Safe modular online updates and upgrades for mixed-criticality systems

Gregor Nitsche, Patrick Uven, Ingo Stierand, Kim Grüttner (German Aerospace Institute, DLR)

Safety-critical systems face an increase in critical software functions that require high-performance hardware platforms. This situation fosters - also in the automotive domain - an ongoing trend away from many small towards few but powerful processing elements. It inevitably comes with a concentration of the deployed functionality, which imposes challenges to the system design. A major issue in designing safety-critical system is to ensure segregation and isolation of the individual system functions of mixed-criticalities (w.r.t. different Design Assurance Levels (DAL) or Safety Integrity Levels (SIL)), which becomes more costly and harder to achieve the more functionality is executed at the same platform. At the same time, Over-The-Air Software Updates (OTASU) become necessary for modern embedded systems as updates and feature enhancements, safety and security fixes, or adaptations to other components become inevitable during their lifetime. Ensuring compliance with safety regulations thus requires an ever-increasing effort up to the point where it is economically not feasible anymore. The talk gives an overview of a domain-independent software paradigm for the development and integration of software applications on mixed-critical cyber-physical systems along the product lifecycle, which enables modular certification and supports secure OTASU. This paradigm is implemented and demonstrated through a new proof-of-concept software architecture and development process that enables remote deployment of updated as well as new applications on heterogeneous computing platforms. In addition, we provide a strategy for future certification of the approach with respect to safety (e.g., IEC-61508, ISO 26262) and security (IEC-62443, ISO 21434) through specific concepts that build on composability, modularity, and observability as key properties to enable dynamic validation of safety and security properties after deployment in the operational environment.

Contact: Kim Grüttner (kim.gruettner@dlr.de)