Complex Engineering Systems: How do we build high-reliability systems from a greater number of increasingly unreliable components? - Outline

By Stuart Jobbins, Sofintsys Ltd

Complex Engineering Systems: Increasingly Unreliable?

Will future components be less reliable – in absolute terms they won't be, but relatively, yes.

In future, our engineered systems will rely on components that have themselves been engineered to achieve critical properties in support of our overall system. We will become increasingly reliant on these engineered properties to achieve our goals. But our component engineering and the natural environment are increasingly in opposition when finessing component properties not just at design or manufacture, but throughout an operational life, and the evidence already exists that system reliability will become frustrated in our overall system engineering.

Systems Engineering the Future

Future complex engineered systems are unlikely to emanate from 'clean sheet' designs that share common architectural attributes, or even attribute priorities, because the component systems will be, or have been, designed at different times, with different original purposes. The new systems will be a composite of new component (systems), legacy component systems that are re-purposed, or evolutionary developments of those component systems. In fact the system componentry may never be stable and may be independently, and asynchronously, adapting to the change in search of a local optimisation. This will not allow us to have a consistent or coherent view on the system response to a perturbation (irrespective of cause e.g. natural event, unconsidered operational scenario or residual design error).

The scale (and cost) of such engineered systems will leave us little opportunity to 'test' its entire behaviour, even if our test experiment could be reliably isolated and described. The huge permutation space may make such an experiment's evidential value of limited worth. The fidelity required of any model to simulate such systems in order to be confident in the outcome of any such test would likely outweigh the cost of engineering the system itself. Our ability to describe failure scenarios and the resultant stimuli will be typically beyond the conception and often comprehension of the system designers.

Although some failures will be manifest from (the ultimately human) failings during the engineering of the system, others will be as a result of increased system sensitivity as we attempt to derive systems at mega-scale, from components at nano-scale. Digital control systems will be pervasive, but are prone to the issues. Digital control provides innate flexibility to command arbitrary relationships between component systems, and in so doing, be able to extract more of the available envelope of the system performance.

The design margin (the difference between the control systems operation and the physical system's limits), whilst neither of its boundaries are a discrete edge, vary with material qualities, manufacture and assembly tolerances and processes, deteriorate with age, use or stress levels. Add in the somewhat less reliable properties of human interaction as part of the system and the boundaries can be very 'fuzzy' in definition. Typically for an 'improvement' to be extracted from existing systems, more of the system envelope needs to be explored, and by implication the design margin reduced.

Not all systems however are amenable to early indication of 'onset of failure' and are prone to abrupt changes caused by natural phenomena at the near molecular level (e.g. digital electronics). As we push systems to smaller scale, onset of failure becomes increasingly difficult to detect and manage in most engineering disciplines. If the reliability of a mechanical system relies heavily on the atomic-level properties of the material, and natural processes of its operational environment have an ability to alter those properties, how do we ensure that the required properties are retained, reliably detected when they are lost, and accommodated when there is a change, before the system utility is lost (let alone a catastrophic failure)?

Conclusions

If it's not possible to detect and accommodate such failures in component properties with early detection, we must be able to predict the reliability of an engineered solution with sufficient certainty to achieve the desired goal.

Like the more simplistic reliability calculations of old, it may be possible to analyse system and environment properties sufficiently to ensure the entire system operates below a 'break-even' point where the rate of failure for a given system complexity can be assured to deliver its utility, or at least conservatively match the useful task (operational) life.

Related articles

Al Geists, How To Kill A Supercomputer: Dirty Power, Cosmic Rays, and Bad Solder - IEEE Spectrum, Feb. 2016

Jianxi Gao, Baruch Barzel & Albert-László Barabási, Universal resilience patterns in complex networks – Nature Feb. 2016