Advances in Reliability, Safety and Security

ESREL 2024
Collection of Extended Abstracts

Perspectives And Challenges For Reliability And Health Management At System Of Systems Level

Pierre Dersin[a], Vitali Volovoi[b]

[a]*Lulea University of Technology, Lulea, Sweden*
[b]*MITEK ANALYTICS LLC, Palo Alto, CA, USA*

Keywords: complexity, reliability, resiilence, prognostics and health management (PHM), system of systems (SoS),critical point

---

The famous "more is different" declared by P.W. Anderson more than half a century ago (Anderson, 1972) feels particularly germane to modern Reliability Engineering. The explosive growth of sensing, collecting, and data processing capabilities relevant to successful delivery of needed functionality ticks all the boxes for "more". Yet when it comes to fundamental methods of reliability, too often the "same" appears to be the answer, including persistent reliance on simplifying assumptions that were necessary in the past, such as stochastic independence of failures, deterministic configurations, unicity of time scale, and often steady-state conditions.

What about machine learning, Large Language Models (LLM), and other recent innovations? While extremely useful, they mainly further contribute to the above-mentioned "more," providing yet more useful inputs into reliability models. LLM analysis of free-form maintenance records can improve failure mode classification for field failures. A new deep learning algorithm can refine Prognostics & Health Management (PHM) policy (Zio, 2022) for an asset, improving the odds of correctly predicting the remaining useful life for that asset.

However, complex systems, and Systems of Systems (SoS), pose a challenge to Reliability Engineering and Prognostics & Health Management (PHM) since convenient assumptions that can be made at component level break down when complexity increases. Goals of PHM are often framed in terms of a specific asset. In contrast, the SoS perspective requires understanding fleet-wide implications of specific PHM policies, and includes not only operational, but logistics considerations as well. Hence there is a need for aggregated representations. Such representations should retain significant characteristics of the object of study while eliminating details. The motivation for this approach is clearly the combinatorial explosion ("the curse of dimensionality") which arises with problem size, and the corresponding computational overload that ensues, even with modern IT capabilities.

We have more useful information, so we expect better decision-making tools. Traditional reliability, whether at the component or system level, deals with relatively standard, nominal sets of scenarios, where operating conditions are well defined. Safety (by necessity a system-level metric) dramatically expands the realm of explored scenarios (in other words, increases variability of inputs). C. Perrow provided (Perrow, 1984) two key axes for assessing system safety: coupling and complexity. Systems that are both tightly coupled and highly complex are inherently unsafe. To put it simply, high complexity makes systems failures inevitable, while tight coupling facilitates fast failure propagation, precluding timely "off-ramp" remedial actions.

There are extreme cases where off-ramp actions are not possible (e.g., the Space Shuttle, or Titan Submersible), but as a rule such actions at least in theory have the highest priority, overriding the reliability requirement to provide the intended functionality. As a result, safety mechanisms for more extreme stresses are usually a one-shot (e.g., airbags, or earthquake-resistant housing), drastically simplifying the corresponding safety analysis and effectively decoupling it from the reliability analysis.

Moving up the aggregation hierarchy, i.e., dealing with Systems of Systems (SoS) (Dersin et al.,2020), brings about the need for more explicit trade-off between safety and delivering functionality. To this end, two related but distinct concepts have received significant attention recently: robustness and resilience, in a wide range of domains, including public policy (Capano, 2017). Both principles aim at managing high variability of inputs, e.g., external stresses. While the definitions vary depending on the domain, informally robustness focuses on embedded (designed) ability to perform under a broad range of inputs. Classic engineering design relied on very large tolerances to compensate for uncertainty and sometimes low-quality (but scalable) manufacturing. In contrast, resilience implies "bouncing back" upon experiencing the stress, recovering the initial functionality. The difference can be illustrated in the context of control theory, where robust control can be contrasted to adaptive control (concept akin to resilience). The topic of resilience for socio-technical systems gained popularity in the last fifteen years, and is closely tied to the SoS, e.g., "openness", lack of boundaries (Bergström, 2015) and complexity (Simon,1962).

The latter brings us back to the "different": emergent behavior, coupling between different time scales, operation near instability limits, occurrence of extreme events and dynamic failure propagation. Examples can be found in a variety of civilian and military situations, including electric power grids, complex transportation networks, health care systems, climate-change dynamics, and aircraft fleet management.

As a result, there is a need for aggregate representations of complex systems and SoS, and the guidelines for these representations in the study of SoS reliability or resilience. Specifically, two concepts from physics appear to be of high relevance: mean field theory and critical points.

Mean-field theory (Kadanoff, 2009) provides a compact way to assume a component-centric view of the system and consider interactions with the rest of the system in an aggregated form. This principle was applied to reliability modeling in the context of opportunistic maintenance (Volovoi et al., 2012) but can be extended to modeling temporal characteristics of the shock-recovery for quantitative resilience.

The second concept is that of the phase transitions and associated critical points (Kadanoff, 2009), and in particular of the distinction between the first (sudden) and second (gradual) order transitions. For instance, in electric power networks, the first order transition leading to cascading failure is of great concern (Dobson, 2007). In this context, it is also important to note that the distinction between the first and second order transition can be caused by the lack of relevant information: if gradual degradation is not properly sensed and analysed, physically gradual phase transition can ***appear*** as sudden. Timing of reaction (similarly to adaptive control) is of the essence.

This leads us back to the importance of PHM technologies, as their system-level and SoS applications can be of critical importance in terms of warning about the system and SoS degradation. More generally, broader acceptance of PHM technologies hinges upon the ability to comprehensively assess systems and SoS trade-offs associated with the introduction of these technologies. Benefits of avoiding operational failures must be balanced against investment (in condition monitoring equipment and PHM algorithms), asset use and possibly more -frequent part replacements, for instance. In SoS Health Management, asset health is typically measured by a health indicator, facilitating failure detection, diagnostics and prognostics.

The complementary (and to date insufficiently addressed) question is how to relate asset health indices to a system health index or system health indices to a SoS health index.

References

Anderson, P.W. 1972, More Is Different, Science 177, 4047.

Bergström, J. et al. 2015. On the Rationale of Resilience in the Domain of Safety. A Literature Review. Reliability Engineering & System Safety 141, 131-141.

Capano, G., Woo, J.J. 2017. Resilience and Robustness in Policy Design: A Critical Appraisal, Policy Sciences 50, 399-426.

Dersin, P., Valenzuela, R. 2020. Designing for Availability in Systems, and Systems of Systems, Tutorial, RAMS 2020.

Dobson, I. et al. 2007. Complex systems analysis of series of blackouts: Cascading failure, critical points, and self-organization. Chaos, An Interdisciplinary Journal of Nonlinear Science 17(2).

Kadanoff, L.P. 2009. More is the Same; Phase Transitions and Mean Field Theories, J Stat Phys 137, 777-797.

Perrow, C. 1984. Normal Accidents, Basic Books, New York.

Simon, H.A. 1962. The Architecture of Complexity, Proceedings of the American Philosophical Society 106 (6), 467-482.

Volovoi, V., Valenzuela, R. 2012. On compact modeling of coupling effects in maintenance processes of complex systems, International Journal of Engineering Science 59, 193-210.

Zio, E. 2022. Prognostics and Health Management (PHM): where are we and where do we (need to) go in Theory and Practice, Reliability Engineering & System Safety 218, Part A.