Insights

What's the Difference Between Safety in Design & System Safety?

It happens to be a question I have found myself asking and trying to answer on a number of occasions over the past few years. I have seen a lot of project documentation use both terms in different sections, talking about some similar things, sometimes obliquely referencing each other, but often not.

In many cases, I have seen them being dealt with in different ways by different people, and often coming to different conclusions about the same thing.

Safety in Design

While "Safety in Design" is a broad term to mean the consideration of safety during the design process, it is typically used to refer to the requirements of the harmonised Australian WHS (Workplace Health and Safety) legislation being progressively adopted across states since 2011.

The model legislation requires designers of plant, substances or structures to consider the safety of people constructing, maintaining and using it through its life, and design it to be as safe as reasonably practicable for all such people.

The emphasis is on achieving safety through good design, rather than relying on procedures and protective equipment. The model WHS regulations requires the designer to provide a "safety report" describing the risks for persons who are to carry out the construction work, and what action has been taken to control those risks through design. Safety in Design is therefore a term used by engineers and architects that come from a construction and civil engineering background.

System Safety

On the other hand, System Safety has its roots in the aeronautics, space and defence industries in the 1960s, particularly in the US, with the Aerospace System Safety Society (now the International System Safety Society) established in 1963. Safety programs were put in place as part of the development of complex aerospace systems.

These programs not only included the identification of hazards and risks and how to control them, but involved detailed causal and consequence analysis using techniques such as fault tree analysis, and other detailed, quantitative analyses of design.

Such extensive analysis was considered necessary because of the costs of such programs and the potentially catastrophic consequences in the event of something going wrong. System safety is closely related to the discipline of systems engineering, which grew alongside it in these industries where the control of complexity and system emergent properties were the challenges of the day.

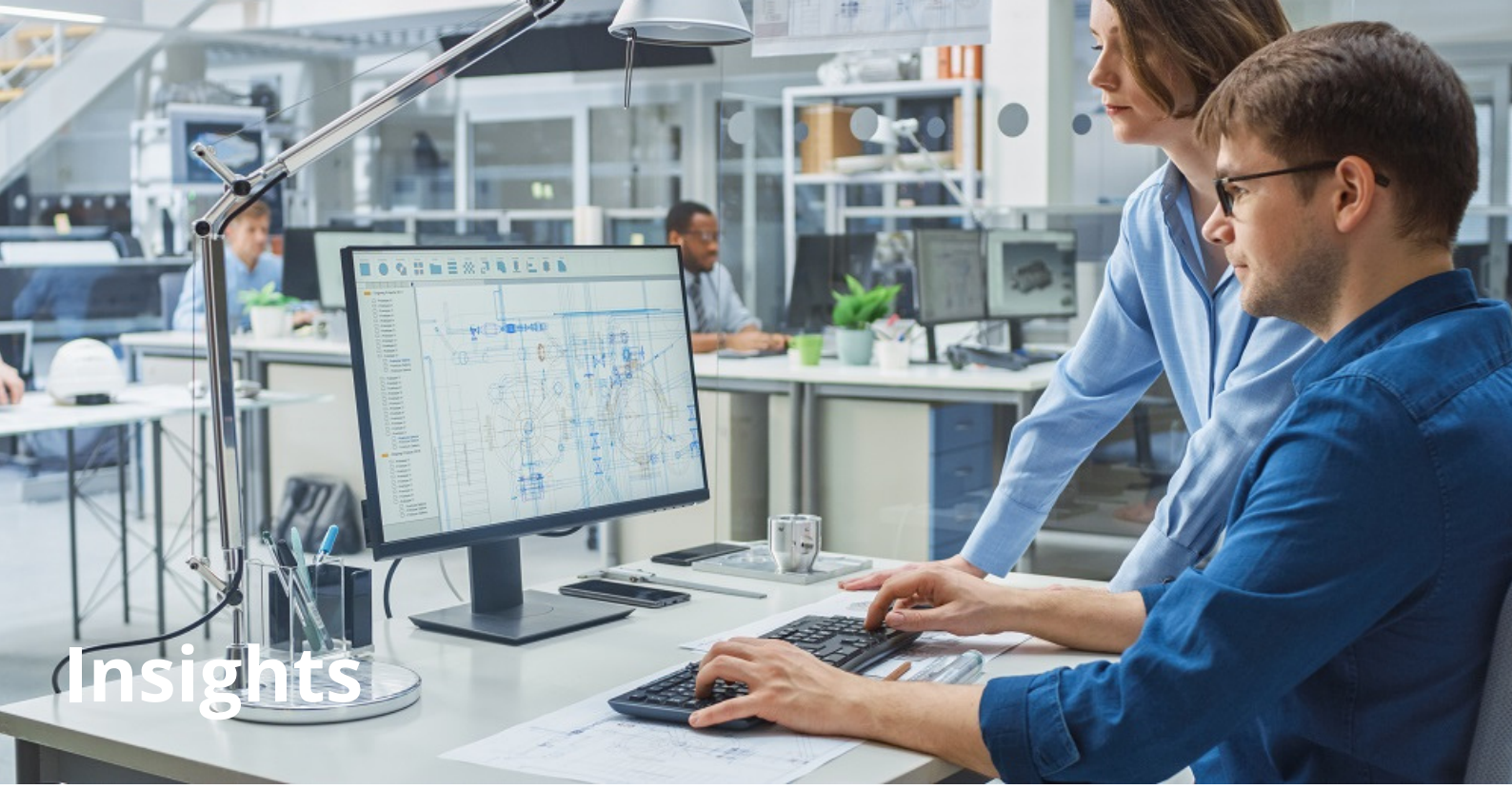
Over the decades, engineers from those industries found their way to rail organisations bringing with them the notion of a systematic, documented approach to safety.

Signalling product developers, who were starting to use software in computer-based interlockings and train protection systems, started to implement processes to control the risk from flaws in software and complex electronics. These processes involved rigorous analysis of potential failures to demonstrate their software was free of potentially dangerous errors.

What are the Differences?

The differences are not clear cut – it is more a matter of their focus and approach. Here is a table that shows how the approaches tend to differ.

	Safety in Design	System Safety
Product Lifecycle	The safety risks associated with construction, installation, maintenance, repair and modification	The risks associated with the built system or installed product
Domain of Application	Buildings and structures	Software-based/programmable systems
Complexity	Simple functions with tangible, visible structure	Distributed systems with complex functionality and interfaces, with significant involvement of people in its operation
Risk	Potential to cause serious injury or death to a worker	Potential to cause catastrophic accidents with multiple deaths
Verification and Validation	Confirmation that hazard controls have been implemented by review	Hazard controls captured as safety requirements and rigorously verified and validated through review, analysis, testing and traceability
Methodology	Simple workshop-based risk assessment and review methods such as CHAIR (Construction Hazard Assessment and Implication Review)	More complex and often quantitative techniques for analysing and modelling risk, such as Fault Tree Analysis, Event Tree Analysis, etc.
Practitioners	Occupational and Work Health and Safety specialists	Systems and safety assurance engineers



Insights

What is the Same?

The differences above reflect the trends in the application of each, but they both essentially address the same problem: the duty to reduce risk so far as is reasonably practicable. Because of that, they are both built on the basic process of identifying, assessing and reducing risk throughout the lifecycle.

Best practice in both is to consider the safety of all those who interact with the product, not just in its final form, but also during its construction, maintenance and demolition/decommissioning.

Most importantly, best practice in both is to apply this process as early as possible and to reduce risk through design. The earlier that is done, the most risk can be reduced with the least amount of fuss.

In both cases, it is not enough to achieve as safe a design as reasonably practicable, but the process by which that has been achieved must be demonstrated through documentary evidence.

Conclusion

- Safety in Design and System Safety are really one and the same thing, but have arisen from different origins and developed by different schools of practitioners.
- Do not duplicate effort by having both.
- Make sure that any risk assessment process clearly includes risks associated with construction, installation and maintenance.
- Make sure the level of rigour in analysis, verification, validation and documentation is commensurate with the risk involved.

Katherine Eastaughffe | Principal Consultant

Acmena

CONTACT US

+61 (0) 478 814 324
enquiries@acmena.com.au
www.acmena.com.au

Acmena Group Pty Ltd
PO BOX 220
Ashgrove West
Brisbane, QLD 4060
ABN: 37 158 514955
ACN: 158 514 955