Faculty of Electrical Engineering & Computer Science
Master Degree Course Electronics Engineering, MSc EE

HSB
Hochschule Bremen
City University of Applied Sciences

Master 2021

Mr. Muhammad Mubashir Latif

Implementation of an AMP System for Functional Safe Products with Hardware-Level Security.

ABSTRACT - Masterthesis

Multicore processor systems are widely used in today's modern Embedded Products, and they can be categorized into Symmetric Multi-Processing systems (SMP) and Asymmetric Multi-Processing systems (AMP). In SMP systems all cores are of the same architecture and can be operated with a single operating system, whereas AMP systems could be based on either multiple Operating Systems or different processor architectures. In general, AMP system designs are modular, optimized, flexible, and easy to get certified.

This thesis is focused on implementing an AMP system using homogenous and heterogeneous processor cores, with different operating systems. Although AMP systems design provide much comfort, this sort of configuration creates different levels of complexities in the design. This thesis work is focused on addressing problems in AMP system design, which are contributed from shared resources like L2 Cache, interrupt controller, memory management, and inter-processor communication. The solution provided by this thesis work has been implemented in different Projects at PLC2 Design GmbH to solve some of the above-mentioned challenges of AMP Systems.

Development and testing have been done using the UltraZed-EG starter kit which consists of UltraZed-EG system-On-Module (SOM), features ZynqMPSoC (Zynq multiprocessor System on Chip) and UltraZed-EG IO carrier card. ZynqMPSoC comprises an APU, features Arm Cortex-A53 quad-core processor and an RPU, and it also features an Arm Cortex-R5 dual core real time processor. As this thesis work focuses on AMP system design for Functional Safety products, ZynqMPSoC has been split into multiple isolated sub-systems, namely APU, RPU and PMU, while each sub-system has its dedicated master, memory, and peripherals.

The main objective of splitting MPSoC into these sub-systems is to ensure that each sub-system runs without any interference from other sub-systems. This isolation configuration serves as back bone for Functional Safe and Secure applications / products. Xilinx protection units and ARM TrustZone technology, both have been used to enforce this isolation configuration. Since this isolation configuration is directly re-

lated to safety and reliability of applications, isolation configuration for each sub-system has been tested by attempting to violate it, to make sure that master of each sub-system can only access their dedicated memory and peripherals. Furthermore, an Inter-processor communication between these isolated sub-systems has been achieved through OpenAMP infrastructure, which is based on shared memory, a standard method for communication within a system and has been provided by the MCA. Additionally, a further layer of hardware level security has been implemented by splitting APU into secure and Non-secure world by using ARM TrustZone technology.