Knowledge – the true shortcut

Name   Kristina Forsberg

Abstract text   When designing dependable systems it is essential to understand the intended function and the level of safety connected to the function. If this is known, we can apply classic redundancy and fault tolerance concepts to achieve sufficiently safe designs. This talk will address what is necessary in order to design safety critical embedded systems (fail-stop and fail-operational) using experiences from the avionics industry. Further, the talk will touch upon challenges with increasing and more advanced functionality - mostly enabled through software. In such software intensive systems, the understanding of intended function and a deterministic behavior in presence of faults and errors is becoming more difficult.

This trend, with ever increasing integrated functions, in embedded systems combined with insufficient assessment methods to cope with the complexity of verifying correct behavior is truly a future challenge in dependable systems design. We know what we know, and to some extent, we know what we don't know - but we can't handle problems that we don't know that we don't know.