The Art of Operational Safety Monitoring and Recovery at System Run Time

Henning Butz

In the field of safety management of complex systems it is reasonable to distinguish between “functional safety cases” and those, which we may label “operational safety cases”.

“Functional safety” is about cases where some (sub-)function of a system goes wrong due to a local component failure, a signal error or a software bug. Functional safety issues are both, easy to predict and to cover at design time, and easy to detect and to compensate at run time of the system. Generally this is achieved by automated means. Well established Methods like FMEA, MBSE, failure injection techniques as well as various bench and route proving test strategies are applied to obtain a quite complete failure coverage. The same applies for functional failure monitoring and recovering techniques being used to maintain the desired safety margin of the system during run time.

In contrast to this “operational safety” cases are much more difficult to identify at design time and even harder to detect as such at run time, while being nearly impossible to compensate by automated means. Operational safety cases concern system failures, where all systems functions perform as specified, but the system exhibits erratic behavior, either due to unforeseen constraint conflicts between some sub-functions within the system or by an inadvertent mismatch of some system states with the environmental operating conditions, under which the system actually performs.

Obviously the operational safety issue is a problem of the correctness, completeness and consistency of the design requirements – in other terms: a matter of the validation quality. If the validation coverage could be complete, operational safety issue won’t happen! This however, is an illusion. The present paper therefore addresses the aspects of operational safety cases at system run time:

- How to identify operational safety cases (i.e. validation flaws that slipped the design validation quality gates)
- How to recover from operational safety situations in order to regain the required safety margin
- The means of semi-automated and automated management of human induced operational safety cases, w.r.t. human – machine – interference and – awareness.