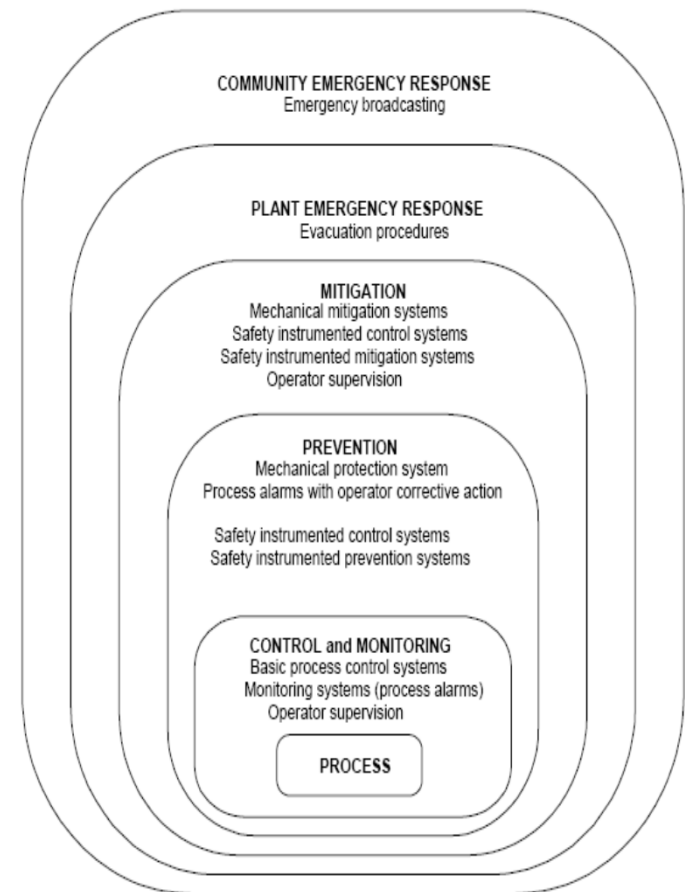


FPSO Aseng en route to Equitorial Guinea

Terminology

On an FPSO there are typically three main safety instrumented systems

- **Process Shutdown System (PSS)** – detects potentially dangerous conditions and executes process shutdowns
- **Fire and Gas System (FGS)** – detects gas release or fire, and executes fire fighting and other mitigation actions
- **Emergency Shutdown System (ESD)** – executes process depressurisation (blowdown), electrical isolations and other global shutdown functions



Standards employed

- API RP 14C implemented for Process Shutdown
- PSS system of 300-350 SIFs, over 1000 I/O
- Shutdowns are not prioritised; all treated the same
- SIL reviews conducted on a number of projects tell us only 10-15% of these shutdowns are for personnel safety
- Fire and Gas and ESD systems are larger still, with up to 1500 I/O

The management of software integrity over such large safety systems presents challenges, the same challenges as for IEC61511 designs, but on a larger scale.

Code review methodology

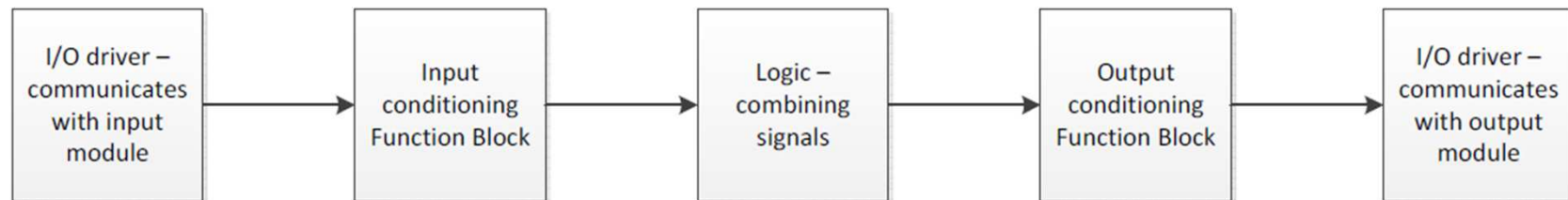
- IEC61511-1 section 12.7.2.3 code review
- Supplemented with a full offline test
- Scope of work, with specific checks specified for consistency
- Recurring errors are highlighted as specific points to check
- Independent party, with required competence

Code review timing

- Final software post validation
- As built design documents
- Completed early enough for errors to be corrected before start-up
- Conducted in phases by safety system and plant area
- Corrections implemented by competent engineer

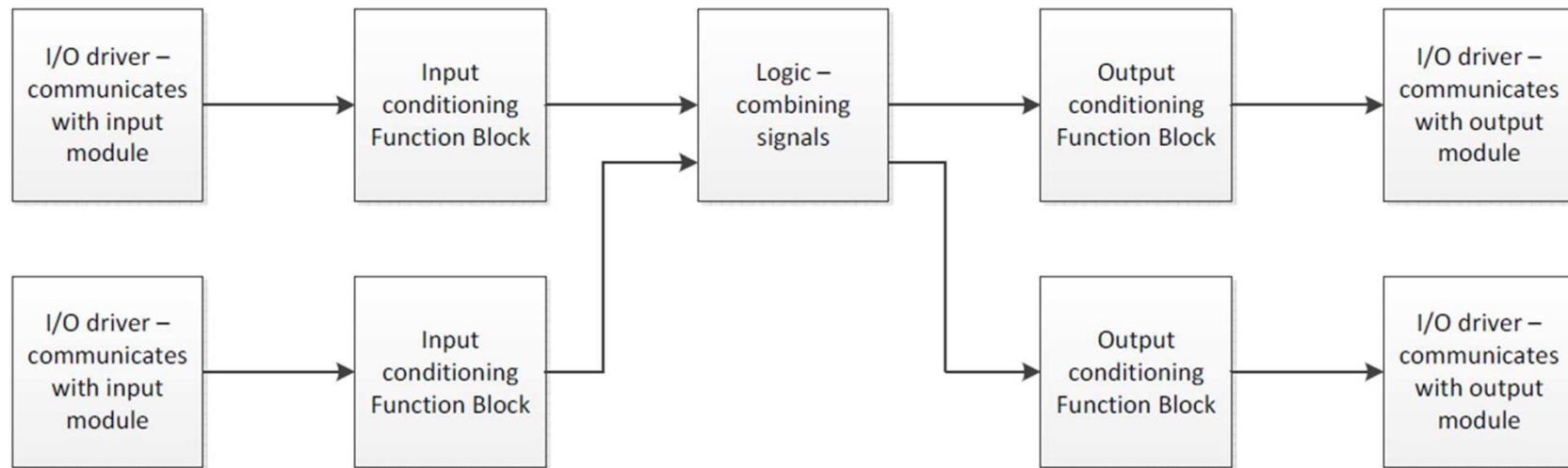
Analysis of results

Basic software structure of a SIF



1. Interfaces with the input module connected to the field sensor
2. E.g. analogue input - HMI interface, signal conditioning, generates trip output. May incorporate latch, override.
3. Logic – e.g. AND, OR, timers, voting
4. E.g. shutdown valve - HMI interface, may incorporate latch
5. Interfaces with the output module, translating a boolean 0 or 1 into typically 0V or 24V outputs.

Basic software structure for a SIF



E.g. high level OR high pressure -> close inlet valve and trip pump

Categories of errors and anomalies found

i) Safety function will not work at all

- Serious breakdown in processes must have occurred
- Many of the errors in this category point to commissioning or brownfield changes where logic is forced or disabled, probably post validation
- Can indicate techniques to modify logic while plant running
- Forces applied during operation phase

Examples:

- Trip setpoint missing or outside range of transmitter
- Trip function switched off on the software function block.
- Software force applied to I/O driver or communications blocks.
- Temporary logic inserted into the application software to defeat logic.

i) Safety function will not work at all

Counter-measures:

- Log forces no matter how temporary, with system to ensure removed
- Only allow self-revealing forces
- Modify test procedures – e.g. to inspect communication blocks, or test SIFs in appropriate order (test the SIF that is required to be forced last)
- Design for testing and operation, avoiding the need for forces. E.g. prohibiting maintenance override may necessitate a force to re-start the plant.
- Competence, auditing, awareness and commissioning supervision of logic solver vendor.

ii) Safety function seriously flawed: will only partly work or work too late

Challenges in managing changes post logic-solver FAT – examples:

- Part of logic missing (some C&E intersections not programmed) – particularly a risk for complex logic with multiple inputs or outputs, some of which may be “convenience actions”
- Trip settings incorrect.
- Timer periods incorrect.
- Incorrect instrument range – usually introduced due to changes.

ii) Safety function seriously flawed: will only partly work or work too late

Counter-measures:

- Clarity and simplicity of design documents – avoid notes on C&E documents
- Strong management of change and verification procedures
- Test each change post-FAT
- Logic solver vendor competence (for post-FAT changes and site work)
- Read back signal via HART and compare to scaled analogue
- Competence – e.g. changes made during operation

iii) Wrong signal connected / tag number discrepancy

Could have serious consequences

- But rarely actually the wrong signal connected
- Can apply to use of “soft tags” identified in Cause and Effects
- As-built corrections not captured in design documents – code reviews reveal discrepancies between as-built documents and the software!
- Can result from design changes post FAT

iv) Safety function will not work in certain circumstances

General group:

- Maintenance override has been configured when not permitted.
- The precedence of two sets of two competing sets of logic incorrect.
- Spurious setting of overrides or modes on logic solver start-up.
- The second pulsed output to generate a general plant alarm will not work
- Fire zone inhibits defeating the wrong signals.
- Extraneous logic connections degrading primary SIF

Counter-measures:

- To explicitly prohibit overrides - connect override enable an “override prohibited” tag
- Multiple pulses – develop a standard software function block.
- Fire zone inhibits programmed to be self-revealing.

v) Safety function will not work in a specific error state

Fail-safe techniques not fully applied

- Normally open field contacts used instead of normally closed.
- Use of energise to trip circuits when fail-safe circuits are required.
- Communications between controllers not set to fail-safe on loss of communications.
- Wrong voting logic used, affecting the logic degrading on sensor failure.
- Revealed sensor error not programmed as required to automatically generate a trip.

Counter-measures:

- Awareness of logic solver team and verification measures
- Awareness of commissioning teams
- Test procedures - specific test for action on failure (e.g. test procedure for specific requirements of the SRS)

vi) Possible dangerous implications

Particularly due to incorrect software techniques, wrong standard software blocks, incorrect implementation:

- High-high trip programmed using the high alarm output – no latch or override
- Incorrect programming of energise to trip circuits – leading to spurious operation on logic solver power-up or loss of communications.
- Tripping of equipment not required to be tripped; typically resulting from changes not fully implemented.

Counter-measures:

- Competence and awareness
- Familiarity with software library and system functionality
- Verification measures

vii) Works but too often, too quickly or too early, causing spurious trips

Plant shutdown and restart are often the most dangerous phases of operation. This category of errors particularly due to incorrect software techniques, wrong blocks, incorrect implementation:

- Incorrect timers (usually too short)
- Trip settings too low
- Wrong software techniques – e.g. permissive programmed as a trip
- Configured to automatically generate a trip on failed transmitter when not required

viii) Degraded integrity

Examples:

- Not following safety manual requirements
- Non-safe programming blocks
- Hardware diagnostics not correctly configured
- Dead code not removed
- Incorrect runtime sequence

Counter-measures:

- Competence and training

Preventative measures

Measures during different project phases

Errors can be introduced during any project phase:

- Design and logic solver FAT
- Post FAT changes – implementation of revisions to design documents
- Commissioning and validation
- Operation
- Minor modifications and brownfield changes

Many of the same controls apply through all phases:

- Quality procedures – e.g. forces/temporary change logging
- Competence

Preventative measures

- Clear responsibilities across contractual boundaries – e.g. engineering company / logic solver vendor / commissioning team
- Use same logic solver and software library project after project – enabling stronger control of FAT, verification and validation procedures
- Early code review at FAT
- Ensure code review results communicated back to team, and using the same team again...
- Audit vendor's MOC and commissioning procedures
- Export software parameters for offline checking

Standardise and build in self-revealing features

- Robust software library – incorporating features to reveal errors – e.g. compare PCS / SIS transmitters, alarm forces
- Develop function block for applications prone to recurring errors
- Design for testing and operation – avoid need for forces
- Develop robust FAT, verification and validation procedures based on the software library

The benefits of simplicity

- A fundamental principle of IEC61511 is the limiting of size and complexity in safety systems
- Small, manageable safety systems designed to IEC61511 are often made larger and more complex through the addition of asset/financial protection functions
- Clearly separate “convenience shutdown” actions from primary safety function
- Segregate highest SIL, or safety SILs in a dedicated logic solver and lock-down after validation (taking signatures)

Non-software based solutions

- Avoid software errors by avoiding software!
- Encouraged by the UK HSE for the protection of pipelines and risers from oil well pressure – where the SIF is the last to operate or only layer of protection
- Mandated by many oil companies – solid state logic solver for “HIPPS”
- Can be considered for other high SIL hazards

Conclusions

- Systems in place to prevent changes post-validation cannot always be guaranteed 100% effective
- Errors identified by code reviews need to be rectified without introducing more errors
- Procedures during operation to prevent modification or forcing cannot be guaranteed 100% effective during the entire plant life.
- Many of the errors described cannot be identified by proof testing
- Additional challenges come from mixing asset shutdowns with safety SIFs, and from secondary convenience shutdown logic.

Conclusions

- Repeat code reviews periodically during operation, starting after say 1 year.
- Use code reviews to strengthen functional safety management and verification procedures

Thank you.

SBM
OFFSHORE

© SBM Offshore 2012, All rights reserved. www.sbmoffshore.com

Specialising in the delivery of Electrical, Control and Instrumentation
(EC&I) systems

PROOF TESTING... the Challenges

Institute of Measurement and Control - Functional Safety 2014



Stuart Main

- Technical Safety Engineer
- HTS Engineering Group



Proof Testing

- **What does IEC 61508 / 61511 say?**
- **Proof Testing and PFD_{avg}**
- **Proof Test Strategy**
- **Proof Test Procedure**
- **Concluding comments**

Proof Testing – What does IEC 61508 / 61511 say?

IEC 61508-6 / 3.8.5 / Edition 2

Proof Test:

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 IEC 61508-4 / 3.8.5 /Edition 2].

IEC 61511-1 / 3.2.58

Proof Test:

Test performed to reveal undetected faults in a safety instrumented system so that, if necessary, the system can be restored to its designed functionality

Proof Testing

- **What does IEC 61508 / 61511 say?**
- **Proof Testing and PFD_{avg}**
- **Proof Test Strategy**
- **Proof Test Procedure**
- **Concluding comments**

Proof Test and PFD_{avg}

- **In the context of IEC 61508 / 61511; the object of proof testing is to reveal dangerous undetected failures, e.g. excluding failures detected by automatic diagnostic mechanisms.**
- **Dangerous undetected failures are failures that will result in the loss of the safety function, not necessarily deviation from equipment specification.**
- **Typically the dangerous undetected failures along with the proof test frequencies are the main driver behind the achieved PFD_{avg} of a Safety Function.**
- **Therefore the estimate PFD_{avg} of a Safety Function will be greatly affected by implementing a different proof test frequency.**

Perfect and Imperfect Proof Testing

- As with the proof test frequency, the estimate PFD_{avg} of a Safety Function can be greatly affected by implementing a different proof test coverage.
- Cannot assume the proof testing will detect 100% of dangerous undetected failures (i.e. perfect proof testing)... in practice this is difficult to achieve.
- Failures that are not detected by proof testing will increase the PFD_{avg} of the safety function year on year despite regular proof testing
- Given enough time the PFD_{avg} will increase to an unacceptable level
- Some examples of imperfect proof testing are:
 - not testing the system under normal operating process conditions
 - not testing impulse lines for blockages
 - failure to check valves close fully and to the required shut off class.

Proof Testing

- **What does IEC 61508 / 61511 say?**
- **Proof Testing and PFD_{avg}**
- **Proof Test Strategy**
- **Proof Test Procedure**
- **Concluding comments**

Proof Test Strategy

Ideal Testing

The proof test of a safety function should reflect the true operating conditions.

Some issues relating to ideal testing are:

- **the safety function should be initiated without causing a demand state.**
- **appropriate risk assessment and additional risk reduction measures implemented.**
- **Practicality of test and associate risk.**
- **Additional testing may be required to test redundant channels.**

Proof Test Strategy

Off-line Testing

Off-line testing is often preferred due to practicalities.

The issue relating to off-line testing is:

- **the safety function is not initiated under true operating conditions and subsequently all failure modes may not be detected.**

Proof Test Strategy

Optimising Off-line Testing

Where a safety function cannot be proof tested under true operating conditions, consideration should be given to how testing can be optimised, ideally during the design phase.

- **Some techniques used to optimise testing are:**
 - **Corroborative measurement of sensing element.**
 - **Valve closure detected by downstream instrumentation.**
 - **A series of partial testing at different intervals.**
 - **Inclusion of diagnostic mechanisms.**

Proof Test Strategy

Partial Testing

- **Partial testing refers to a test that is capable of revealing certain failure modes.**
- **By carrying out a series of partial tests it may be possible to reveal all failure modes.**
- **Partial tests can be carried out at different frequencies.**

An example of partial testing would be the testing of an actuated valve.

- **Partial test 1:** Witness valve transition from operation position to the safe state in a smooth manner whilst the plant is shut down.
- **Partial test 2:** Flow scan of the valve and compare performance results against results taken when new.
- **Partial test 3:** Leak test of valve, requires valve to be removed from service.

Proof Test Strategy

Where Proof Testing Cannot Detect All Dangerous Failures

IEC 61508-6 / B.3.2.5 / Edition 2

Faults in the safety system that are not detected by either diagnostic tests or proof tests may be found by other methods arising from events such as a **hazardous event requiring operation of the safety function** or **during an overhaul of the equipment**. If the faults are not detected by such methods it should be assumed that the **faults will remain for the life of the equipment**.

Proof Test Strategy

Hazardous Event Requiring Operation of the Safety Function

One technique is to utilise a demand on the safety function as a means to identify dangerous failures.

The following criteria must be considered if this approach is to be taken:

- Validation that the SIF prevented the hazardous event and not by other means.**
- How failures in redundant channels will be detected.**
- How demand rate will be estimated.**

Proof Test Strategy

During an overhaul of the equipment

An overhaul of equipment can be considered as a means of returning equipment to an “as new” condition (IEC 61508) or its designed functionality (IEC 61511).

Proof Test Strategy

Life of the Equipment

When certain failures can not be detected by proof testing, additional maintenance activities (e.g. equipment overhaul) or SIF demands, **the proof test interval should be considered the life of the equipment.**

Proof Test Coverage Determination

How to Determine Proof Test Coverage

The following are examples of how proof test coverage can be estimated:

- **Manufacturers guidance.**
- **Failure Mode and Effects Analysis (FMEA) / Failure Mode Effects and Diagnostic Analysis (FMEDA) whereby a specific test has been considered.**
- **Reviewing failures encountered during operation and identifying how many would have been detected by the defined proof test.**
- **Identifying failures modes and failure mode distribution from a data source e.g. OREDA, FARADIP, SINTEF, etc. and identifying which of these failure modes would be detected by the defined proof test.**
- **Engineering judgement based on sound evidence.**

Proof Test and PFD_{avg} Distribution

PFD_{avg} Distribution

- Typically the PFD_{avg} is generally not evenly distributed across each subsystem.
- It is common for subsystems comprising of mechanical devices to be the driver for the complete SIF PFD_{avg} .
- Consideration to PFD_{avg} distribution should be made when allocating the effort and potential process disruptions to a specific test.

Proof Testing

- **What does IEC 61508 / 61511 say?**
- **Proof Testing and PFD_{avg}**
- **Proof Test Strategy**
- **Proof Test Procedure**
- **Concluding comments**

Proof Test Procedures

- **Documented and auditable for each safety function.**
- **Developed in a systematic manner with the objective of determining the dangerous failures that have not been detected by other means.**
- **Clear Pass/Fail criteria.**
- **Suitable method for recording failures.**
- **The degree of detail should take into account the training and competence of the persons who are carrying out the proof tests.**

Additional Tasks

Additional Activities Included in Proof Testing Procedure

Typical additional activities that may be included in a proof testing procedure are:

- **Visual inspection (IEC 61511-1/2 / 16.3.2.).**
- **Testing diagnostic mechanisms e.g. open/short circuit, over/under range.**
- **Loss of motive power e.g. removal of air supply to valves.**
- **Calibration of sensors.**

Proof Testing

- **What does IEC 61508 / 61511 say?**
- **Proof Testing and PFDavg**
- **Proof Test Strategy**
- **Proof Test Procedure**
- **Concluding comments**

Concluding Comments

- **The inability to fully test a safety instrumented function will have adverse effects on the risk reduction it provides if incorrect assumptions on the proof test coverage have been made. The tolerable risk target may not be met.**
- **PFD_{avg} contribution of devices and subsystems should be considered when allocating effort to optimising proof testing.**
- **The user and the designer of the safety instrumented function should address jointly the means by which it will be maintained throughout its lifetaking into account a realistic proof test coverage.**

Thank You

Any Questions?

www.htsgrp.com








HTS Engineering Group Ltd
17 Beeston Court
Stuart Road
Manor Park
Runcorn
Cheshire
WA7 1SS



Functional Safety 4th -5th November 2014

**Annex A of IEC 61508-2 and its effect
in SIL determination**

Dr Hassan El-Sayed
Functional Safety Consultant
Sira Test & Certification
Functional Safety Department
hassan.el-sayed@siracertification.com
Tel: 00441244670900

-  Definition of Annex A of IEC 61508 part 2
-  Use of Annex A tables in the derivation of DC and SFF
-  Implementation of diagnostics for final element
-  Review of assessed products based on diagnostic tools
-  Summary

Definition of Annex A

- ④ T&M for safety of E/E/PE related systems; controls of failure during operation.
- ④ Used to limit the maximum diagnostic coverage that can be claimed which directly influences the SFF.

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_D} \qquad SFF = \frac{\lambda_S + \lambda_{DD}}{\lambda_S + \lambda_{DD} + \lambda_{DU}}$$

- ④ T&M are provided to control failures during the operation which are built in features of the safety related systems.
- ④ T&M are provided to avoid the failures during the realisation phases of the safety lifecycle

Definition of Annex A

- ④ The analysis should include all components, E/E/M/EM necessary to implement the safety functions.
- ④ Identify the possible dangerous modes of failures of all components which prevent a safe response during a demand
- ④ Dangerous failures are detected by automatic on-line diagnostic tests which improve the DC fraction.
- ④ Types of diagnostics tests may include, Continuous signal monitoring, External stimuli, Built in checksums, comparison of measured values by redundancy approach, implemented by another element within the SRS.
- ④ Diagnostic can operate continuous or periodical upon PTI.

Annex A of IEC 61508-2 Table A1

Component	See table(s)	Requirements for diagnostic coverage claimed		
		Low (60 %)	Medium (90 %)	High (99 %)
Electromechanical devices	A.2	Does not energize or de-energize Welded contacts	Does not energize or de-energize Individual contacts welded	Does not energize or de-energize Individual contacts welded No positive guidance of contacts (for relays this failure is not assumed if they are built and tested according to EN 50205 or equivalent) No positive opening (for position switches this failure is not assumed if they are built and tested according to IEC 60947-5-1, or equivalent)
Discrete hardware	A.3, A.7, A.9			
Digital I/O		Stuck-at (see Note 1)	DC fault model (see Note 2)	DC fault model drift and oscillation
Analogue I/O		Stuck-at	DC fault model drift and oscillation	DC fault model drift and oscillation
Power supply		Stuck-at	DC fault model drift and oscillation	DC fault model drift and oscillation

Annex A of IEC 61508-2 Table A1

<p>Bus</p> <p>General</p> <p>Memory management unit (MMU)</p> <p>Direct memory access (DMA)</p> <p>Bus-arbitration (see Note 5)</p>	<p>A.3 A.7 A.8</p>	<p>Stuck-at of the addresses</p> <p>Stuck-at of data or addresses</p> <p>No or continuous access</p> <p>Stuck-at of arbitration signals</p>	<p>Time out</p> <p>Wrong address decoding</p> <p>Change of addresses caused by soft-errors in the MMU registers (see Notes 3 and 4)</p> <p>DC fault model for data and addresses</p> <p>Change of information caused by soft-errors in the DMA registers</p> <p>Wrong access time</p> <p>No or continuous arbitration</p>	<p>Time out</p> <p>Wrong address decoding</p> <p>Change of addresses caused by soft-errors in the MMU registers</p> <p>All faults that affect data in the memory</p> <p>Wrong access time</p> <p>No or continuous or wrong arbitration</p>
<p>Central Processing Unit (CPU)</p> <p>Register, internal RAM</p> <p>Coding and execution including flag register</p> <p>Address calculation</p> <p>Program counter, stack pointer</p>	<p>A.4, A.10</p>	<p>Stuck-at for data and addresses</p> <p>Wrong coding or no execution</p> <p>Stuck-at</p> <p>Stuck-at</p>	<p>DC fault model for data and addresses</p> <p>Change of information caused by soft-errors</p> <p>Wrong coding or wrong execution</p> <p>DC fault model</p> <p>Change of addresses caused by soft-errors</p> <p>DC fault model</p> <p>Change of addresses caused by soft-errors</p>	<p>DC fault model for data and addresses</p> <p>Dynamic cross-over for memory cells</p> <p>Change of information caused by soft-errors</p> <p>No, wrong or multiple addressing</p> <p>No definite failure assumption</p> <p>No definite failure assumption</p> <p>DC fault model</p> <p>Change of addresses caused by soft-errors</p>

Annex A of IEC 61508-2 Table A1

Component	See table(s)	Requirements for diagnostic coverage claimed		
		Low (60 %)	Medium (90 %)	High (99 %)
Interrupt handling Interrupt Reset circuitry	A.4	No or continuous interrupts (see Note 6) Stuck-at Individual components do not initialize to reset state	No or continuous interrupts Cross-over of interrupts DC fault model Drift and oscillation Individual components do not initialize to reset state	No or continuous interrupts Cross-over of interrupts DC fault model Drift and oscillation Individual components do not initialize to reset state
Invariable memory	A.5	Stuck-at for data and addresses	DC fault model for data and addresses	All faults that affect data in the memory
Variable memory	A.6	Stuck-at for data and addresses	DC fault model for data and addresses Change of information caused by soft-errors	DC fault model for data and addresses Dynamic cross-over for memory cells Change of information caused by soft-errors No, wrong or multiple addressing
Clock (quartz, oscillator, PLL)	A.11	Sub- or super-harmonic Period jitter	Incorrect frequency Period jitter	Incorrect frequency Period jitter
Communication and mass storage	A.12	Wrong data or addresses No transmission	All faults that affect data in the memory Wrong data or addresses Wrong transmission time Wrong transmission sequence	All faults that affect data in the memory Wrong data or addresses Wrong transmission time Wrong transmission sequence
Sensors	A.13	Stuck-at	DC fault model Drift and oscillation	DC fault model Drift and oscillation
Final elements	A.14	Stuck-at	DC fault model Drift and oscillation	DC fault model Drift and oscillation

Annex A of IEC 61508-2 Table A2

Diagnostic technique/measure	See IEC 61508-7	Maximum diagnostic coverage considered achievable	Notes
Failure detection by on-line monitoring	A.1.1	Low (low demand mode) Medium (high demand or continuous mode)	Depends on diagnostic coverage of failure detection
Monitoring of relay contacts	A.1.2	High	Relay switching rate should be taken into account when quantifying the effect of random failures
Comparator	A.1.3	High	High if failure modes are predominantly in a safe direction
Majority voter	A.1.4	High	Depends on the quality of the voting
NOTE 1 This table does not replace any of the requirements of Annex C.			
NOTE 2 The requirements of Annex C are relevant for the determination of diagnostic coverage.			
NOTE 3 For general notes concerning this table, see the text preceding Table A.1.			

Annex A of IEC 61508-2 Table A3

Diagnostic technique/measure	See IEC 61508-7	Maximum diagnostic coverage considered achievable	Notes
Failure detection by on-line monitoring	A.1.1	Low (low demand mode) Medium (high demand or continuous mode)	Depends on diagnostic coverage of failure detection
Comparator	A.1.3	High	High if failure modes are predominantly in a safe direction
Majority voter	A.1.4	High	Depends on the quality of the voting
Tests by redundant hardware	A.2.1	Medium	Depends on diagnostic coverage of failure detection
Dynamic principles	A.2.2	Medium	Depends on diagnostic coverage of failure detection
Standard test access port and boundary-scan architecture	A.2.3	High	Depends on the diagnostic coverage of failure detection
Monitored redundancy	A.2.5	High	Depends on the degree of redundancy and of the monitoring
Hardware with automatic check	A.2.6	High	Depends on the diagnostic coverage of the tests
Analogue signal monitoring	A.2.7	Low	

Annex A of IEC 61508-2 Table 9

Table A.9 – Power supply

Diagnostic technique/measure	See IEC 61508-7	Maximum diagnostic coverage considered achievable	Notes
Overvoltage protection with safety shut-off or switch-over to second power unit	A.8.1	Low	
Voltage control (secondary) with safety shut-off or switch-over to second power unit	A.8.2	High	
Power-down with safety shut-off or switch-over to second power unit	A.8.3	High	
NOTE 1 This table does not replace any of the requirements of Annex C.			
NOTE 2 The requirements of Annex C are relevant for the determination of diagnostic coverage.			
NOTE 3 For general notes concerning this table, see the text preceding Table A.1.			

Annex A of IEC 61508-2 Table A13

Table A.13 – Sensors

Diagnostic technique/measure	See IEC 61508-7	Maximum diagnostic coverage considered achievable	Notes
Failure detection by on-line monitoring	A.1.1	Low (low demand mode) Medium (high demand or continuous mode)	Depends on diagnostic coverage of failure detection
Analogue signal monitoring	A.2.7	Low	
Test pattern	A.6.1	High	
Input comparison/voting (1oo2, 2oo3 or better redundancy)	A.6.5	High	Only if dataflow changes within diagnostic test interval
Reference sensor	A.12.1	High	Depends on diagnostic coverage of failure detection
Positive-activated switch	A.12.2	High	
NOTE 1 This table does not replace any of the requirements of Annex C.			
NOTE 2 The requirements of Annex C are relevant for the determination of diagnostic coverage.			
NOTE 3 For general notes concerning this table, see the text preceding Table A.1.			

Annex A of IEC 61508-2 Tables 15, 16 and 17

- Ⓢ Table 15,16 and 17 are recommended as T&M for the systematic safety integrity to:
- Ⓢ control of failures caused by hardware design (see Table A.15).
- Ⓢ control of failures due to environmental stress or influences (see Table A.16) and
- Ⓢ control of failures during operation, see Table 17.

Table A.15 – Techniques and measures to control systematic failures caused by hardware design

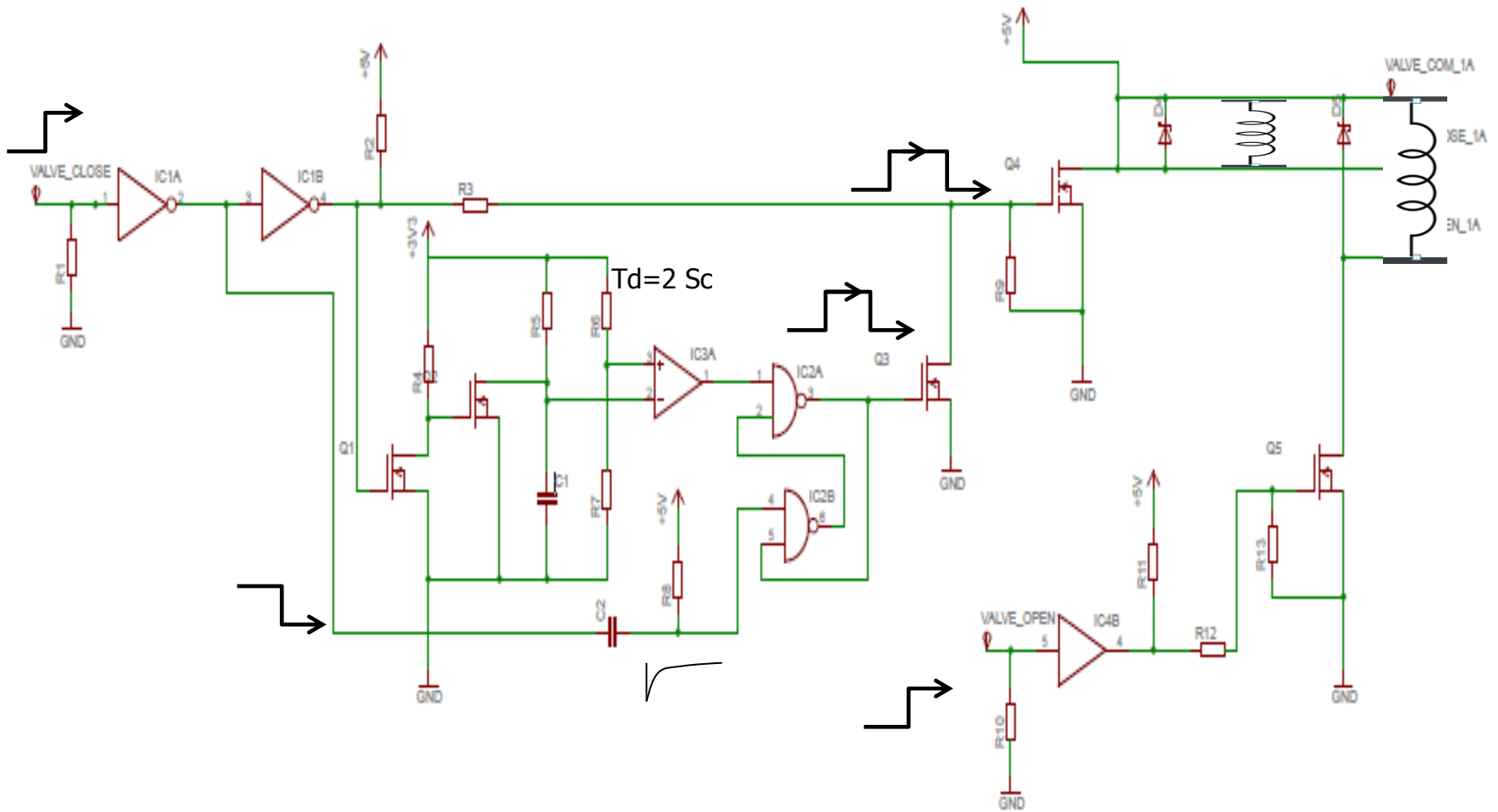
	Technique/measure	See IEC 61508-7	SIL 1	SIL 2	SIL 3	SIL 4
	Program sequence monitoring	A.9	HR low	HR low	HR medium	HR high
	Failure detection by on-line monitoring (see Note 4)	A.1.1	R low	R low	R medium	R high
	Tests by redundant hardware	A.2.1	R low	R low	R medium	R high
	Standard test access port and boundary-scan architecture	A.2.3	R low	R low	R medium	R high
	Code protection	A.6.2	R low	R low	R medium	R high
	Diverse hardware	B.1.4	– low	– low	R medium	R high

Annex A of IEC 61508-2

Table A.16 – Techniques and measures to control systematic failures caused by environmental stress or influences

	Technique/measure	See IEC 61508-7	SIL 1	SIL 2	SIL 3	SIL 4
	Measures against voltage breakdown, voltage variations, overvoltage, low voltage and other phenomena such as a.c. power supply frequency variation that can lead to dangerous failure	A.8	M low	M medium	M medium	M high
	Separation of electrical energy lines from information lines (see Note 4)	A.11.1	M	M	M	M
	Increase of interference immunity	A.11.3	M low	M low	M medium	M high
	Measures against the physical environment (for example, temperature, humidity, water, vibration, dust, corrosive substances)	A.14	M low	M high	M high	M high
	Program sequence monitoring	A.9	HR low	HR low	HR medium	HR high
	Measures against temperature increase	A.10	HR low	HR low	HR medium	HR high
	Spatial separation of multiple lines	A.11.2	HR low	HR low	HR medium	HR high
	Idle current principle (where continuous control is not needed to achieve or maintain a safe state of the EUC)	A.1.5	R	R	R	R
	Measure to detect breaks and shorts in signal lines		R	R	R	R
	Failure detection by on-line monitoring (see Note 5)	A.1.1	R low	R low	R medium	R high

Implementation of diagnostics for final element



FMEA of the (close/open)

Circuit type A

No.	Values	Safe Rev'led	Safe Un-rvld	Dangrs Detect	Dangrs Un-detec	Safe Rev'led	Safe Un-rvld	Dangrs Detect	Dangrs Un-detec	Safe No-effect	Dangrs detect	Safe No-effect
1	R1											0
2	R2											0
13	C1											0
14	D4											0
15	D5											0
16	Q1											0
20	Q5											0
23	IC4	0	0.00037	0	0	0	0	0	4.1E-05	0		0.00888
24	IC4	0	0	0	0.00037	0	4.1E-05	0	0	0	0	0.00888
		s		no	No	d		No	no diagnostics			0.00888
		d	0	0	0.0001	0	0.0004	0	0	0	0	0.00888
		d	0.00096	0	0	0	0	0	0	0	0.0086	
		s	0	0	0	0	0	0	0.00024	0	0.0086	
		d	0.00096	0	0	0	0	0	0	0	0.0086	
31	IC3	0	0.00096	0	0	0	0	0	0	0	0	0.00888
		s		no	No	d		No	no diagnostics			0.0086
		s	0.00062	0	0	0	0	0	0	0	0	0.0069
		d	0	0	0	0	0	0	0	0	0.00718	
		s	0	0	0	0	0	0	0	0	0.0069	
		d	0	0	0.00062	0	0	0	0	0	0.00718	
32	IC2	0	0	0	0	0	0	0	0	0	0	0.005
		d		no	No	d		No	no diagnostics			0.005
		n	0	0	0	0	0	0	0	0	0.00888	0.00513
		n	0	0	0	0	0	0	0	0	0.005	
		n	0	0	0	0	0	0	0	0	0.00513	
		n	0	0	0	0	0	0	0	0	0.00654	
40	IC1											0.00654
45	IC1											0.00654
		n	0	0	0	0	0	0	0	0	0	0.00676
		n	0	0	0	0	0	0	0	0	0	0.00654
		n	0	0	0	0	0	0	0	0	0	0.00676
46	R8											0.00041
47	C2											0.0005

0.0000

0.0000

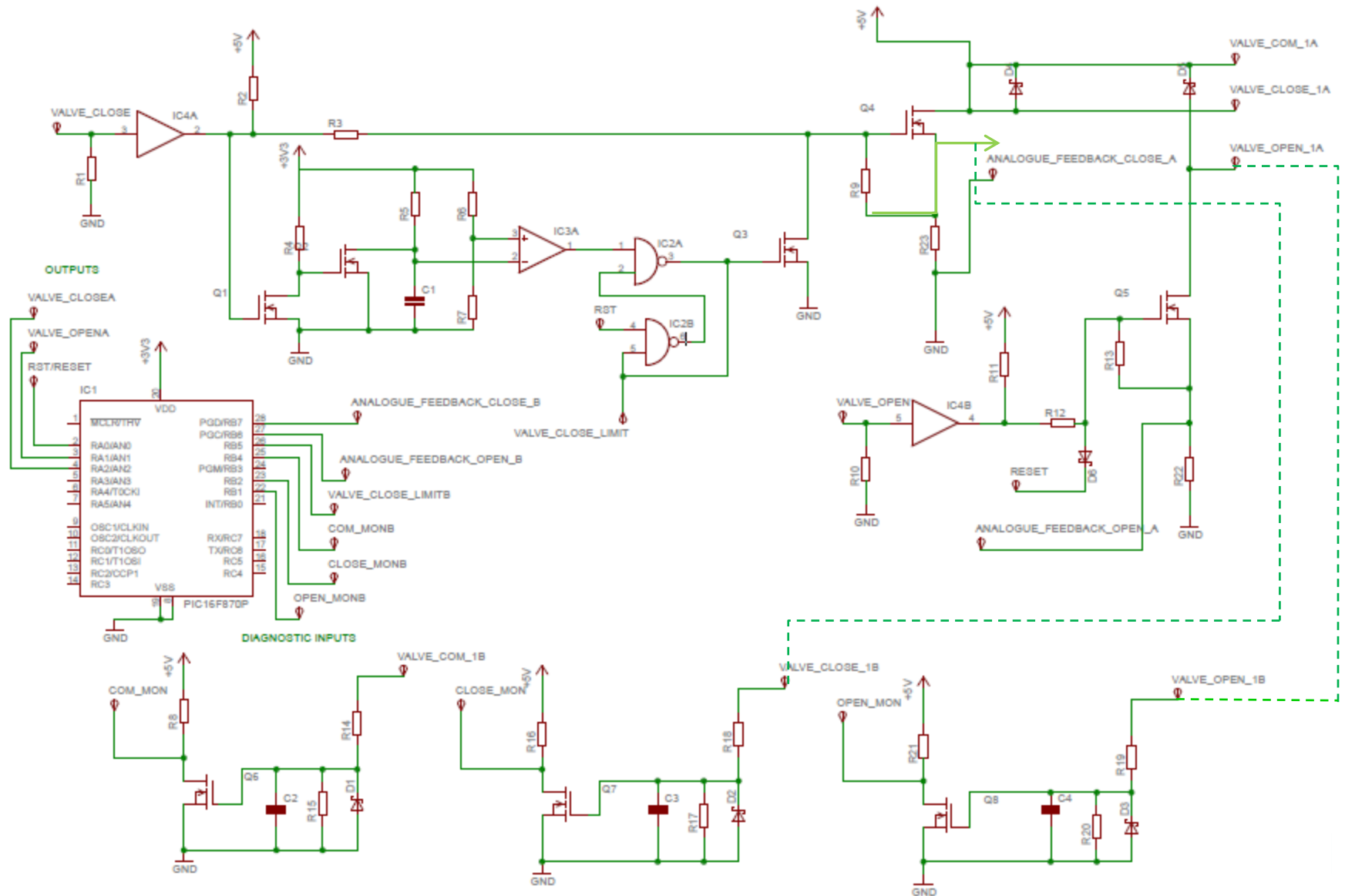
short to pin below

FMEA of the (close/open) Circuit type A

1001 EQUATIONS

Parameter name	Symbol	Equation / source	Close/Open without diag
Proof Test Interval [PTI]	T	Given, for this example	2190
Mean Time To Repair	MTTR	Given, for this example	8
Type A/B	type A	Given, for this example	type a
Total failures:	λ	From FMEA	5.85E-08
Safe diagnosed failures:	λ^{SD}	From FMEA	0.00E+00
Safe undiagnosed failures:	λ^{SU}	From FMEA	1.05E-08
Dangerous diagnosed failures:	λ^{DD}	From FMEA	0.00E+00
Dangerous undiagnosed failures:	λ^{DU}	or High demand mode, PFH per (hour)	4.80E-08
Safe no-effect failures	λ^{NE}	From FMEA	1.46E-06
Diagnostic coverage:	DC	$\lambda_{DD} / (\lambda_{DU} + \lambda_{DD})$	0%
Safe Failure Fraction:	SFF	$(\lambda_{SD} + \lambda_{SU} + \lambda_{DD}) / \lambda$	18 %
Channel equivalent down time	t_{CE}	$(\lambda_{DU} / \lambda_D)(T/2 + MTTR) + (\lambda_{DD} / \lambda_D) MTTR$	1.10E+03
PFD_{AVG} (using 61508-6 equation)	PFD_{AVG}	$(\lambda^{DU} + \lambda^{DD}) t_{CE}$	5.30E-05
PFD_{AVG} (using simplified equation)	PFD_{AVG}	$\lambda^{DU} (T / 2 + MTTR) + (\lambda^{DD} MTTR)$	5.30E-05
PFD_{AVG} (using IEC 61508-6, equation)	PFD_{AVG}	$1 - \varepsilon^{-(\lambda_{DD} + \lambda_{DU}) t_{CE}}$	5.30E-05
SIL capability (Low demand mode)			SIL 1

DC and SFF of SF (close/open) type B wz diag.



FMEA of the (close/open) Circuit type B wz diag.

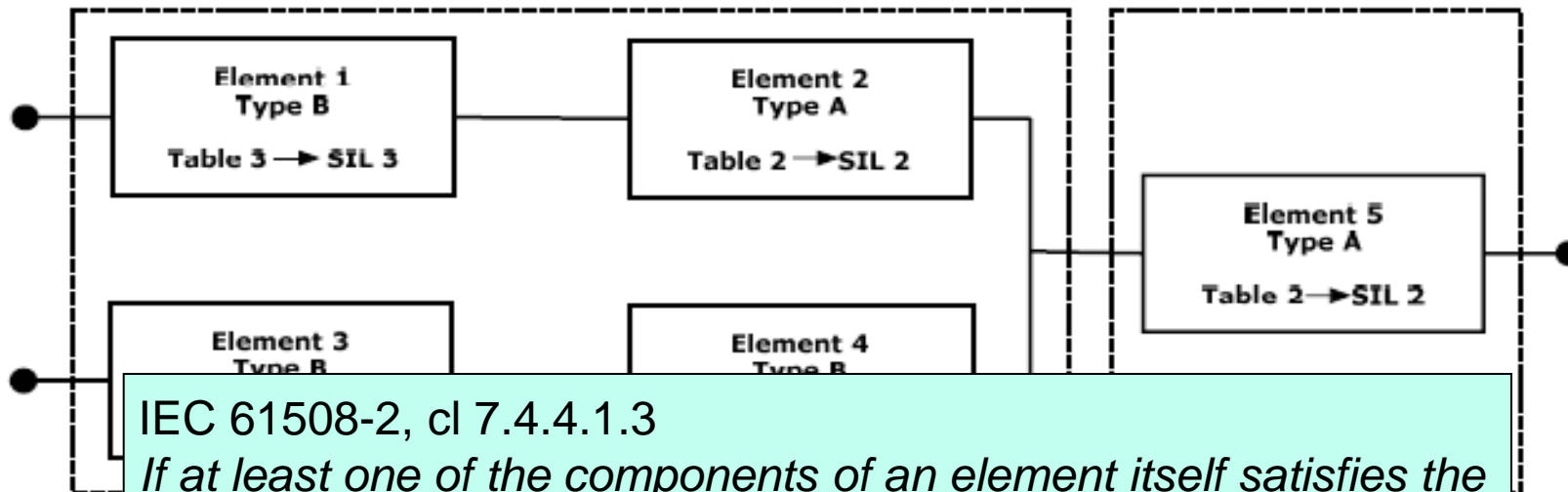
No.	Values	Description	Component Failure Rate	Failure modes	Failure modes types	Qty of	safe=S danger=D	Diagnostic Detect=Y	Redundancy	safe=S danger=D	Diagnostic Detect=Y	IEC61508 Annex A, D.coverage	Safe Rev'led	Safe Un-rvld	Dangrs Detect	Dangrs Un-detec	Safe No-effect
1	R1	Resistor															
23	R23	Resistor															
22	C1	Capacitor															
26	D1	Diode															
32	Q1	MOSFET															
43	IC4	BUFFER IC															
			safe=S danger=D no-effect=N	Diagnostic Detect=Y Undet=N	Redundancy ?		safe=S danger=D no-effect=N	Diagnostic Detect=Y Undet=N		safe=S danger=D no-effect=N	Diagnostic Detect=Y Undet=N	IEC61508 Annex A, D.coverage					
1			Safe Rev'led	Safe Un-rvld	Dangrs Detect	Dangrs Un-detec	Safe Rev'led	Safe Un-rvld	Dangrs Detect	Dangrs Un-detec	Safe No-effect						
23																	
22		COMPARA															
48	IC3																
26			0 d 0.00037	yes	No	0 d 0	3.7E-05	4.1E-06	medium	0	1						
32			0.00037 s 0	no	No	0 s 4.1E-05	0	0	medium	0	1						
43			0 d 0	yes	No	0 d 0	0.00036	0.00004	medium	0	1						
53	IC2	74LVC2G0	0 d 0.0058	yes	No	0 d 0	0	0	medium	0	1						
			0 d 0	yes	No	0 n 0	0.00223	0.00025	medium	0	1						
			0 d 0	yes	No	0 n 0	0	0	medium	0.0086	1						
60	uP	Microcontr	0 d 0	yes	No	0 n 0	0	0	medium	0.0086	1						
			0 n 0	no	No	0 n 0	0	0	no diagnostics	0.0086	1						
			0 s 0	no	No	0 n 0	0	0	no diagnostics	0.0088	0						
		Microcontroller PIC12 small controller - PIN 28 Open Coil FB	0 0.00028	0	0	0 0	0	0	low	0	0.0086						
			0.0091	0.00714 open	0	1 s 0	yes	No	n	No	low	6.5E-05	0	0	0	0	0.0091
			0.0091	0.00714 short to +	1	s	yes	No	n	No	low	6.5E-05	0	0	0	0	0.0091
			0.0091	0.00714 short to -	1	s	yes	No	n	No	low	6.5E-05	0	0	0	0	0.0091
			0.0091	0.00714 short to pin above	1	s	yes	No	n	No	low	6.5E-05	0	0	0	0	0.0091
			0.0091	0.00714 short to pin below	1	s	yes	No	n	No	low	6.5E-05	0	0	0	0	0.0091
		Microcontroller PIC12 small controller - UN-USED PINS	0.0091	0.5714 NOT USED	1	n	no	No	n	No	no diagnostics	0	0	0	0	0	0.0143
61	sol	Thompson solenoid	0.0152	0.52 short	1	d	yes	No	n	No	low	0	0	0.00474	0.00316	0	0.0152
			0.0152	0.28 sticking	1	d	yes	No	n	No	low	0	0	0.00255	0.0017	0	0.0152
			0.0152	0.14 spring failure	1	d	yes	No	n	No	low	0	0	0.00128	0.00085	0	0.0152
			0.0152	0.06 open	1	d	yes	No	n	No	low	0	0	0.00055	0.00036	0	0.0152

FMEA of the (close/open) Circuit type B

1oo1 EQUATIONS

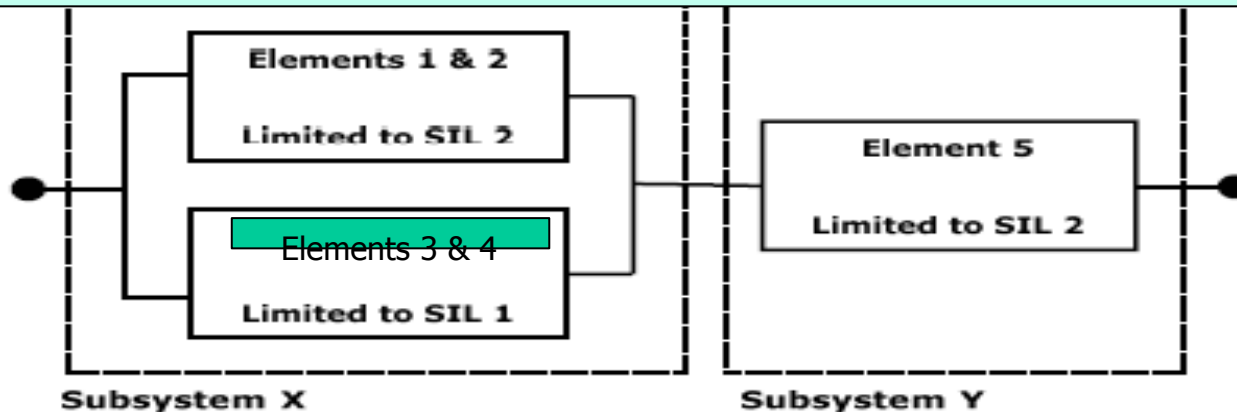
Parameter name	Symbol	Equation / source	Close/Open with diag
Proof Test Interval	T1	Given, for this example	2190
Mean Time To Repair	MTTR	Given, for this example	8
Type A/B	type A	Given, for this example	type b
Total failures:	λ	From FMEA	9.42E-08
Safe diagnosed failures:	λ^{SD}	From FMEA	2.04E-08
Safe undiagnosed failures:	λ^{SU}	From FMEA	2.38E-08
Dangerous diagnosed failures:	λ^{DD}	From FMEA	3.22E-08
Dangerous undiagnosed failures:	λ^{DU}	or High demand mode, PFH per (hour)	1.77E-08
Safe no-effect failures	λ^{NE}	From FMEA	1.26E-06
Diagnostic coverage:	DC	$\lambda_{DD} / (\lambda_{DU} + \lambda_{DD})$	64%
Safe Failure Fraction:	SFF	$(\lambda_{SD} + \lambda_{SU} + \lambda_{DD}) / \lambda$	81 %
Channel equivalent down time	t_{CE}	$(\lambda_{DU} / \lambda_D)(T/2 + MTTR) + (\lambda_{DD} / \lambda_D) MTTR$	3.97E+02
PFD_{AVG} (using 61508-6 equation)	PFD_{AVG}	$(\lambda^{DU} + \lambda^{DD}) t_{CE}$	1.98E-05
PFD_{AVG} (using simplified equation)	PFD_{AVG}	$\lambda^{DU} (T / 2 + MTTR) + (\lambda^{DD} MTTR)$	1.98E-05
PFD_{AVG} (using IEC 61508-6, equation)	PFD_{AVG}	$1 - \varepsilon^{-\lambda^{DD} + \lambda^{DU} t_{CE}}$	1.98E-05
SIL capability (Low demand mode)			SIL 1

FMEA of the (close/open) Circuit type B

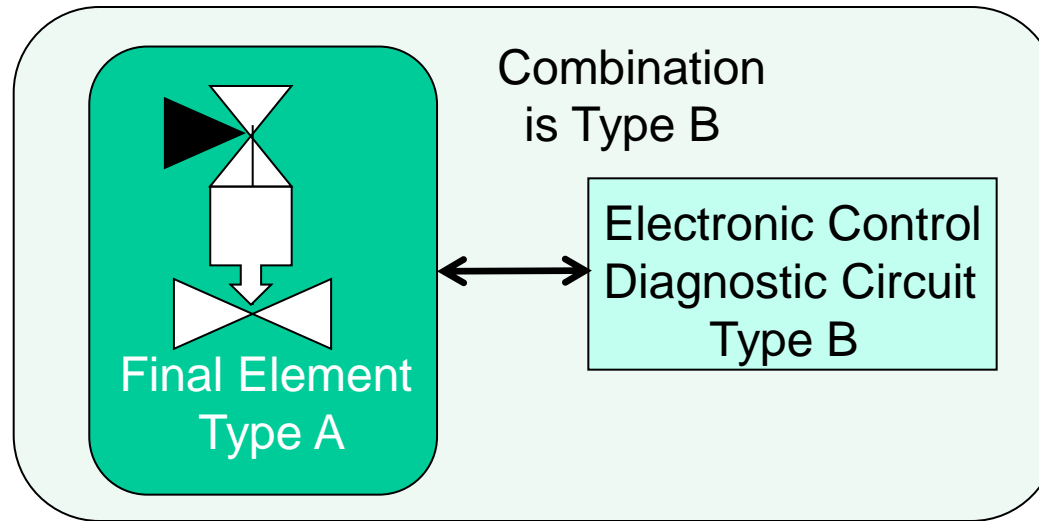


IEC 61508-2, cl 7.4.4.1.3

If at least one of the components of an element itself satisfies the conditions for a type B element then that element will be regarded as type B rather than type A.



FMEA of the (close/open) Circuit type B



- ④ Diagnostics can be internal or external as defined in clause (part 2, 7.4.9.4)
- ④ Diagnostics Internal or external, its random hardware failures assessment must be considered
- ④ Ed.2 says (part 2, clause 7.4.9.4-J) : The failure rate of the diagnostics, due to random hardware failures should be specified. Why? to enable the derivation of the safe failure fraction (SFF) and DC of the element .

FMEA of the (close/open) Circuit type B

- ④ The example has demonstrated that diagnostics used for example (PST) is a good credit for improving PFD and SFF of the final element.
- ④ New SFF of the final element is improved, but the final element should be assessed to IEC 61508-2 table 3 (type B), hence the product is SIL1, otherwise assessment to IEC 61508 is violated.
- ④ The big question is why final elements are claimed as SIL 3 if PST is used?
- ④ The verdict accepted by end users, why, these elements approved by recognised agencies, hence results accepted in good faith

FMEA of the (close/open) Circuit type B

- ④ Market is still under the belief that PST is a diagnostic tool , hence credit is claimed for without further assessment to PST firmware.
- ④ Ignoring that PST is a complementary test to FST coverage.
- ④ The good news is that the WIB process automation , FE WG has addressed the PVST certification as published in the 69th Annual Instrumentation Symposium for the process industry in Jan. 2014.
the link: <http://instrumentation-symposium.che.tamu.edu/2014-symp/2014-program>.
- ④ PVST article can be downloaded from:
<http://www.siracertification.com/resources.aspx?page=173>
- ④ Recommendation is to form a FS group such as T6A acting as independent body for market review certification.

Conclusion

- ④ Using Annex A Table requires deep knowledge in electronics analysis to select the appropriate DC figure.
- ④ Less competent assessors will lead to produce high uncertainty in the SIL calculation.
- ④ Working FMEA is time consuming, for high dense ICs.
- ④ Conducting FMEA for type B product must work in parallel with SW analysis to identify if diagnostic measures used.
- ④ Insertion test results must be provided for every claimed diagnostic block.

Question Time

Thank you for your attention





Luis Duran

Functional Safety Conference 4/5 Nov 2014

Cybersecurity Safety and Security

- Why is it important?
 - It's real and it's here NOW
- What is it?
 - Faces of Cyber Security
 - Impact on Industrial Control Systems
- Safety and Security
- Myth 1: Safety Systems are “isolated”
- Myth 2: Let IT “fix it”
- Myth 3: All we need is Certification
- Myth 4: There's no hope

Why is it important?

Examples of recent events

FINANCIAL TIMES
ft.com/global/economy

September 23, 2010 7:39 pm

Stuxnet worm causes worldwide alarm

By Joseph Menn and Mary Watkins

No one knows the ultimate goal of the Stuxnet worm, which has infected an unknown number of industrial control systems. It sends out instructions to machinery and factories to shut down. It could destroy gas pipelines, cause power plants to explode. Perhaps it already has.

Forbes

INVESTING | 10/21/2011 @ 12:27PM | 9,193 views

'Duqu' Virus Likely Handiwork Of Sophisticated Government, Kaspersky Lab Says

+ Comment Now + Follow Comments

the guardian | The Observer

News | Sport | Comment | Culture | Business | Money | Life & style

News | Technology | The networker

Series: The networker

How Flame virus targeted everything for control

The Flame virus went undetected for months, but a security firm. Now they've traced it to a group of hackers who targeted the world's PCs from malware.

The Duqu Trojan probably a government operation. What is it looking for? And which countries are behind it remains a mystery.

regular threats, like botnets, but the Duqu, considered the most sophisticated of

BBC NEWS TECHNOLOGY

Home | UK | Africa | Asia | Europe | Latin America | Mid-East | US & Canada | Business | Health | Sci/Environment

17 August 2012 Last updated at 14:22 GMT

Shamoon virus targets energy sector infrastructure

1.1K + Share

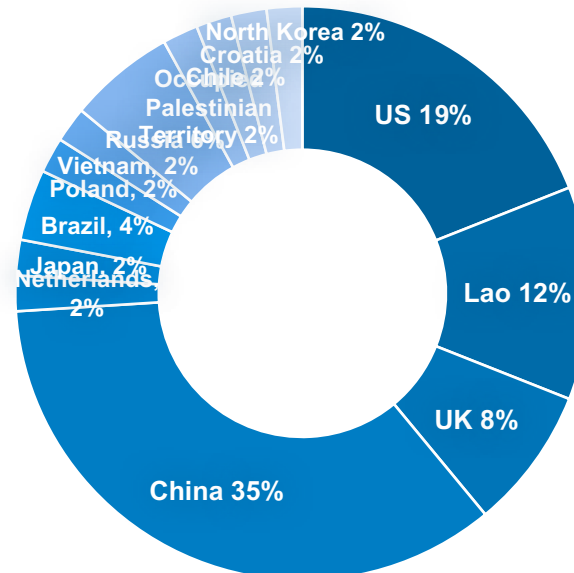
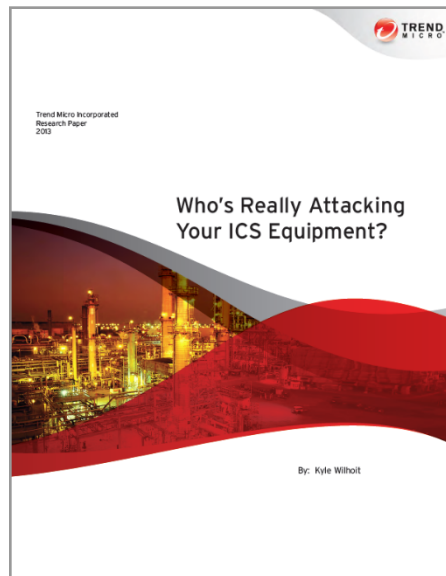
Why is it important?

Other real case examples

1. IT department use vulnerability scanning tools

2. Neeris brought in by USB-stick

3. A control system could be targeted with 39 attacks in 28 days!



What is Cyber Security?

Different faces



Hacking



**Malicious
software**



**Employee
Mistake**

- **Safety:**

Freedom from unacceptable risk of physical injury or of damage to the health of people, either directly or indirectly as a result of damage to property or to the environment.

IEC 61508

- **Security:**

Preventing intentional or unintentional interference with the proper and intended operation, or inappropriate access to confidential information in industrial automation and control systems

ANSI/ISA-99.00.01-2007

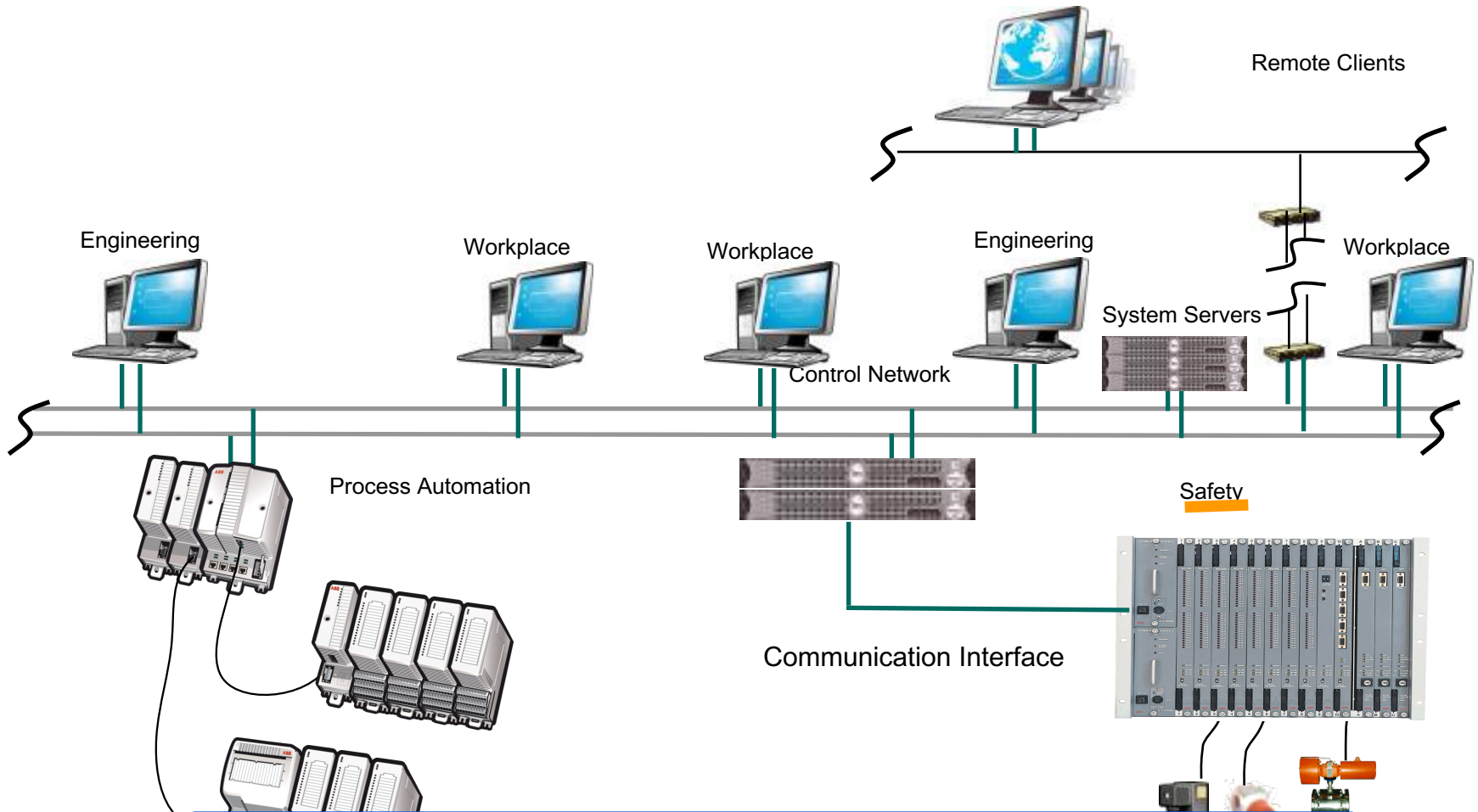


Cyber Security and Safety: Avoid problems

Somebody does something that causes something bad

Who does what (Cause)	Problem type	Causes what (Effect)
<p>Laws of Nature causes unit failure</p> <p style="text-align: right;">Not on purpose</p> <ul style="list-style-type: none"> ▪ ICS unit ▪ Process equipment <p>“Good” person makes mistake (Engineering, operation, maintenance, ...)</p>	<ul style="list-style-type: none"> ▪ Spoofing ▪ Tampering ▪ Repudiation ▪ Info disclosure ▪ Denial of Service ▪ Elevation of Privileges 	<p>People health problem</p> <p>Environmental problem</p> <p style="text-align: right;">Safety</p> <p>Economical loss</p> <p>Inconvenience</p>
<p>“Evil” person</p> <ul style="list-style-type: none"> ▪ hacker ▪ disgruntled employee (insider) <p>penetrates ICS</p> <ul style="list-style-type: none"> ▪ targeted ▪ not targeted <p>Physical attack</p> <p style="text-align: right;">On purpose</p>	<p style="text-align: center;">Not Cyber Security</p> <ul style="list-style-type: none"> ▪ Confidentiality ▪ Integrity ▪ Availability <p style="text-align: center;">Not required for SIL certification Handled by Security</p>	

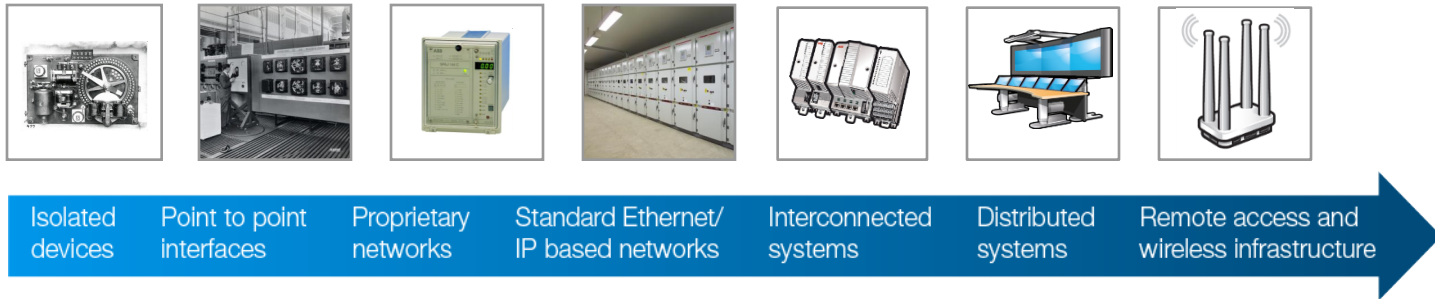
Safety System Isolation: Air Gap



SIS operation shall not be dangerously affected by Failures, Operation or Maintenance of the BPCS

What is Cyber Security?

Why is it an issue?



Threats to standard IT systems largely also apply to ICS



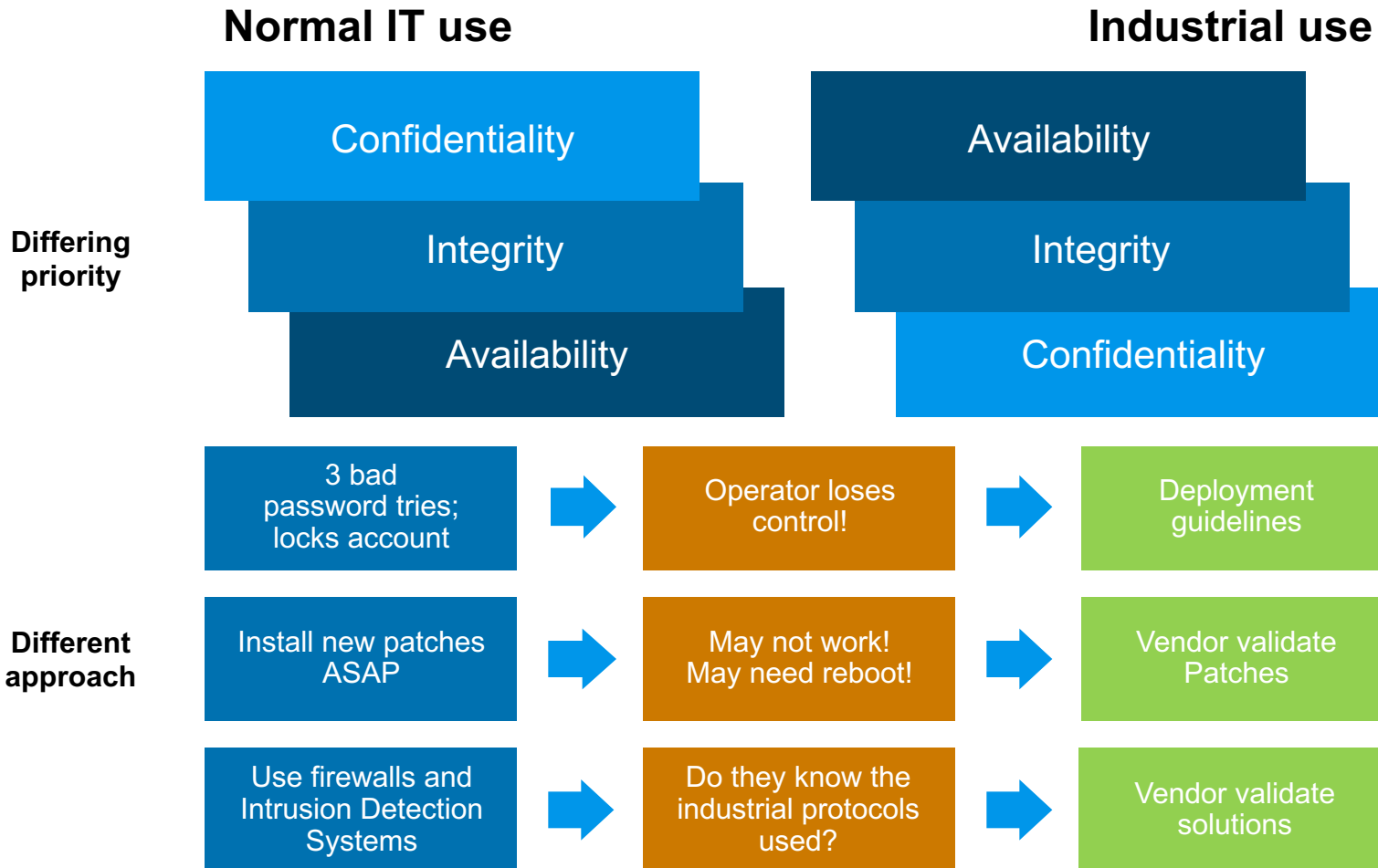
IT focused criminal ecosystem



Increased risk!

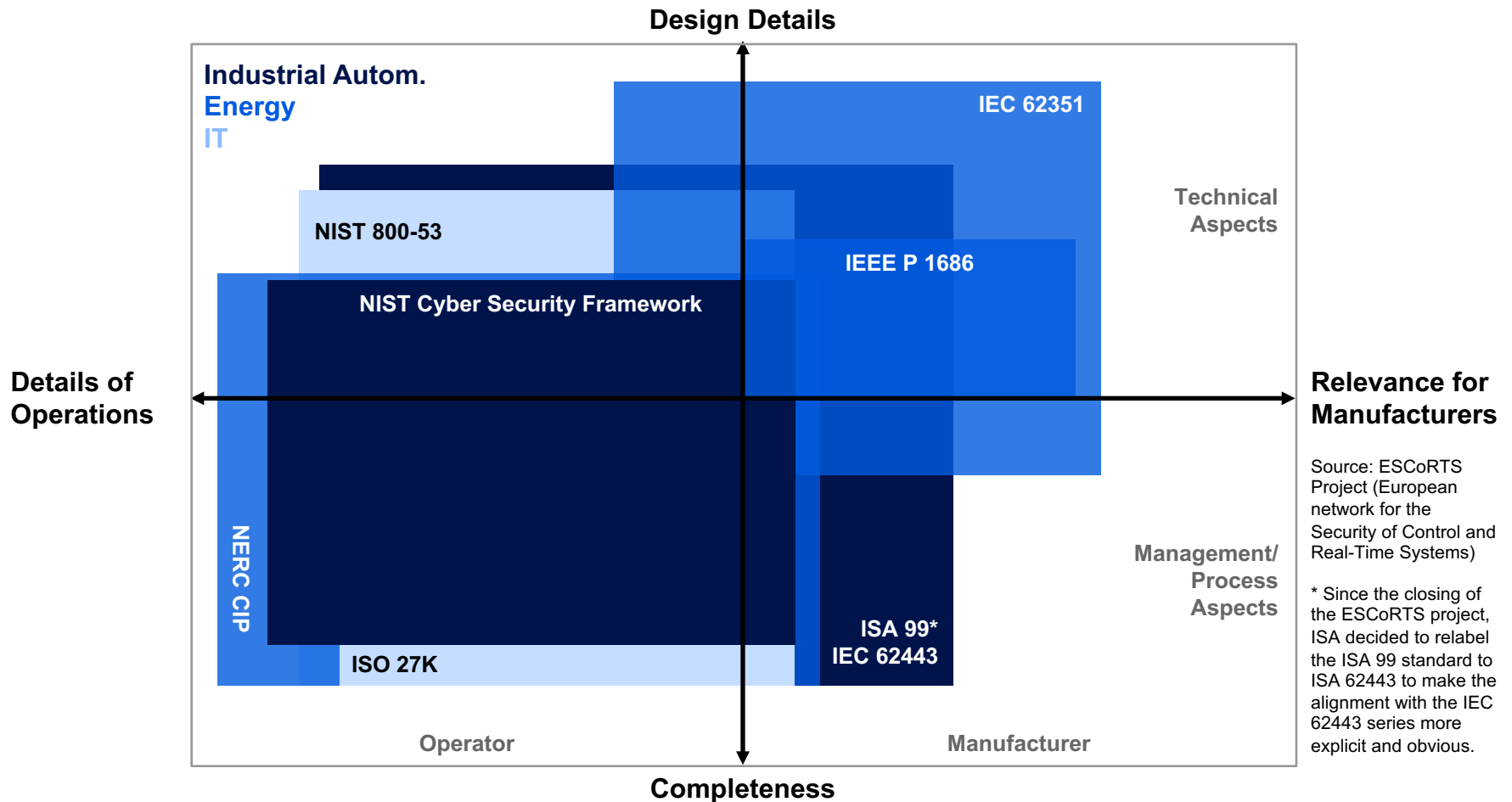
Cyber security best practices

Normal IT vs. Industrial best practices



Cyber security best practices

A lot of support available



Source: ESCoRTS Project (European network for the Security of Control and Real-Time Systems)

* Since the closing of the ESCoRTS project, ISA decided to relabel the ISA 99 standard to ISA 62443 to make the alignment with the IEC 62443 series more explicit and obvious.

Cyber security best practices

Defense in Depth

The coordinated use of multiple security measures, addressing people, technology, and operations.

Physical Security

Procedures and Policies

Firewalls and Architecture

Computer Policies

Account Management

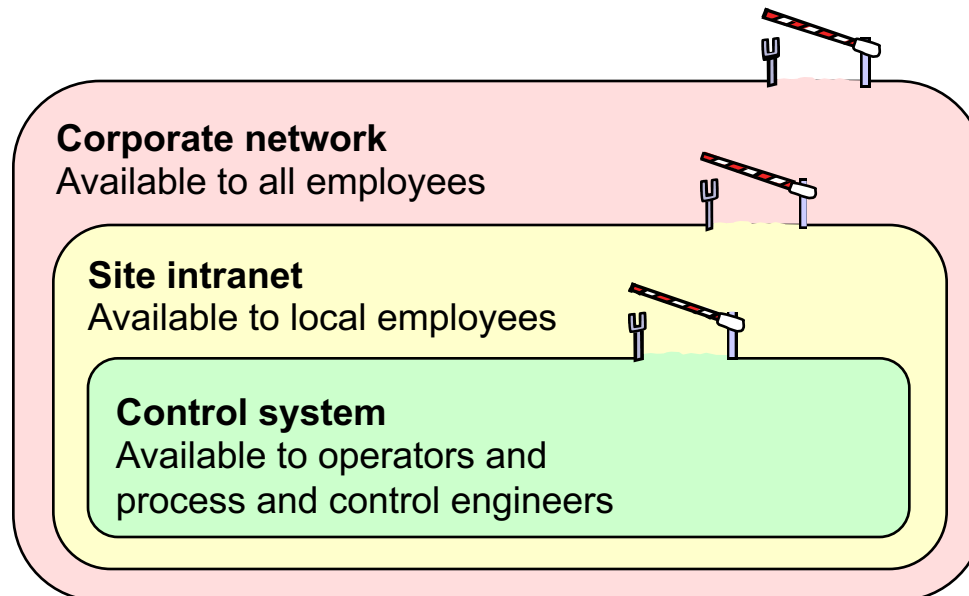
Security Updates

Antivirus Solutions



Security Zones

- Different zones for different security levels
 - All resources in the same zone must have the same minimum security level (trust level)
 - Access between zones only through secure conduits
 - Provides perimeter protection of critical system assets
 - Basic principle in the ISA 99/IEC 62443 series of standards

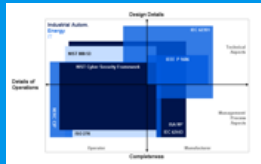


Cyber security best practices

Implement a Security Management System

1.

Standards:
Guidelines



Risk
Assessment



Management
Buy-in



Security
Policy



2.

Balance Security Measures:
Value for me \leftrightarrow Value for X \leftrightarrow Mitigation cost
Combine measures:
Defense in Depth
Work with system vendors.
Request selected measures.



3.

Incident response
Disaster recovery

Audit policy
compliance

4.

Power and productivity
for a better world™





Rob Pashby & John Walkington

InstMC Functional Safety Conference 4/5 Nov 2014

Legacy Safety Instrumented Systems: When to Maintain or Evolve?

- Introduction and background to legacy safety systems
- The technical drivers for change
- Engineering and meeting good practice
- Identification of a strategy to maintain or evolve?
- Conclusions



Introduction

Background to legacy safety systems

- Increased application of E/E/PES technology platforms over the last 30 years
- Asset Owners will have had good and/or poor experience in terms of reliability and availability
- Operation and maintenance processes will have been developed to address:
 - Equipment lifecycle and spares availability issues
 - Additional spurious tripping caused by increasing system degradation
- Set against a backdrop of continued high profile industry incidents
- A changing regulatory and standards backdrop on meeting minimum expectations and industry good practice i.e. IEC61511



The Technical Drivers for Change - 1

- MOC processes with a mixture of technology solutions that comply with differing engineering standards
- Maintainability, product lifecycle management & obsolescence
- Alignment to operating plant life expectancy i.e. shutdown/decommissioning
- Maintaining SIS operational knowledge and experience
- Increasing servicing and call-out costs, increased spares usage and increasing production downtime



The Technical Drivers for Change - 2

- Ensuring safety measures are maintained during the final stages of technology life
- MoC implications as safety functions are either added or removed
- Consideration of any changes in asset information management requirements for asset improvement
- Consideration of any impact from the local regulatory authorities and industry good practice expectations



The Engineering Process

The Impact of Change

- Root cause failures associated with 'safety instrumented safety systems'
- Asset Owners and the Supply Chain are trying to apply a safety management lifecycle (FSMS) approach
- Design & engineering solution matches the Asset Owners risk reduction requirements
- Asset Owners are seeking a supply chain partner who can deliver the solution and address any potential issues via the management of functional safety



Demonstrating Industry Good Practice

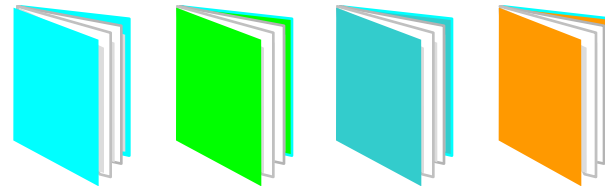
- Managing technology that has differing standards, detailed supporting documentation and prescriptive ‘back in the day’ design assumptions
- Difficulties of aligning the older information with the requirements of current good practice approaches i.e. IEC 61511
- Identification of the true risk reduction SIF’s within the complexity of the existing SIS I/O count with the potential lack of traceability to the associated plant specific hazards
- Implementing MOC with risk assessments that require the problem to be re-visited from first principles:
 - Cost
 - Expertise (In-house or bought-in)
- *Is there a fear that a first principle assessment may wake-up some sleeping dogs?*

What constitutes Good Practice for SIS?

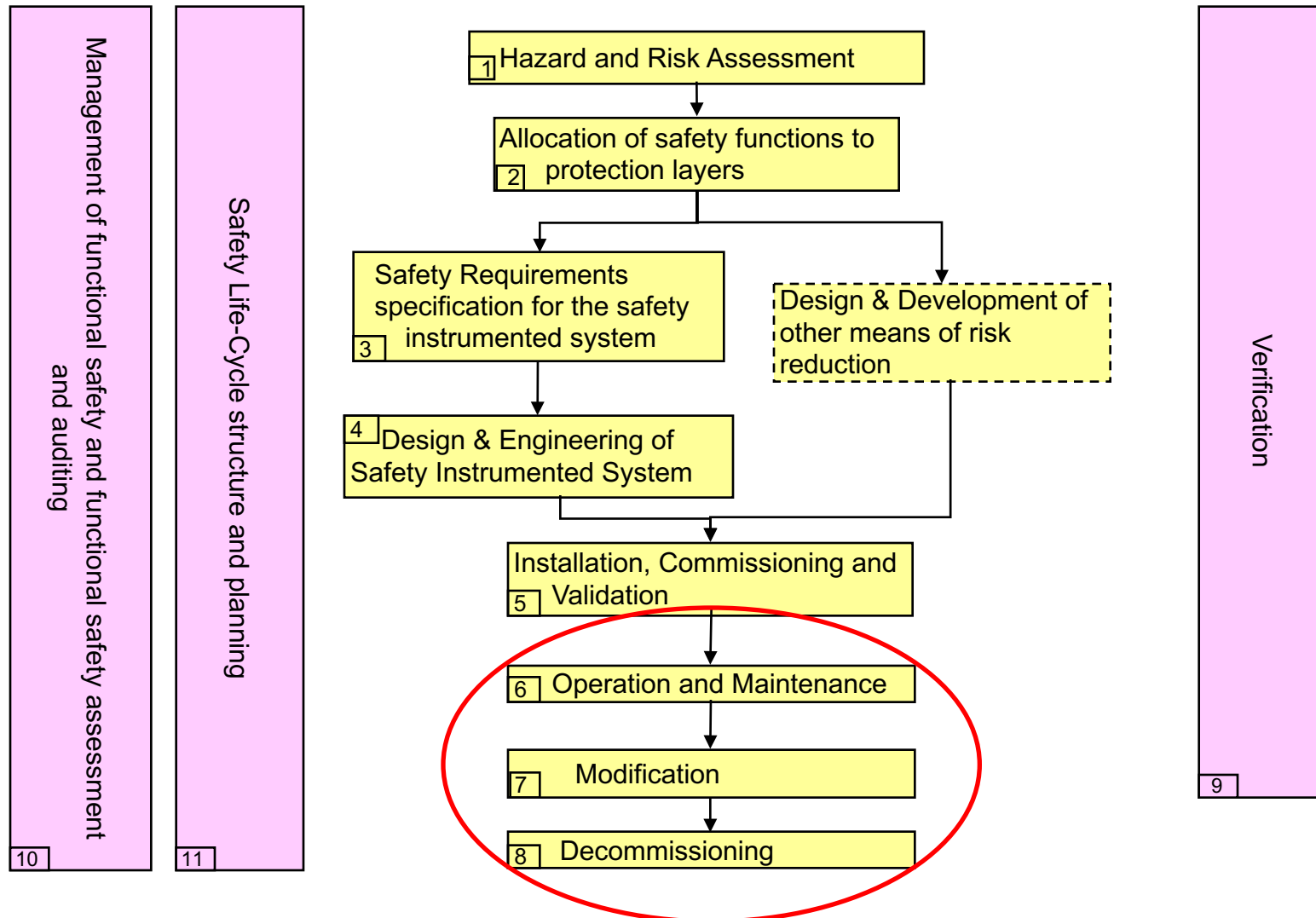
- Industry wide globally adopted standard(s) for safety instrumented systems
- Used within the Process Industries since 1998 and the Asset Owner variant 61511 since 2003 – now seen as Industry norms for SIS
- Asset Owners will develop RFQ or ITT with requirements for compliance to these standards
- Regulators and corporate stakeholders for safety will audit facilities using IEC 61508/61511 as the audit content / references to good practice
- Regulators use it as a good practice benchmark when undertaking incident investigations



Sector & Product Standards



Lifecycle Management O&M Phases



IEC61511 Safety Lifecycle

The Safety Systems we are Addressing

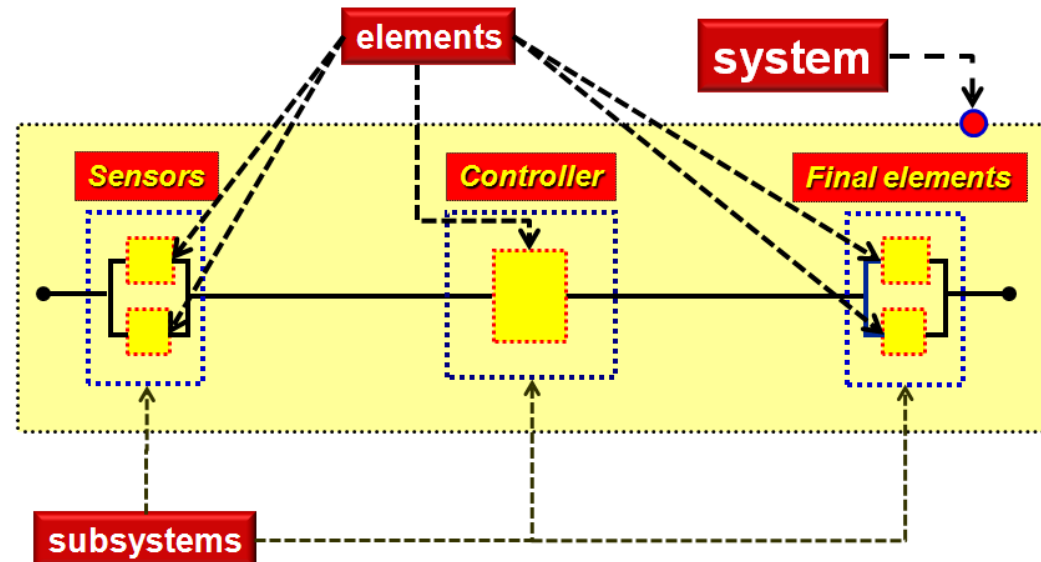
- The SIS is intended to implement the required safety function to the necessary level of integrity
- Safety instrumented functions necessary to achieve a safe state for the "Equipment Under Control", or to maintain it in a safe state.

ESD

PSD

BMS

Etc.....



The safety function is made up of all the element safety functions

Harnessing Today's Technology

- New technology platforms are certificated in alignment with IEC 615108 Ed 2 / IEC 61511
- Compliance with a lifecycle approach to managing risk which is allocated into protective measures
- Provide clarity on separation between control and dedicated safety systems
- Optimised fully integrated asset management solutions to increase productivity safely
- Asset management systems that monitor the performance of the SIS
- Alarm management, ergonomics and human factors are included
- *When is the right time to switch from maintaining my older system to embrace the new technology?*



- Managing of three key requirements
 - Modifying the system to change, add or remove safety functionality dependent on operating requirements for existing plant, new plant, decommissioning, etc.
 - Maintaining the system to the 'as new condition' including performing proof tests, recommended maintenance and repairs
 - Applying items 1&2 above to plant operating life expectancy
- Application of MOC processes
 - Impact & gap assessments completed (end user and SIS system level)
 - Documentation is updated and maintained as valid
 - Basis of safety is periodically assessed i.e. every 3-5 years
 - Identification of appropriate Techniques and Measures
- Competency assessment
 - Requirements for Authors, Reviewers and Approvers

Time to Evolve? – 1

Operational Trending

- *Are you seeing the following?*
 - Increase in spares optimisation
 - Formal notification of OEM support closure date
 - Corporate memory drain or local resource availability to respond
 - Fire-fighting rather than proactive management and planning
 - Increase within the plant spurious trip rates
 - Audits and FSA's identifying increasing trends on overrides and bypasses being left in position for 'normal running'



Time to Evolve? - 2

Decide on a Strategy

- Impact assessment should also include the key area of ‘Operating Plant Life Expectancy’
- Formulate a strategy plan based on the likely outcomes identified as the following strategies:
 - Maintain to End of Life
 - Modify and Evolve to Meet New Operating Requirements
 - Apply a “Sticking Plaster” Approach
 - Go for a Direct and Full Replacement



Time to Evolve? – 3 Strategies 1 & 2



- *Strategy 1: Maintain to End of Life*
 - Good basis of design available
 - Not seeing the KPI's for failures/increasing costs for the systems as stands
 - Prepared to maintain for life of plant with established resources
- *Strategy 2: Modify and Evolve to Meet New Operating Requirements*
 - Good basis of design available
 - KPI's may or may not be providing evidence of failures/cost
 - Plan for evolution for life time of plant – change in operating strategy

Time to Evolve? – 4 Strategy 3a and 3b



- *Strategy 3a: Sticking Plaster (short plant life)*
 - No good basis of design available
 - Recognition that the SIS is failing/cost spiraling, KPI's supporting the issues
 - Not prepared to replace during remaining plant life
 - Will undertake small scale installation of compliant SIS to run in parallel with legacy
- *Strategy 3b: Sticking Plaster (interim solution)*
 - Good or bad basis of design potentially available
 - Recognition that the SIS is failing/cost spiraling, KPI's supporting the issues
 - Are prepared to replace during remaining plant life
 - Need breathing space to implement new SIS solution – interim strategy plan to be evolved prior to full upgrade
 - Will undertake small scale installation of IEC 615108 compliant SIS to run in parallel with legacy

Time to Evolve? – 5 Strategy 4

- *Strategy 4: Direct Replacement*
 - Good or bad basis of design potentially available
 - Recognition that the SIS is failing/cost spiraling, KPI's supporting the issues
 - Are prepared to replace during remaining plant life
 - Will schedule evolution in timely manner i.e. plan to evolve next 3-5 year period



Time to Evolve? – 5

Functional Safety Focus

- For all options, once the strategy is agreed; compliance to a functional safety management system will be crucial for successful delivery
- Importance for focus will be on:
 - Revalidated basis of safety leading to the development of a detailed SRS
 - Cause & effects from existing SIFs are accurate
 - Designing the change to Target SILs
 - Ensuring verification and validation ensures compliance to the SRS



- A “maintain” or “evolution” strategy for your SIS requires a structured review and should form a key part of your overall asset management business philosophy
- Once all implications have been addressed and a strategy agreed, then implementation should be in accordance with IEC 61511 principles
- By doing so, your operational strategy is understood and endorsed by all relevant stakeholders and is much more preferable than reactive management i.e. fire-fighting the effects of obsolescence and the potential for failure on demand.
- A proactive functional safety management approach should be in place and be seen as a senior management requirement for development and implementation, regardless of the strategy to be applied



Power and productivity
for a better world™





IEC 61131-6

Edition 1.0 2012-10



Rail

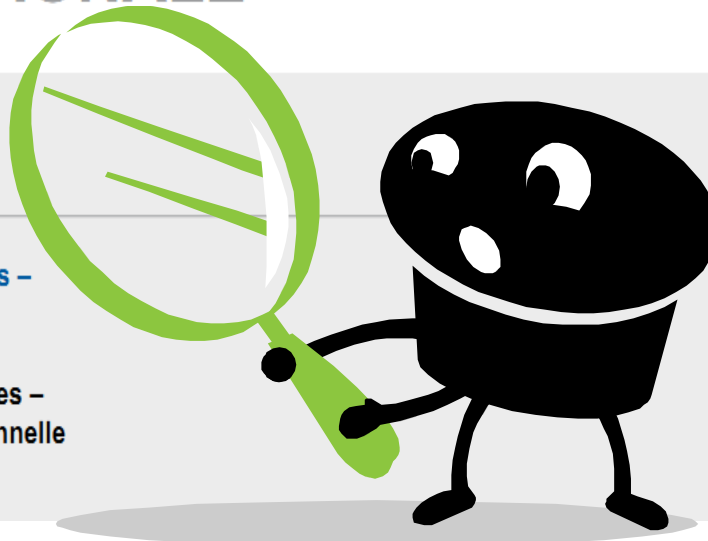
Choose certainty.
Add value.

INTERNATIONAL STANDARD

NORME
INTERNATIONALE

Programmable controllers –
Part 6: Functional safety

Automates programmables –
Partie 6: Sécurité fonctionnelle



Applicability of IEC 61131-6 for Programmable Controllers



intention of the standard

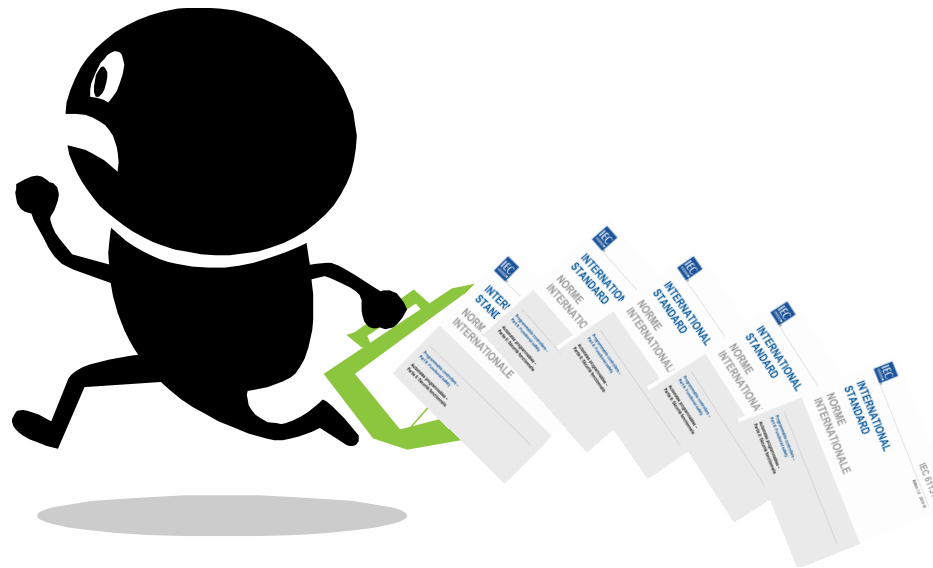
applicability

pros and cons

IEC 61131-x for PLC

IEC 61508, IEC 62061 and ISO 13849-1 add-on for S-PLCs

IEC 61131-6 Edition 1.0 released since 2012



... so what?

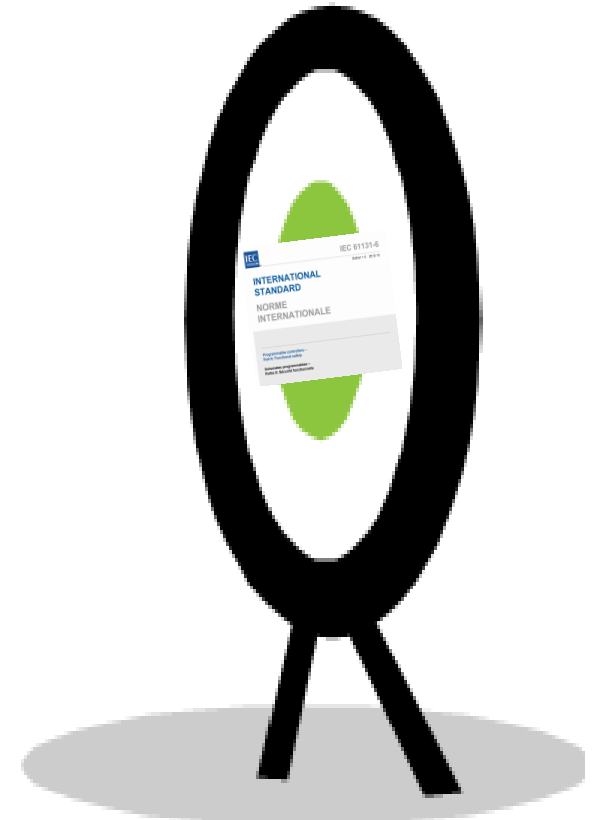
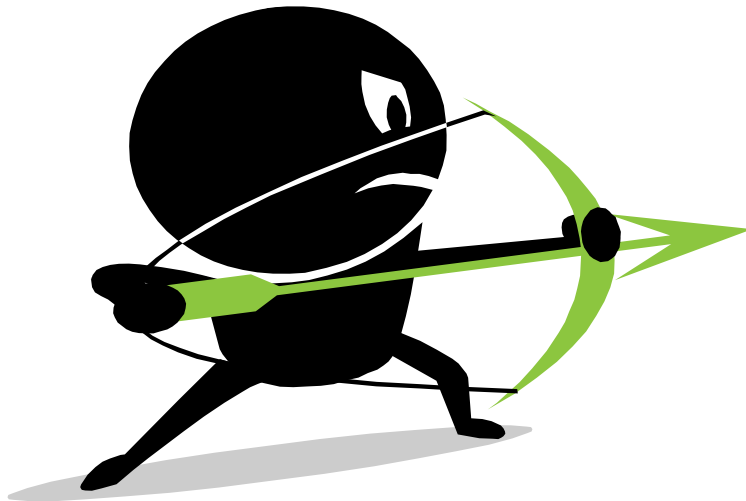
let's take a closer look



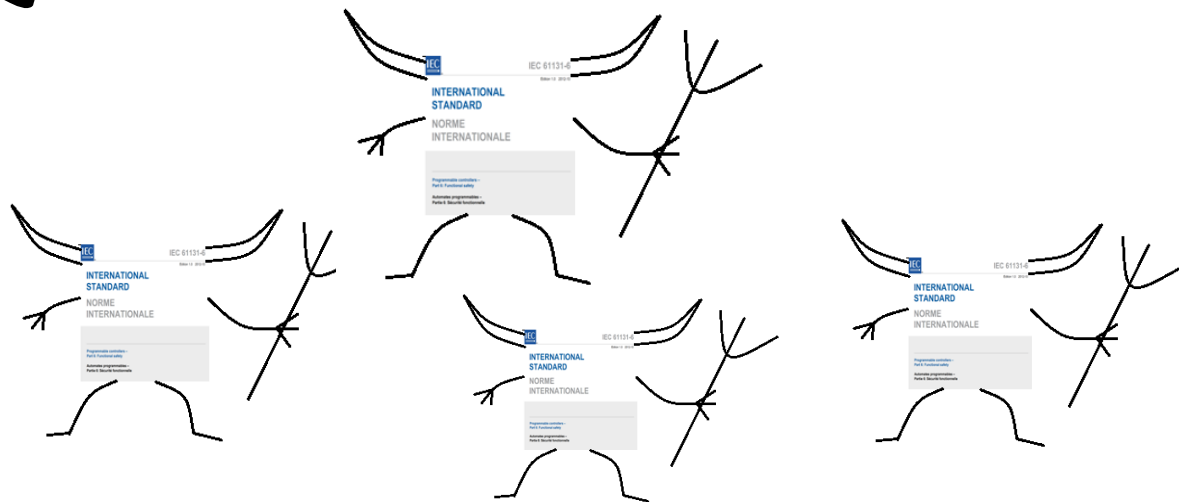
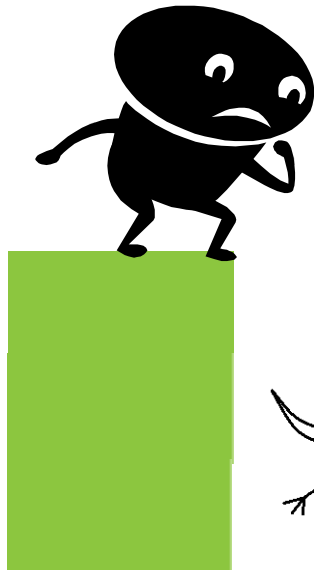
„Cook Clever“ recipt for Safety PLCs

less fuzziness for PLC developers

less confusion of assessors



- not mandatory according to the european machinery directive
- no additional requirements for „state-of-the-art“ S-PLCs
- up to now no references from other standards like e.g. IEC 61511

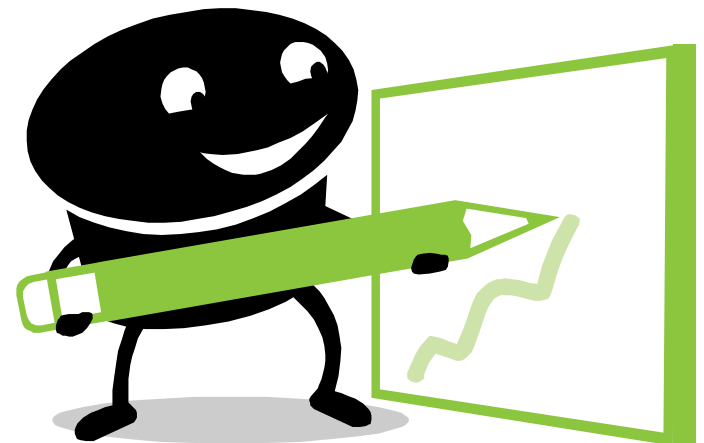


- easier to read than IEC 61508
- precise minimum requirements
- examples for several items like FMEA, tools, SRS etc.
- clear references for applicative environment
- easy conclusion from IEC 61131-6 to IEC 61508



Advantage for tenders and installations:

- compatibility to sensors & actuators as IEC 61131-2 becomes mandatory for safety
- comparability of products
- compatibility to other standards (same SIL/HFT/...) and easier integration



- easier to read than IEC 61508
- precise minimum requirements
- examples for several items like FMEA, tools, SRS etc.
- clear references for applicative environment
- easy conclusion from IEC 61131-6 to IEC 61508



IEC 61131-6 helps to get a common understanding based on established SIL between users and developers of PLCs and related tooling



easier to read than
IEC 61508

not written 100%
consistent and precise



IEC 61131-6

Edition 1.0 2012-10

INTERNATIONAL
STANDARD

NORME
INTERNATIONALE

Programmable controllers –
Part 6: Functional safety

Automates programmables –
Partie 6: Sécurité fonctionnelle



tailored to S-PLC
development

FSM / Process etc. not
easier to execute



IEC 61131-6

Edition 1.0 2012-10

INTERNATIONAL
STANDARD

NORME
INTERNATIONALE

Programmable controllers –
Part 6: Functional safety

Automates programmables –
Partie 6: Sécurité fonctionnelle



minimum
requirements on
SRS

well...nothing bad here



IEC 61131-6

Edition 1.0 2012-10

**INTERNATIONAL
STANDARD**

**NORME
INTERNATIONALE**

Programmable controllers –
Part 6: Functional safety

Automates programmables –
Partie 6: Sécurité fonctionnelle



clarifications on
Route 1H, Lifecycle,
...

Limitations on “proven
in use” approaches



IEC 61131-6

Edition 1.0 2012-10



INTERNATIONAL
STANDARD

NORME
INTERNATIONALE

Programmable controllers –
Part 6: Functional safety

Automates programmables –
Partie 6: Sécurité fonctionnelle

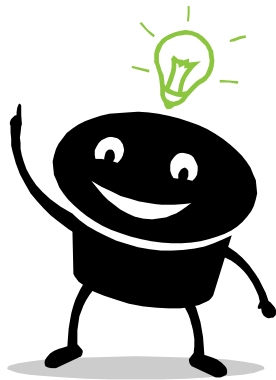
clarifications on
tools, programming
environment ...

some working practice
might have to change



IEC 61131-6

Edition 1.0 2012-10



INTERNATIONAL
STANDARD

NORME
INTERNATIONALE

Programmable controllers –
Part 6: Functional safety

Automates programmables –
Partie 6: Sécurité fonctionnelle

minimum requirements on climate, electrical safety, EMC

strong relation to automation industry, not oil&gas, process industry



IEC 61131-6

Edition 1.0 2012-10

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Programmable controllers – Part 6: Functional safety

Automates programmables – Partie 6: Sécurité fonctionnelle



Higher comparability
EN 61131-2
mandatory

Limitation for “special”
applications possible

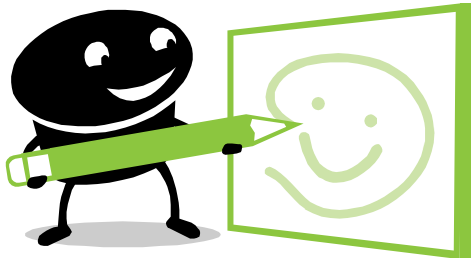


IEC 61131-6

Edition 1.0 2012-10

INTERNATIONAL
STANDARD

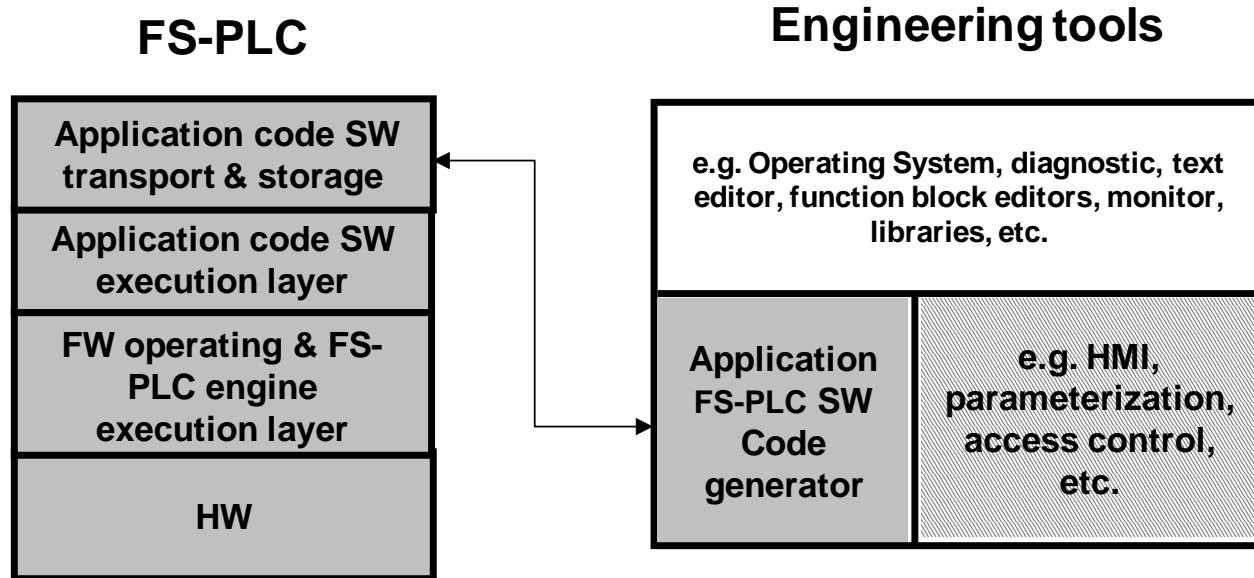
NORME
INTERNATIONALE



Programmable controllers –
Part 6: Functional safety

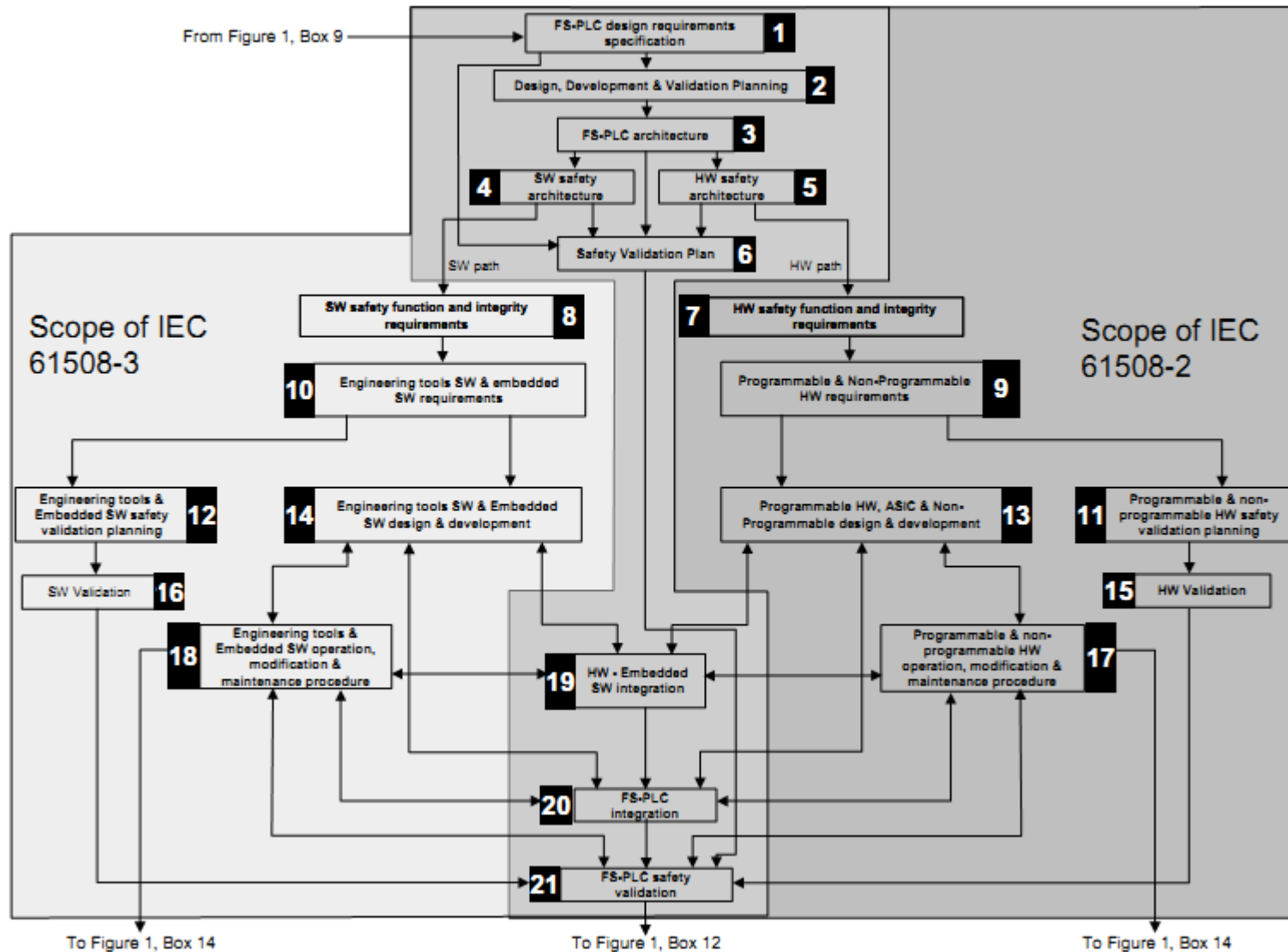
Automates programmables –
Partie 6: Sécurité fonctionnelle

What is part of the S-PLC system?



NOTE 1 Gray blocks are FS-PLC related areas and must be addressed, The white block is not a safety related part of FS-PLC, i.e. interference free. The cross-hatched block indicates possibility of this item being considered safety-related based on criticality analysis and thus needs to be addressed.

NOTE 2 The examples in white and cross-hatched blocks are for illustrative purposes only and may or may not be determined to be safety related in the application.



DSS=Defined Safe State

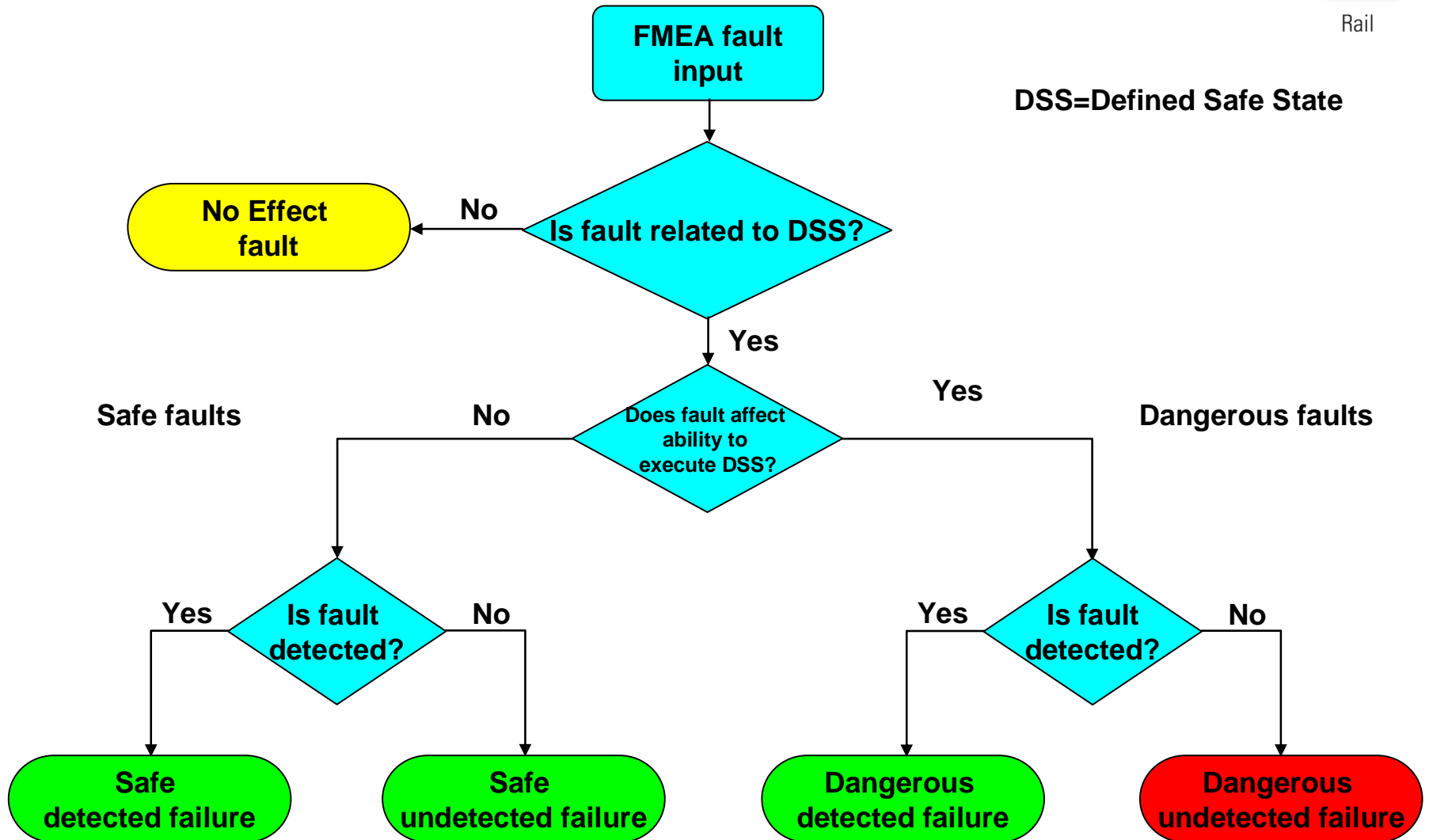
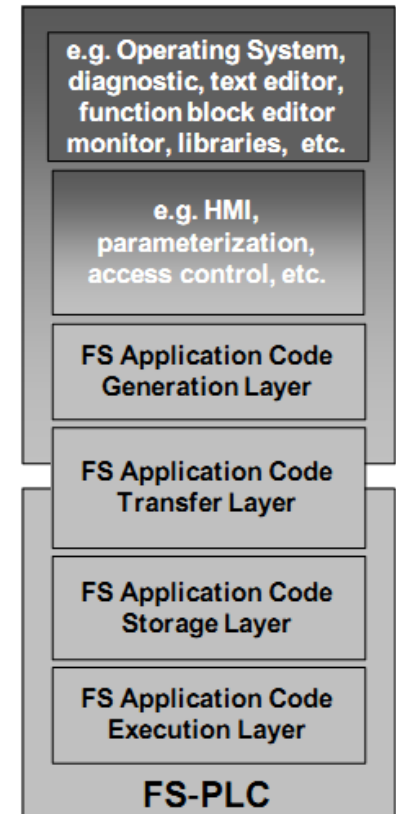


Table 7 – Examples of tool classification

Class of tools ^a	Class	Reasoning
Engineering Tools – PC OS, diagnostic, text editor, function block editor, monitor, libraries, etc	T1	The output of the tool(s) is verified and validated by the user prior to use in a FS-PLC
Engineering Tools – HMI, parameterization, access control, etc.	T1	Generates no outputs which contribute to the executabl the safety rel
Engineering Tools – FS application code generation layer, HMI, parameterization	T3	Generates outputs which contribute to the executa
Engineering Tools – FS application code transfer layer	T3	May directly or indirectly cc code of the safet
FS-PLC – application code storage layer	n/a	Embedded sys
FS-PLC – application code execution layer	n/a	Embedded sys

^a Tools may have different classifications depending on their output or code generation

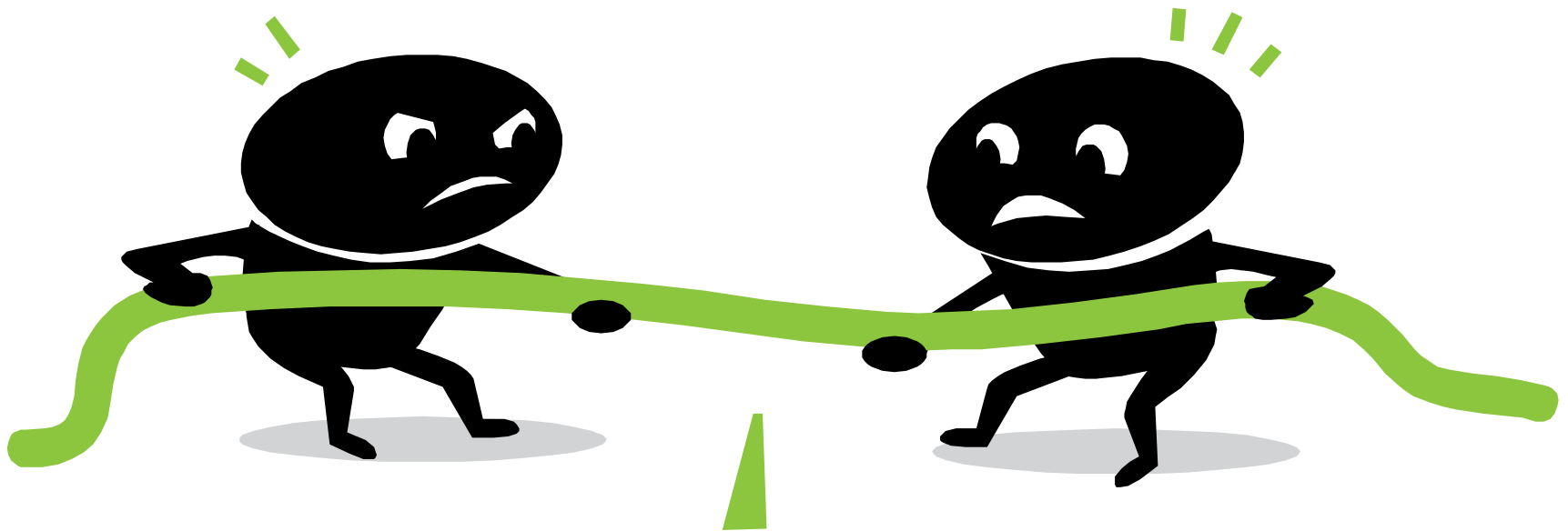
Engineering tools



Result:

usefull= YES

mandatory= NO





Rail

Choose certainty.
Add value.

enjoy the tea & coffee

guido.neumann@tuev-sued.de

+49 89 5791 3233

TÜV SÜD Rail GmbH – Embedded Systems

Barthstraße 16

80339 Munich





Man könnte noch Dinge reinbringen wie „Doku hat keine Probleme gemacht“, Unklarheiten bei Umwelttests etc, sind in Projekten weniger geworden, Firmen machen bessere Angaben in SRS / Handbuch und/oder
Keine wirklich relevanten Änderungen in den Projekten, Diese Norm hätte es nicht wirklich gebrauch, „Anfänger“ und Sensor/Aktor-hersteller profitieren etwas

