ESC
The Technical Safety Company

"Safety in numbers – is target risk really just a number?"

Risk targets, Probability of failure, likelihood of consequences, number of occurrences, Safety Integrity Level (SIL), Risk Matrices and Fault Tree Analysis (FTA)… All these statistical and probabilistic analysis methodologies (as well as other risk management tools) empower us to make decisions, informed of the estimated risk based on the information available, and we often place focus (*and sometimes hope*) on the quantitative aspect of risk management, as the ability to quantify a target and/or a performance requirement can provide us with feeling or achieving as a form of control we can grasp and use to make decisions. ***(Are your decisions based solely on the numbers you have?)***

"Number is the ruler of forms and ideas, and the cause of gods and demons"
-Pythagoras

… but what does history tell us? Does the past really confirm that the numbers we so fondly look forward to estimating are at the core of managing risk?

Key incidents in history like BP Texas, Buncefield, Flixborough, Boeing 737 MAX quote (among other aspects) poor human factors practices, inadequate alarm management, issues with maintenance and control of work, emergency response, specification errors, incorrect or inadequate design practices… (***Noting that none of these are driven by equipment failure rate, so how do we manage them****?*).

In these key historical events, potential mis-estimation of failure rates seems to have played little or no part in the root causes involved in the incidents, hinting that maybe most incident causes are systematic in nature and focused on people, rather than equipment failure rate.

The Health and Safety Executive (HSE) 2003 publication "Out of Control: Why control systems go wrong and how to prevent failure" which reviewed 34 incidents involving control systems identified that the primary cause of incidents (approximately 60%!) were "built-in" to the safety related systems (The ones we rely on protecting us) before being taken into service (See Figure 1 below)

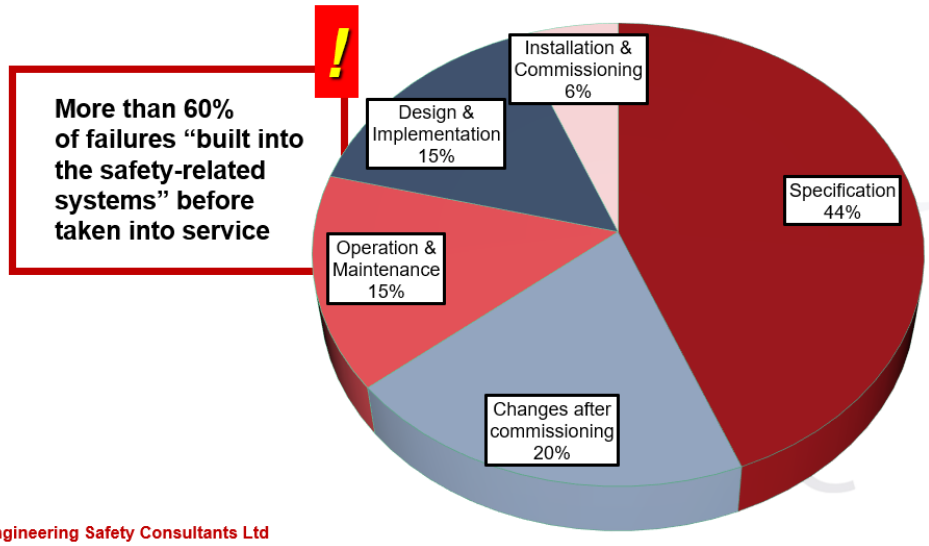

Figure 1 - Primary causes of incidents involving control systems (from "Out of control"HSE publication[1])

Based on this… Is it reasonable to then assume that the focus on numbers an unnecessary burden to an already complex topic? Should we just focus on doing the right things at the right time and hope it is enough?

"Hope is not a strategy."[2]

[1] From https://www.hse.gov.uk/pubns/books/hsg238.htm,
[2] From "Site Reliability Engineering: How Google Runs Production Systems", Beyer, Jones. Petoff and Murphy, 2016, 1st Ed

Systematic approach to risk reduction

IEC61508[3] standard for Safety Related Systems presents a safety system lifecycle which could be described as a 3-part process:

- Part 1 - Risk Assessment and systems specification
- Part 2 – Realisation (including design and implementation)
- Part 3 - Use and modification.

The application of this process for the process industry is captured in IEC61511[4] which also defines a safety lifecycle as shown below in Figure 2.

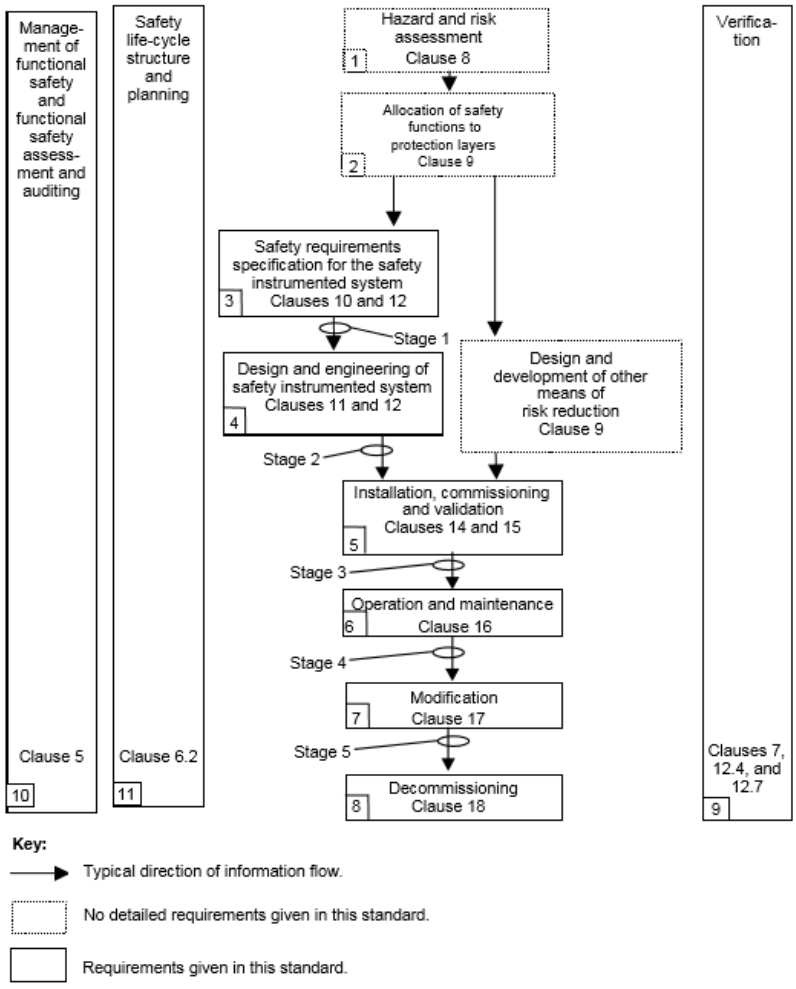

Figure 2 - Safety Lifecycle from IEC61511-2017[5]

The Risk assessment process (part 1) gives us a key body of information to allow us to maintain a "tandem" approach to both numerical/quantified system analysis and the systematic application of recognised good practices… that body of information comes in the form of a **target failure measure -** the Probability of Failure on Demand (PFD)/average dangerous failure rate per hour (PFH) target for the assessed Safety Instrumented Function (SIF).

This opens up a myriad of aspects within the standard, from depth of numerical analysis required (to confirm adequate risk reduction to meet the estimated **target failure measure**), to the expected development and implementation practices associated with the required level of risk reduction or PFD/PFH.

[3] IEC61508-2:2010 – Functional Safety for Electrical/Electronic/Programmable Electronic safety related systems
[4] IEC61511-1:2017 - Functional safety - Safety instrumented systems for the process industry sector
[5] From IEC61511-1:2017 - Functional safety - Safety instrumented systems for the process industry sector

It does so by establishing bands of PFD/PFH ranges which define the group of measures necessary for meeting the defined **target failure measure** … this is also known as the Safety Integrity Level (SIL) bands as shown in Table 1.

Table 1 - SIL and target failure measure table

Safety Integrity Level (SIL)	LOW DEMAND MODE	HIGH DEMAND OR CONTINUOUS MODE
	Target average probability of failure on demand (PFD)	Target frequency of dangerous failures to perform the safety instrumented function (per hour) – (PFH)
4	$\geq 10^{-5}$ to $< 10^{-4}$	≥10-9 to <10-8
3	$\geq 10^{-4}$ to $< 10^{-3}$	≥10-8 to <10-7
2	$\geq 10^{-3}$ to $< 10^{-2}$	≥10-7 to <10-6
1	$\geq 10^{-2}$ to $< 10^{-1}$	≥10-6 to <10-5

The lifecycle "splits" into numerical estimation for hardware capability (random hardware failures – PFD/PFH) and recognised good practices to address potential for error introduction, avoidance and control, which can be seen as a reinforcement of the idea that the numbers are only there as an exercise in mathematical futility… when in truth this isn't so at all.

For each SIL band there is a required package of measures which must be implemented to confirm that the non-quantifiable aspects of risk reduction have been addressed with similar (or equivalent) diligence to the quantified aspects.

In other words, it makes sure that the practices we use apply but cannot quantify, cannot affect the number we are using to quantify the necessary and achieved risk reduction. This approach introduces a new concept: Systematic Safety Integrity, also defined as Systematic Capability (SC). This is illustrated in Figure 3

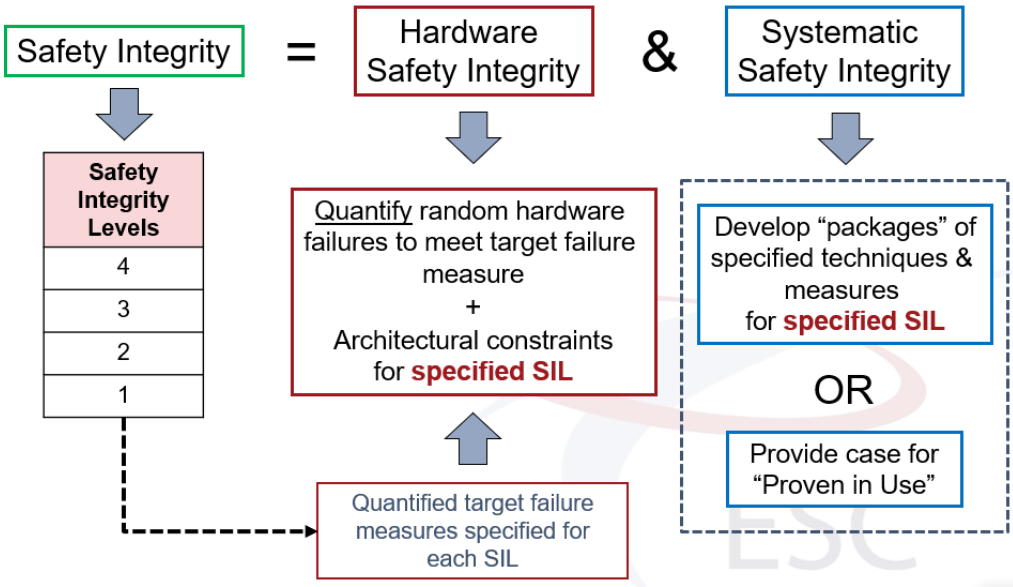

Figure 3 - SIL and its parts

Systematic Capability “measures” the adoption of practices which avoid, reduce and control error introduction of errors into each phase of the lifecycle to support the estimated failure rate for the system or element (also considers existing operational experience). [6]

SIL cannot be defined without considering both the hardware Safety Integrity (i.e. PFD/PFH) and Systematic Safety Integrity/Systematic Capability (SC)

So It makes sense to state that SIL assignment and achievement only makes sense when PFD/PFH and SC is understood, and PFD/PFH are only relevant if all aspects associated with allocating a SIL are observed, i.e. systematic and numerical analysis approaches according to the required risk reduction.

In IEC61508/IEC61511 context, target risk is more than a number, and should be considered as a detailed demonstration of the ability the meet the required risk reduction in all aspects which can support (or undermine) the risk reduction provided by a safety related system…

This is arguably an approach applicable to all risk management related aspects, which then poses the question…

” Can numbers tell the whole story when it comes to safety related systems, i.e. is there really safety in numbers alone?”

… Safety in numbers?

Yes, when the numbers are used to drive good engineering and people practice.

[6] Acceptable practices and (where possible) use of current operational experience for existing systems/elements via Proven in Use route (Prior Use in IEC61511) are defined within the standard with clear guidance however this is covered in a separate topic and discussion