Emergency Shutdown System Demonstrator using AutoFOCUS3

Abstract—For safety critical applications, separation is needed in hardware and software. The model based development tool AutoFocus 3 supports design, simulation and verification of safety critical applications. It uses a hierarchical component based model and provides a complete tool chain from application design to running code. Our separation platform provides spatial and temporal separation in a shared memory architecture. Temporal separation is archived through a special DDR2 arbiter, while spatial separation is enforced through a MPU that guards the shared memory. The Emergency Shutdown System Demonstrator – jointly implemented by Danfoss Drives and fortiss GmbH – implements a software controlled emergency shutdown system. It uses a dual core architecture. All inputs are forwarded to both cores. When the emergency switch is hit, both cores independently shut down the system. The application logic is designed and verified using AF3. The application components are deployed to the cores. Finally the automated code generation of the AF3 tool chain is used to bring the application to the hardware.

Index Terms—AutoFOCUS3, Danfoss, Emergency Shutdown Demonstrator