Contribution ID: **28** Type: **Poster**

Adaption of Low Cost Safety COTS MCU For Low Level Radiation Applications in Accelerator Facilities

Wednesday, 28 September 2016 17:36 (1 minute)

Our work targets soft errors in embedded systems operating in particle accelerator physics experiments. We propose to use the safety mechanisms included in the low cost Cortex-R4F to mitigate Single Event Effects, as well as additional procedures to recover data from external memories. These procedures include making an interleaved backup of the program data by using the DMA controller. In case the CRC mechanism detects a mismatch either in the interleaved backup data or in the program/heap/stack, the faulty data can be rewritten from the copy or the original data.

Summary

Our work is motivated by the growing concerns of soft errors in embedded systems operating in particle accelerator physics experiments. Until now, the problem is handled by using Application Specific Integrated Circuits (ASIC) with high radiation tolerance. Such ASICs are pricey and only available upon special fabrication ordering. Therefore, we propose to use and exploit the safety features of low cost, automotive, Commercial Off The Shelf (COTS) Micro Controller Units (MCU) with fault-tolerant Cortex-R4F processor, such as the TMS570 from Texas Instruments. This Cortex-R4F runs in lockstep mode to achieve dual processor redundancy, has ECC mechanisms for internal, tightly coupled memories as well as for flash program memories. It furthermore operates CPU-independent Cyclic Redundancy Check (CRC) and Direct Memory Access (DMA) controllers. The CRC is commonly used to detect mismatches of written data in several kinds of memories, among them the ones connected to the External Memory Interface (EMIF). Such mismatches can be caused for example by Single Event Effects (SEE). We furthermore propose additional procedures to recover data from memories managed by the EMIF which can be program memory, stack or heap data. These procedures include making an interleaved backup of the program data, to be stored in the external memory, by using the DMA controller. In case the CRC mechanism detects a mismatch either in the interleaved backup data or in the program/heap/stack, the faulty data can be rewritten from the copy or the original data, depending on where the error occurred. In ordinary MCUs, errors can propagate across operations, which leads to a situation where it is impossible to recover any damaged data. Thus, the inclusion of checkpoints is proposed, offering the following advantage: Any fault detected by the MCU safety features such as lockstep, ECC of internal memory, clock signal integrity and PLL status can be monitored in specific registers. For control applications in accelerator facilities, such as CERN, EPICS libraries were adapted to the redundant COTS Cortex-R4F MCU by using the Real Time Executive Multiprocessing System (RTEMS) Board Support Package (BSP). Therefore, if an MCU error occurs without involving the EPICS libraries and Ethernet driver, the user can be informed immediately by porting the failure from the MCU fault register to an EPICS process variable which can be subsequently monitored in any computer connected to the EPICS Channel Access CA. For the future work, we intend to establish radiation limits where such a device can be operated by exposing the MCU to a wide variety of beam types. We will also look for mechanisms in which erroneous data can be recovered by other MCUs connected to the EPICS CA, or implement a different protocol in the same layer as CA to recover damaged data.

Primary author: LUCIO, Antonio (Goethe-Universität Frankfurt am Main)

Co-author: KEBSCHULL, Udo Wolfgang (Johann-Wolfgang-Goethe Univ. (DE))

Presenter: LUCIO, Antonio (Goethe-Universität Frankfurt am Main)

Session Classification: POSTER

Track Classification: Radiation