TÜVRheinland®
Risktec

RISKworld / The Newsletter of Risktec Solutions / Spring 2020 p6-7

2020 Vision – Clear sight of safety in the design of complex high hazard systems

The modern world is reliant upon complex systems across many sectors – aviation, petrochemical, nuclear power, transport and beyond – each with the potential for catastrophic failure. Surely if given enough time, with enough rolls of the dice as it were, such failure is inevitable?

WHAT THE DOG SAW

In 2009, in his collection of essays entitled "What the Dog Saw and Other Adventures", Canadian writer Malcolm Gladwell wrote of the inevitability of failure of modern and technologically complex systems, in a cogent and well-informed piece that drew upon real-world examples such as the Space Shuttle Challenger and Three Mile Island nuclear reactor disasters.

Gladwell remarks that the investigations and lessons subsequently learnt from such disasters "are as much exercises in self-deception as they are opportunities for reassurance", and referred to a revisionist view that "high technology accidents may not have clear causes at all. They may be inherent in the complexity of the technological systems we have created".

Gladwell addressed in particular the Three Mile Island accident of 1979, which was caused by five concurrently occurring but otherwise discrete equipment failures and events. Notably, this reactor had been the subject of, for its time, an extensive Probabilistic Safety Assessment. This had captured all of the events that ultimately led to a meltdown of the core; but its treatment of dependent failures was less than ideal by today's standards, to the extent the accident sequence was dismissed on low frequency grounds.

The Challenger disaster of 1986 concerns the very different, yet similarly complex, arena of space exploration. Through reference to revisionist sociological research, Gladwell observed that no evidence could be found of the deliberate sacrifice of safety by either NASA or its lead contractors.

These represent just two examples of highly complex systems, engineered from the outset with a keen and necessary eye for safety, where failures nonetheless occurred with catastrophic consequences.

CONTINUOUS IMPROVEMENT

Today's principles of safe design have improved markedly in comparison to those of the time of the Three Mile Island reactor, and Gladwell's rather nihilistic perspective warrants a respectful, robust counter-argument. In the UK, for example, the Office for Nuclear Regulation today demands absolute separation of systems for reactor control and protection, in stark contrast to the approach of the seventies.

Multiple, independent, engineered lines of defence are required to fundamentally halt in their tracks the progression of the most serious sequences of events. Operational controls may support engineered safeguards, but only where necessary. Collectively, lines of

Three Mile Island Nuclear Power Plant

- Multiple, independent engineered lines of defence
- Independence of protection systems from control systems
- Redundancy, separation, segregation and diversity of systems and components
- Use of passive or automatic systems in preference to manual control
- Fault tolerance

Table 1 – Design Safety Principles

defence are designed to preclude the potential for common mode failure of like components, through the introduction of design and manufacturing diversity. In a similar fashion, designs must address the potential for common cause failures, such as might arise from fire, explosion or loss of services, through the provision of separation, segregation and independence of power sources.

KEEPING IT SIMPLE

The effect of applying these design safety principles (see Table 1) is to simplify the complexity of the design at a system level, so that for any given fault or hazard, its progression and the barriers in place to prevent serious consequences are one dimensional – as well as being straightforward to assess. In essence, the design safety principles break the myriad interactions and dependencies that would otherwise characterise a complex design.

To test the extent to which this has been achieved, designs are assessed both deterministically and probabilistically. The first approach uses a conservative set of black and white rules, which embed design safety principles, to assess the adequacy of defence in depth. The second entails the development of a detailed, probabilistic risk model able to examine the influence of any residual common mode or common cause failure (since in practice, these cannot be fully eliminated). The steady evolution since the seventies of ever more powerful computing capabilities has boosted the power of such Probabilistic Safety Assessment. Risk models need not be limited in scope and can cover the multitude of more frequent faults with less immediate consequences that, in the case of Three Mile Island, acted concurrently to create a far worse event.

CHALLENGING CULTURE

Returning to the Challenger disaster, it is noteworthy that the report on the fateful launch by American Nobel prize-winning physicist Richard Feynman, found an astonishing divergence between the risk assessments of NASA's engineers and those of its managers. While engineers reckoned on odds of disaster of roughly one in 100, their management considered it closer to one in 100,000.

In recognition of the ultimate total of two losses over the entire Space Shuttle programme of operations, it would appear the engineering perspective was exceptionally accurate; and arguably it was an endemic cultural failure that led to NASA management not deferring to the expertise of its engineers. Indeed, it is now widely recognised that organisational culture is a crucial factor in the success or otherwise of efforts to maintain safety in complex, high hazard systems. High performing organisations responsible for the design, construction and operation of such systems nowadays must demonstrate that a strong safety culture is embedded throughout all levels of the organisational structure. Arguably it was this key ingredient that was lacking in the NASA of the eighties. A visit to any nuclear power station will quickly reveal how deeply embedded safety-focused culture has become, with no exceptions or privileges offered, regardless of role.

CONCLUSION

As a society we have a choice: we could accept the status quo, and resign ourselves to occasional accidents in complex systems. Alternatively, we possess the capability and culture to apply tried and tested design safety principles – to keep things simple – and undertake meaningful safety analysis to improve designs further. The end result is genuine, evidence-based reassurance that catastrophic failures of complex systems are most certainly *not inevitable*.

Email:
enquiries@risktec.tuv.com