1. Publishable summary

Complexity Management for Mixed-Criticality Systems

CoMMiCS

Cyber-physical systems are computer systems that tightly interact with physical processes, typically for command and control purposes. Some cyber-physical systems have to be dependable, which means that the overall failure of the system may lead to loss of human life or significant assets. These dependable cyber-physical systems are categorized as dependable systems. The avionics system in an airplane is such a dependable system. Here dependable cyber-physical systems have replaced hydro-mechanical systems to control the airplane. While this shift towards dependable cyber-physical systems happened in the aviation industry already decades ago the automotive industry is about to implement similar technologies. Electric cars are likely to speed up this adoption process.

Dependable systems are, hence, omnipresent in our daily lives and are becoming increasingly large and complex. As a consequence of this trend it is apparent that the correct development of such complex systems requires a sound architectural basis. In the absence of architectures we will either build systems of insufficient quality or will simply not be able to build systems beyond a certain level of complexity at all. The time-triggered architecture (TTA) as developed at the Institut für Technische Informatik at the Vienna University of Technology is an extraordinary example of an architecture for dependable embedded systems. The TTA tremendously simplifies the development of dependable cyber-physical systems. It has been successfully applied in industries that demand a high level of determinism such as the avionics industry in which predictability of system operation is a key property. TTP and TTEthernet are implementations of the TTA. TTP is applied, for example, in the new Boeing 787 Dreamliner, whereas TTEthernet has been selected for the NASA Orion Space Program.

While the aerospace and space industries (as well as automotive and similar industries) are traditional areas for dependable systems, we also observe emerging areas with increasing dependability requirements. Examples include surgery robots in the medical area, datacenters in the financial and other critical industries, as well as the smart grid that aims at decentralized energy production and efficient energy use. TTEthernet is currently evaluated for several of these areas.

Given the observations as sketched above we can reasonably conclude that over time more and more dependable systems will become mixed-criticality systems: as the complexity and size of traditional dependable systems grows, cost restrictions as well as size, weight and power (SWaP) requirements will force the industry to utilize their computation/communication resources more efficiently. By sharing physical resources between applications of different criticality levels the efficiency of a system can greatly be improved. To some degree we see the concept of mixed-criticality systems already being implemented in the aeronautic industry (“integrated modular avionics”). On the other hand,

the emerging systems will not instantaneously become dependable-only systems, but gradually become more and more dependable. Systems that host applications with different criticality requirements will be the normal case and not the exception.

Architectures such as the TTA can be applied to mixed-criticality systems to some extent, but as these systems have additional requirements to the ones the TTA has been originally designed to, novel architectural approaches are necessary. The CoMMiCS Marie Curie Fellowship researches such novel approaches by using formal methods for the verification, configuration, and algorithm design for mixed-criticality systems. The CoMMiCS project is hosted by TTTech Computertechnik AG in Vienna, Austria and by SRI International, Menlo Park, California.

The CoMMiCS project addresses the problem of complexity management for mixed-criticality systems in three workpackages (called research objectives), RO_A, RO_B, and RO_C.

The main result of RO_A is the executable formal specification of the TTEthernet synchronization protocol in two parts. A first part focuses on the integration aspects of startup, restart, and some low-level diagnosis functionality. Due the state-space explosion problem we have chosen to represent time as a discrete entity in this first part of the executable specification. However, the second part of the executable specification addresses some particular lower-level synchronization functions and represents time as a continuous entity.
The main result of RO_B is a new approach of using the SMT-solver for configuring mixed-criticality systems. In particular, we have included the YICES SMT-solver in tools for scheduling of time-triggered traffic, traffic performance analysis of event-triggered traffic, and design of time-triggered schedules with a provision for event-triggered traffic integration.
The main research results of RO_C comprise formal models of TTEthernet in PVS and SAL that have been used to generate new algorithms, in particular a diagnosis algorithm and a clock rate-correction algorithm. Furthermore, these models have shown for the first time that clock-synchronization protocols for fault-tolerant systems can be verified fully automatically by means of model checking. A paper reporting the PVS research results has been awarded the “best of session” and “best of track” awards at the 30th IEEE/AIAA Digital Avionics Systems Conference.

During the return period of the CoMMiCS Marie Curie International Outgoing Fellowship the research results have been disseminated within TTTech Computertechnik AG and use cases for the application of the research results have been developed.

Contact:

Dr. Wilfried Steiner
Marie Curie Fellow
TTTech Computertechnik AG
Schoenbrunner Str. 7
1040 Vienna
Austria
wilfried.steiner@tttech.com

Dr. Stefan Poledna
Scientist in Charge
TTTech Computertechnik AG
Schoenbrunner Str. 7
1040 Vienna
Austria
stefan.poledna@tttech.co