## Prognostication Complications

"Risk" conceptualized as the probability of a pre-diagnosed state, in a reasonably complex technological system, involves complications that are difficult to ignore. Topping the list are the following three:

1. Time must exist,
2. Event probabilities must be proposed, and
3. Proposed probabilities must be validated.

The list is not comprehensive, but nearly so. For example, Solberg and Njå identify five elements that include uncertainty and consequences but leave validation out:

> "..., we find five common elements concerning the concept of risk. Those are: time (the future), events, consequences, uncertainty and something of human value related to the consequences."

Uncertainty is essentially probability, but consequences and human value are candidates for addition to the list. However, it seems risk could be evaluated, as such, and human value as Solberg and Njå point out could subsequently be assigned, according to individual preference and circumstances at the time of the particular event.

Time is inextricably connected because risk determination requires assessment of the past, the present, and the future states of affairs albeit, under incomplete knowledge. Another view is that the existence of future states must be based on what is known at the present. Because the past no longer exists in the present, it is impossible to "go back" and study the state of affairs, that is, the past state of affairs is typically inferred in the present. For example, a realistic process may ask for a motor to be actuated by a relay when the pressure, in a monitored system decreases below a set point. Ideally, the pressure transducer and the relay would have unbiased random errors in pressure measurement and relay actuation. It is unlikely the pressure measurement error and the relay actuation error would be correlated. Therefore, in this example, quantifying the probability, for actuation at the proper pressure would be straightforward. Now suppose these devices are in a realistic protection setting that includes redundant channels and regular maintenance on a staggered basis. The redundant configuration may be designed to avoid "false" actuations by, for example, including an auctioneering scheme, say two out of four pressure measurements at the relay set point, to actuate the relay. Maintenance typically checks the output over the range of operation to ensure, or alternatively, adjust outputs within required tolerances. Under this circumstance, the random errors would become time-dependent. It is furthermore unlikely that over time the pressure transducer and the relay settings would remain unbiased. In robust designs such as the one with redundancy described, actuation signal failures would be rare. Therefore, the maintained system with time-dependent future probability of failure would be difficult not only to quantify, but to validate, in any proposed quantification scheme.

What can be done to overcome the complications of time, knowledge, and validation? It seems ideas such as Uncertainty Quantification (UQ) may not be sufficient since they also fail to overcome uncertainty (state of knowledge) contained in the physical models used in UQ simulations. A typical example is outlined by Mandelli et al. where a reactor safety simulation is integrated into a sophisticated Probabilistic Risk Assessment (PRA) logic structure that would give probability of failure absent support (for the quantified probabilities). It could be said that engineers understand risk management as a control problem with feedback. That is, they from observations of the current state of affairs, they make adjustments to overcome the uncertainty inherent in past decisions. By performing root cause analysis on unexpected states, they can better inform future performance. Another example is the tightly coupled feedback process used to guide a controllable missile to accurately hit a target. In this example, the target is made to produce a signal to which the missile continuously adjusts its path. Engineers inherently recognize that the more real time control that can be exercised, the better they can manage risk going forward. Condition-based maintenance and operating equipment instrumentation telemetry reflect the nature of practical engineering risk management. Such tools continuously update the engineer on the current state of affairs so she can react appropriately to unexpected observations.

## References

Mandelli, D., A. Alfonsi, C. Wang, Z. Ma, C. Parisi, T. Aldemir, C. Smith, and R. Youngblood (2021). Mutual integration of classical and dynamic pra. *Nuclear Technology 207*(3), 363–375.

Solberg, Ø. and O. Njå (2012, October). Reflections on the ontological status of risk. *JOURNAL OF RISK RESEARCH 15*(9), 1201–1215.