Emerging Challenges in Embedded Software

Jan Tobias Miühlberg[1] and Silvia Nuñez[2]

[1] iMinds-DistriNet, KU Leuven, Celestijnenlaan 200A, B-3001 Belgium
[2] SQS, Avda. Zugazarte 8, 1 - 6, 48930 Getxo, Vizcaya - Spain

Embedded software is becoming an essential part of everyone's life, without us necessarily being aware of it. Embedded software is designed to control increasingly complex machines or devices that are not typically thought of as computers, and that we entrust with essential activities or even our lives, every single day. As examples, think of computer programs that operate cars, railway systems, aircrafts, telecommunication and multimedia devices, power plants, hospital equipment and even medical implants such as insulin pumps or pacemakers: an ever-growing subset of our society's critical infrastructure is controlled by computer programs for which failure is simply not an option.

In the very near future we will be sitting inside autonomous cars that drive in smart cities on smart roads, and live in smart houses that make optimal use of renewable energy resources that are provided by a smart electricity grid. Even more embedded software will take over tedious activities and support us in making the most of our time – in professional contexts as well as in our private lives. This renders embedded systems a fast-growing and very innovative market in which software takes a prominent role.

Embedded systems development is traditionally characterised by a strong focus on system safety, in particular in the avionics, automotive, medical and nuclear industries. Here, stringent standards prescribe a software life-cycle that involves carefully coding, inspection, documentation, testing, verification and analysis of the system. Decades of experience have lead to a wealth of knowledge in effectively managing quality and in implementing reliable software.

One of the most recent challenges to embedded systems engineering is security. While in the last decade, embedded software would typically run on isolated micro-controllers that can be physically secured against manipulations, modern embedded systems operate in networked environments and are often remotely accessible and controllable. Typical examples for this are smart vehicles that communicate traffic conditions with each other and with roadside devices to guarantee safe and efficient operation. Or the smart electricity grid where smart home-appliances can be remotely controlled and would manage their power consumption based on immediate change of tariffs and the overall network situation. Attacks against industrial control systems (Stuxnet) and cars (Miller & Valasek) gained a lot of popular attention. However, the overall security of our current and future embedded ICT landscape remains mysterious to all but the most skilled analysts.

In the past years, the EU has taken a step forward to place the protection of critical infrastructure in the focus of international research and development activities. Yet, a permanent exchange of experience between professionals from

all across the world is necessary to tackle emerging problems in embedded ICT. In Europe, a number of large conferences such as EuroStar and EuroSys aim to foster this exchange. Taking a focus on quality assurance and testing of embedded systems, QA&Test (SQS, Bilbao) is a fairly specialised key player in this domain, bringing together professional from industry and academia.

Processes for producing functionally correct, reliable and secure embedded control systems are incredibly complex. Good conferences organiser embrace this complexity. They know that one needs to employ a range of tools to achieve this goal, and devise presentation tracks and invited talks to address management approaches, standardisation, technical ideas and case studies independently. Still, this may not excite the entire audience and certainly presentations are not the only reason to attend professional conferences. More engaging than lectures is the in-depth exploration of emerging tools and techniques in tutorials or interactive workshops. Of course, there are many ways to learn and sharpen our skills these days – webinars, blogs or podcasts – you name it. Those are all not quite like being at a conference. In particular they lack the networking opportunities, the chance to meet and engage in active discussions with experts and like-minded participants, the opportunity to learn about tools and techniques that may be novel and unusual or simply outside of our daily scope of operation. There are many unknown problems ahead of us. In embedded systems those come with new technology, challenging application domains, changing environmental conditions and emerging attack scenarios. Being engineers and scientists, we should be comfortably excited with this unknown, and find solutions together.