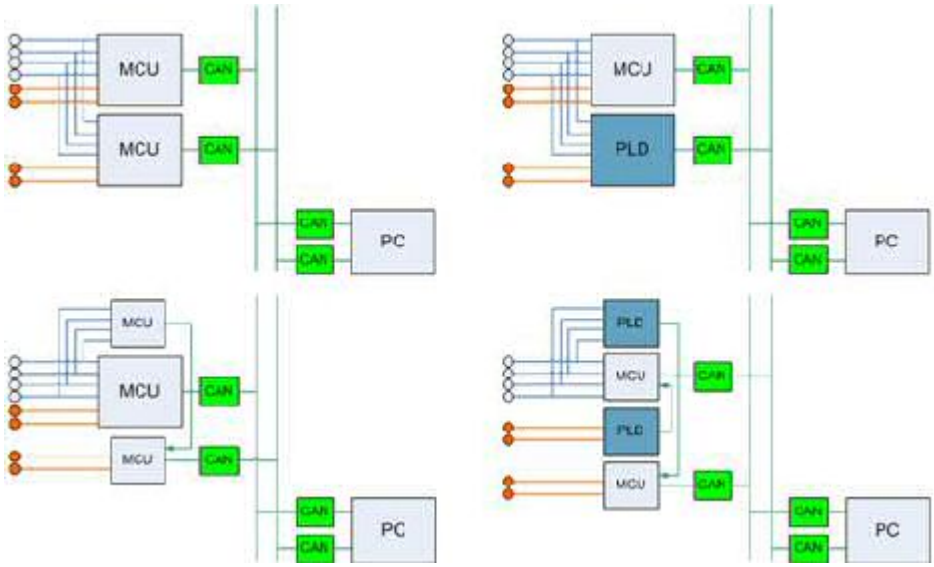
Safety-Critical Embedded Systems

Traditional methods for achieving safety properties mostly originate from hardware-dominated systems. Software-intensive embedded systems require new approaches, as they are for example suggested by the emerging standard IEC 61508. We are interested in developing constructive and analytical methods for ensuring safety that have a sound formal basis but are also efficiently applicable in different domains, like automotive or railway systems.

One of our interests in this field is the influence of hardware decisions on safety and reliability of the according software. We see a chance to improve safety and reliability of a system by finding the optimal hardware-software combination. On the one hand this could be an appropriate microcontroller (MCU) with the according software or a programmable logic circuit (PLD) such as a FPGA or a CPLD designed in a suitable hardware description language. In this context, we have conducted several experiments in order to get the necessary basic data to work with. Examples for different hardware structures for analyzing the influence on the according software are given below.



On the other hand, the optimal hardware-software combination could be a partition of the systems functionality on a suitable microcontroller/microprocessor with the corresponding software and an appropriate programmable logic circuit. One of the major problems when dealing with software safety is complexity. However, the safety critical functions are in some cases of a simpler nature. Thus, the idea is to implement the safety critical part in a very simple way on the programmable logic circuit and leave the complex higher level functionality to the microcontroller. The advantage of this approach is that the basic safety critical functions on the programmable logic circuit do not depend on the CPU but can be implemented in redundant hardware modules and are easier to verify (e.g. timing analysis of programmable circuits is usually easier than that of software running on a CPU). It has to be analyzed which functionalities are suitable for this partition and how it should be realized in the design flow. In order to provide our results for other designers of safety critical systems, we plan to allocate them in a pattern catalogue with the according building codes.

Another topic is the model based specification and analysis of safety requirements. Here we see a close connection to the research field of model checking.

Contact

- Dr.-Ing. Falk Salewski