Report: Block review for the Mixed Criticality Systems project cluster

Workshop 20.05.2015 Milano - Dreams Proxima Contrex

Answers by Haydn Thompson (Thhink)

Common Message: "Smarter and Safer in an Increasingly Complex World"

Journalistic Questions:

General Aspects:

- What does the term “Mixed Criticality System” mean?

  Mixed criticality refers to the mixture of safety-critical and non safety-critical functions on the same hardware. An example would be providing Internet connectivity in a car to allow people to surf the web but also use the same functionality to provide automated driving features which would be safety critical.

- What are the problems, they are dealing on?

  The main issue is that the traditional approach is to carefully separate safety-critical and non safety-critical functions. The move towards multicore processors means that both can be put on the same computer modules saving space, weight and energy but this raises issues of separation and how do we guarantee that non-safety critical functions e.g. playing a video does not affect other functions which are important for driving.

- Why do those problems occur now? What is the time-horizon for this?

  The problems are occurring now because the processor manufacturers can no longer scale their devices to provide more computing power. 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 which are operated at lower speeds managing the thermal problem). A problem is that this is driven by the consumer sector, mobile devices, tablets, laptops, mobile phones etc. and 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. The very big problem for safety-critical applications is that for certification it is necessary to guarantee timing (i.e. that critical software produces results within critical deadlines). In order to adopt multicore devices the processor manufacturers use multiple cores 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. So we need a solution!

- What happens, if there is nothing done about it?

  If nothing is done, then all processors in the future will be multicores and it will not be possible to certify, e.g. prove the safety of future systems. Note that Europe is a leader in area, e.g. aerospace, automotive, etc.

- What is the worst case scenario?

  The worst case scenario is that we cannot prove the safety of future systems.

- How do the Solutions to these future problems look like?

  We do not know the answer at the moment. The key thing is to crack the analysis problems so that we can guarantee safety, we also need to develop the tool support around this so that engineers can use the new approaches. Finally, we need to convince the certification authorities that these new techniques can be used to prove that systems are safe.

- What is the best case scenario?

  The best case scenario is that new tools and techniques are created that allow people to partition software such that safety-critical and non safety-critical functions can be placed on the same multicore devices. This would allow the safety-critical industry to move to multicore processors (which it really does not have a choice about). 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.

- Can you give a simple example for this?

  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)

Questions regarding the three Projects:

- What are differences between those 3 Projects - all of them are working on Mixed Criticality Systems?
  The projects are working on different aspects of mixed criticality systems.

PROXIMA – is working on reliability, analysability 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 – 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 thrmral management is particularly important for applicitions that are battery powered, e.g. mobile devices.

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 funcitonality 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.

- In which areas do they overlap?
  Actually there is only a very slight overlap between CONTREX and PROXIMA in the sense that they are both looking at timing analysis, the critical difference is that PROXIMA is developing a radical new approach to timing analysis which if successful will be a major change in the industry, whereas CONTREX is adopting a more traditional technique to timing analysis but is also looking at power consumption and temperature at the same time and the interactions between the three which are also key considerations.

- What were the most important results the representatives of the projects reported at the review? One sentence for each Project?

  PROXIMA – A radical new technique for timing analysis which can be employed for both conventional processors, programmable logic and multicore processors.
  CONTREX – A holistic approach to considering performance parameters, timing, power and temperature with specific relevance to battery powered equipment.
  DREAMS – Development of an architectural style that can be used for safe, reliable and secure networked multicore systems.

- What are the next steps going to be? One sentence for each project?

  PROXIMA – Proving and demonstration of the technique and promotion to the certification authorities
  CONTREX – Further development of the toolset and demonstration in aerospace, automotive and telecoms applications

  DREAMS – Further development and demonstration in an avionics system, wind turbine and safety-critical medical monitoring.

- When can we expect the first results - when will the first solutions be ready to be implemented? Can you give an example?

  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.

Conclusion:

- What is the expected impact of these changes on industry?
  The expected impact is that we will be able to adopt multi-core processors in future safety-critical applications, automotive, aerospace, rail, medical monitoring, etc.

- What is the expected impact of these changes on society?

  This means that we will have safer systems, with much more functionality, that will be lighter more compact and consume less power (reducing CO2).

- Is there a need for political action in these fields?

  The safety-critical industry is driven by standards bodies and independent regulatory bodies so there is no need for direct intervention. There is a need for education and awareness building and this is where there is a role for political action. There is also a need to bring together and develop an ecosystem to support this area.

- What advice do you have for politicians?

  Europe has many of the leading industrial companies in the aerospace, automotive and rail sectors and European 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.

- Why should the public care for these topics?

  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.