Should Nuclear Safety Care About Resilience Engineering?

J. Paries[1]

[1]*Dedale S.A.S, Paris, France*

Corresponding Author: J. Paries, jparies@dedale.net

The current nuclear industry safety paradigm is based on the deterministic and/or probabilistic anticipation of all potential situations, and the predetermination of all the (safe) responses. Even the defense in depth concept, which is the core of the nuclear safety strategy and is intended to handle situations in which part of the control is lost, heavily relies on detailed anticipations. In other words, nuclear safety is mainly expected from the real world's conformity to a designed-to-be-safe world, i.e., a well controlled world, where organizations, processes, hardware, teams, and individuals comply with their rationally predetermined behaviors. In this "command and control" perspective, risk is seen as mainly generated by deviations and variations from rules, procedures, norms, and expectations. However, real operations are complex, even in normal situations, which means that they include some unpredictable events and adaptation behaviors. The traditional "command and control" perspective fail to properly acknowledge the limits to predictability inherent to a complex adaptive system. It actually strives to reduce complexity through tighter compliance to specifications and to improve predictions capabilities through a tighter monitoring of "weak signals" and "precursors". But in a complex world, precursors are usually obvious after the event, while not identifiable before. And the efforts made to reduce complexity may also simultaneously tighten couplings between system's components — hence increase complexity — and reduce the diversity and flexibility needed to respond to it.

The notion of Safety Culture has developed in the nuclear industry in the aftermath of the Chernobyl disaster as a form of recognition of the limitations of a mere compliance-based approach to safety management. It has rightfully accounted for more complex determinants of collective safety behavior such as values, commitment, risk cognizance, situation awareness, leadership, trust and honesty. However, it still sounds like an added layer to the traditional "command and control" perspective, rather than like a well integrated evolution. It still carries elements of denial towards complexity. It recognises in principle that mechanical compliance cannot do the job — and it calls for knowledge, competence and good judgment, but it does not really tell how to reconcile compliance and intelligence during the course of action (rather than after the event, with the benefit of insight). One of the hard lessons from Fukushima is that there is a need to reconcile predetermination and adaptation in the nuclear safety philosophy, and the notion of resilience may be of some help to achieve this. It first implies to fully recognise complexity and unpredictability: as Scott Sagan sagely expressed, "Things that have never happened before happen all the time". It also implies one must better understand (research) and recognise how the current nuclear organizations and their staff actually handle the unexpected, and get (daily) success rather than (rare) failures. It calls for a targeted effort to reinforce these abilities, including a specific approach to the design of the system (technology, processes, procedures, resources), as well as to the design of the organization (structures, roles, responsibilities, cooperation modes). Typical related issues include the empowerment of front line operators, the management of margins

of manoeuver, the development of sense-making and imagination skills, the provision and management of functional flexibility and diversity, the maintenance of stocks, dampers, slack, buffers in all processes.

References

[1] "The Limits of Safety: Organizations, Accidents, and Nuclear Weapons", Scott D. Sagan, Princeton University Press, 1993.