Sabine Appelhagen
www.FitForCamera.de

Report: (Workshop 20.05.2015 Milano)

New Challenge for the Aerospace-, Rail- and Automotive Industry in Europe: The need for Solutions for Safety Critical Applications on Multicore Processors

Milano, May 20th 2015 Three Projects presented at the Block review for the Mixed Criticality Computing Cluster - all working towards the same goal: developing new tools and techniques that allow safety-critical and non-safety-critical functions to be placed on the same multicore devices.

At the moment there are major changes going on in the computer industry: The traditional approach was to carefully separate safety-critical and non-safety-critical functions in any application. Now there is the need to move towards multicore processors. This is saving space, weight and energy. "But it also raises issues of separation and how can we guarantee that non-safety critical functions do not affect other functions? "As Haydn Thompson (from THHINK) puts it. "There is a need to be smarter and safer in an increasingly complex world."

Let´s take the example of the board computer of a car: Automotive currently uses many processors throughout the car to provide different functionality. This is segregated into different functionalities with separate databus connections, e.g. for infotainment and safety-critical vehicle control. By having lots of boxes it is expensive, complicated and heavy. By integrating functionality into less units the system can be simplified with fewer boxes and provide more functionality for users. (A bit like our smart phones, that allow you to call, surf the web, take photos, play music/games etc. all on one small device)

In the past processing speed and functionality doubled according to Moore's Law as higher and higher clock speeds were used. This is no longer possible due to the density of the transistors on devices and the problem of trying to get heat out from the processor. The industry has moved towards multiple cores to address this: effectively more processing power is provided by using more than one computing core. These multicores are operated at lower speeds to manage the thermal problem. But to save complexity they share key resources, e.g. memory and on-chip connections for communications. This sharing makes it impossible to prove that critical timing needs can be met and

thus applications using multicores cannot be certified for safety-critical applications in aerospace, rail, etc. (i.e. that critical software produces results within critical deadlines).

The projects presented at the Milano block review are working on different aspects of mixed criticality systems:

PROXIMA – A radical new technique for timing analysis which can be employed for both conventional processors, programmable logic and multicore processors.
PROXIMA is working on reliability, analyzability and performance with a concentration on development of a new technique for proving that time deadlines will be met. As highlighted traditional approaches cannot be used so the project is working on a new technique that uses probabilistic analysis. The project is working with the certification authorities to pave the way for early adoption of this technique in industry.

CONTREX – A holistic approach to considering performance parameters, timing, power and temperature with specific relevance to battery powered equipment.
CONTREX – is working on techniques to allow different functionalities to be integrated onto multicore platforms. Here the focus is on design and analysis of power consumption, temperature and timing constraints early in the design before hardware is available. Power consumption and thermal management is particularly important for applications that are battery powered, e.g. mobile devices.

DREAMS – Development of an architectural style that can be used for safe, reliable and secure networked multicore systems.
DREAMS – is defining an architectural style for networked multicore chips considering safety, security, real-time support and adaptivity. Here an aim is to quickly adapt functionality to different applications or product lines much as they do in the smart phone industry where different variants can be supplied with different functions. This product line approach based on a model driven methodology is targeted at promoting widespread adoption of the technology.

The projects are closely driven by industry. Some of the applications are very near term, e.g. the CONTREX application for telematics is developing a black box to record minor car crashes and damage by vandalism when the car is parked – here the concept has been demonstrated with real hardware and software and the interest in this has been shown by Vodafone buying the SME that started the project with the intent of rolling out products in the near term. Other applications are developing tools that will be available to industry to help them develop mixed-criticality systems within 2 to 3 years. Other outputs such as the new approach to certification needs time to become accepted but may be adopted in the 5 to 10 year timescale.

Europe has many of the leading industrial companies in the aerospace, automotive and rail sectors and citizens benefit from the mobility provided by various forms of transport. Support for development of the underlying techniques and European support for research and development are essential to maintain our lead in this sector. But: The safety-critical market aerospace, rail,

automotive etc. only accounts for a very small percentage of device market (much less than 1%!). The processor manufacturers have no interest in producing “small” numbers of single core devices so these are gradually being phased out. This is the reason why they have to move on to the multicore processors.

Also by using multicore processors there are lots of advantages to be gained from reduced space, weight and power consumption and also from offering increased functionality to users.
This means that we will have safer systems, with much more functionality, that will be lighter more compact and consume less power (reducing CO2).
Mobility is central to Europe’s citizens, we use cars, trains, aircraft for business and pleasure in our everyday lives. We want to know that these are safe. In the future adoption of multicore processors with mixed criticality functions will allow provide greater functionality giving us better and safer systems (e.g. assisted driving functionality), more options for entertainment – Internet surfing, and greater connectivity and access to information.

All Information in this article is taken from the Interview (attached) with Haydn Thompson from THHINK)