Abstract

This thesis focuses on the conceptual design and prototypical implementation of a Checkpoint Management System (CMS) based on the L4 Fiasco.OC microkernel and the Genode OS Framework version 21.08. The context of this management system is the Cooperative Integration Architecture for Future Smart Mobility Solutions (KIA4SM), which envisions a larger homogeneity of Electronic Control Units (ECUs) inside smart vehicles through virtualisation. Such a homogeneity entails further reduced necessity of failure safety through redundancy, as created through higher numbers of ECUs in vehicle systems, since any ECU can perform any operation. Expanding on this concept, the Real-Time Checkpoint Restore (RTCR) was developed to snapshot the state of target processes and restore them in case of failure. This however doesn't cover complete ECU breakdown, for which the CMS was actually envisioned. The manager of this system is designed as a centralised component, receiving checkpoints from RTCRs via distributed shared memory, storing them securely in a network addressed storage, and migrating and restoring them in case of failure or for load-balancing reasons, with a second redundant manager as a fallback. The implemented prototype operates without redundancy and a proper DSM, but is able to receive checkpoints and store them to a NAS component. If one of two RTCR dummies, simulating a real RTCR, calls for migration, the manager can retrieve the desired checkpoint and send it to another RTCR dummy, which is selected by comparing a metric consisting of RAM- and capability usage. All in all, as these main functionalities behave satisfactorily, the CMS is viewed as a successful proof of concept.