12th International ERCIM/EWICS/ARTEMIS Workshop on Dependable Smart Embedded Cyber-Physical Systems and Systems-of-Systems (DECSoS 2017)

12th International ERCIM/EWICS/ARTEMIS Workshop on Dependable Smart Embedded Cyber-Physical Systems and Systems-of-Systems (DECSoS 2017)

European Research and Innovation Initiatives in the Area of Cyber-Physical Systems and Systems-of-Systems

Erwin Schoitsch[1] and Amund Skavhaug[2]

[1] Digital Safety & Security Department, AIT Austrian Institute of Technology, Vienna, Austria
Erwin.Schoitsch@ait.ac.at
[2] Department of Production and Quality Engineering, NTNU, Norwegian University of S&T, Trondheim, Norway
Amund.Skavhaug@ntnu.no

1 Introduction

The DECSoS workshop at SAFECOMP follows already its own tradition since 2006. In the past, it focussed on the conventional type of "dependable embedded systems", covering all dependability aspects as defined by Avizienis, Lapries, Kopetz, Voges and others in IFIP WG 10.4. To put more emphasis on the relationship to physics, mechatronics and the notion of interaction with an unpredictable environment, the terminology changed to "cyber-physical systems" (CPS) and "Systems-of-Systems" (SoS). The new megatrend (and hype?) IoT ("Internet of Things") as super-infrastructure for CPS as things added a new dimension with enormous challenges. Collaboration and co-operation of these systems with each other and humans, and the interplay of safety, security and reliability are leading to new challenges in verification, validation and certification/qualification. Examples are e.g. the smart power grid (power plants and power distribution and control), smart transport systems (rail, traffic management with V2V and V2I facilities, air traffic control systems), advanced manufacturing systems ("Industry 4.0"), mobile co-operating autonomous robotic systems, smart health care, smart buildings up to smart cities and the like.

Society as a whole strongly depends on CPS and SoS - thus it is important to consider dependability (safety, reliability, availability, security, maintainability, etc.), resilience, robustness and sustainability in a holistic manner. CPS and SoS are a targeted research area in Horizon 2020 and public-private partnerships such as the ECSEL JU (Joint Undertaking) (Electronic Components and Systems for European Leadership), which integrated the former ARTEMIS (Advanced Research and

Technology for Embedded Intelligence and Systems), ENIAC and EPoSS efforts. Industry and research ("private") are represented by the industrial associations ARTEMIS-IA, AENEAS (for ENIAC, semiconductor industry) and EPoSS ("Smart Systems Integration"), the public part are the EC and the national public authorities of the member states. Funding comes from the EC and the national public authorities ("tri-partite funding": EC, member states, project partners).

2 ARTEMIS/ECSEL: The European Cyber-physical Systems Initiative

This year the workshop is co-hosted by the ARTEMIS and Horizon 2020 projects

- CRYSTAL ("Critical Systems Engineering Factories", http://www.crystal-artemis.eu),
- ARROWHEAD1 ("Ahead of the Future", http://www.arrowhead.eu/),
- EMC2 ("Embedded Multi-Core systems for Mixed Criticality applications in dynamic and changeable real-time environments", http://www.artemis-emc2.eu/) and
- CP-SETIS ("Towards Cyber-Physical Systems Engineering Tools Interoperability Standards", http://cp-setis.eu/), a Horizon 2020 project, funded only by the EC, but executed by ARTEMIS-IA members.

These projects finished this year, and results are partially reported in presentations at the DECSoS-workshop.

Last year started the co-hosting ECSEL projects AMASS (Safety & Security Multi-Concern Assurance), ENABLE-S3 (Automated Vehicles), IoSENSE (IoT and Industry 4.0) and SemI40 (Semiconductor - Industry 4.0). This year are starting AQUAS (Quality, Safety, Security and Performance Multi-Concern). The projects AutoDrive (Autonomous Vehicles – Road, Rail, Aircraft) and Productive 4.0 (Smart Manufacturing, Industry 4.0), the largest ECSEL project in this field with up to now (110 partners), are so-called "Light-House projects". The first one for Mobility, the second one for Production, i.e. they should attract co-operations across project boundaries and be the core for the next generation of projects joining the "lighthouse" party. Detailed references are on the project- and EU-CORDIS web site, see also Acknowledgements at the end of the article. The DECSoS chair who is partner in most of these projects, will also provide some overview and explain some context in the workshop introduction of the workshop.

ARTEMIS was one of the European, industry-driven research initiatives and is now part of the ECSEL PPP. The last ARTEMIS projects finished this year, but work in the research fields addressed continues within the ECSEL JU. The four co-hosting ARTEMIS projects that finished their work this year are described briefly, the "new-comers" have just started last and this year, but are already referenced in some presentations.

CRYSTAL, a large ARTEMIS Innovation Pilot Project (AIPP), aimed at fostering Europe's leading edge position in embedded systems engineering by facilitating high quality and cost effectiveness of safety-critical embedded systems and architecture

platforms. Its overall goal was to enable sustainable paths to speed up the maturation, integration, and cross-sector reusability of technological and methodological bricks in the areas of transportation (aerospace, automotive, and rail) and healthcare providing a critical mass of European technology providers. CRYSTAL integrated the contributions of previous ARTEMIS projects (CESAR, MBAT, iFEST, SafeCer etc.) and further developed the ARTEMIS RTP (Reference Technology Platform) and Interoperability Specification.

CP-SETIS ("Towards Cyber-Physical Systems Engineering Tools Interoperability Standards" (IOS)) was a H2020 support-action-like Innovation Action (IA). CP-SETIS created a sustainable eco-system for the IOS by finding a host and service structure (ARTEMIS-IA as hosting and funding organization, a small start-up to maintain the Database and IOS Coordination Forum (ICF) of stakeholders interested in the IOS specifications, standards and guidelines, which can be active during the next years. This is insofar a considerable achievement as very often with end of a project the activities are ceased, the follow-up not guaranteed. The ARTEMIS and ECSEL JU and their organizations differ insofar from other funding schemes as the sequence of projects builds on the preceding ones and work is continued over long-term schedules.

ARROWHEAD, a large AIPP addressing the areas production and energy system automation, intelligent-built environment and urban infrastructure, is aiming at enabling collaborative automation by networked embedded devices, from enterprise/worldwide level in the cloud down to device level at the machine in the plant. The goal is to achieve efficiency and flexibility on a global scale for five application verticals: production (manufacturing, process, energy production and distribution), smart buildings and infrastructures, electro-mobility and virtual market of energy.

EMC² is up to now the largest ARTEMIS AIPP bundling the power of innovation of 100 partners from embedded industry and research from 19 European countries and Israel with an effort of about 800 person years and a total budget of about 100 million Euro. The objective of the EMC² project is to develop an innovative and sustainable service-oriented architecture approach for mixed criticality applications in dynamic and changeable real-time environments based on multi-core architectures.

It provides the paradigm shift to a new and sustainable system architecture which is suitable to handle open dynamic systems:

- Dynamic Adaptability in Open Systems, scalability and utmost flexibility,
- Utilization of expensive system features only as Service-on-Demand in order to reduce the overall system cost,
- Handling of mixed criticality applications under real-time conditions,
- Full scale deployment and management of integrated tool chains, through the entire lifecycle.

The AIPPs ARROWHEAD and EMC² are addressing "Systems-of-Systems" aspects in the context of critical systems, whereas CRYSTAL and CP-SETIS are devoting their major efforts towards creating a sustainable eco-system of a CRTP (Collaborative Reference Technology Platform) and the harmonization of efforts towards an IOS (set of standards, specifications and guidelines for tool interoperability).

3 This Year's Workshop

The workshop DECSoS'17 provides some insight into an interesting set of topics to enable fruitful discussions during the meeting and afterwards. The mixture of topics is hopefully well balanced, with a certain focus on mixed-criticality and multi-core systems and concerns, cybersecurity & safety co-analysis and on collaborative and autonomous systems. Presentations are mainly based on ARTEMIS/ECSEL, EU FP7 and Horizon 2020, and nationally funded projects mentioned above and on industrial developments of partners' companies and universities.

The session starts with an introduction and overview to the ERCIM/EWICS/ARTEMIS DECSoS Workshop setting the European Research and Innovation scene. The first session on **Critical Software Analysis and Development** comprises two presentations:

(1) "Analysis of Potential Code Vulnerabilities involving Overlapping Instructions" (Research of the University of Erlangen-Nuremberg, Germany, work funded by the German Federal Ministry for Economic Affairs and Energy, in the project SMARTEST),
(2) "Increasing dependability in Safety Critical CPSs using Reflective Statecharts", work developed and funded by the Basque government and continued now in the ECSEL-JU project Productive4.0, which was mentioned before as a "Lighthouse project" of ECSEL JU).

The second session covers **Mixed Criticality and Multi-Core Systems** by three papers:

(1) "A Survey of Hardware Technologies for Mixed-critical Integration Explored in the Project EMC²", an invited paper, providing an overview over and reflecting on hardware aspects and challenges, and on bridging solutions explored in the ARTEMIS EMC² project, therefore many co-authors are mentioned, from the different areas and industrial use cases.
(2) "Safe Implementation of Mixed-Criticality Applications in Multicore Platforms: A Model-Based Design Approach". This paper reflects also on significant results of the EMC² project, addressing the critical challenges of multi-core and hybrid architectures with respect to system's safety and safe implementation.
(3) "GSN Support of Mixed-Criticality Systems Certification". Using the Goal-Structuring Notation GSN, safety arguments are stored in an argument database to support automatic composition of safety cases for variants of products. This is an outcome of the FP7 DREAMS project, OPENCOSS and AMASS are also mentioned in this context.

The session after lunch is dedicated to **Reliability, Safety & Cybersecurity (Co-) Engineering**, a general topic nowadays for all areas of CPS and IoT in an connected (smart) world:

(1) The session starts with a presentation on reliable communication, which is a major factor in daily life and particularly for large infrastructures, autonomous driving etc. where services have to be provided and interruption may be critical:

"Concepts for Reliable Communication in a Software-defined Network Architecture" on how sharing of the internet is possible in an innovative, reliable and secure manner. The project was funded by the Austrian Federal Ministry of Transport, Innovation and Technology, projects OFSE (Open Flow Secure Grid) and OPOSSUM (SDN Open Flow-based communication system for multi-energy domains).

(2) "Combining Safety & Security Analysis for Industrial Collaborative Automation Systems" – IoT is a key enabler for collaborative automation. Safety and security assessments are gaining increasing importance, particularly when legacy equipment and devices are part of automation systems, which is regularly the case. An industrial application in Austria is demonstrated, which was developed in context of the ARTEMIS project ARROWHEAD.

(3) "Software Updates in Safety and Security Co-engineering" presents a review of safety & security standards with respect to software updates, which are on the one hand critical from the safety point of view ("safety expert: never change a certified system"), but on the other hand often necessary as countermeasure to mitigate security threats. A roadmap of relevant standards is provided as well as result of the review.

(4) "Detailed analysis of security evaluation of automotive systems based on JASO TP15002". Recent cases of hacker attacks on automotive systems revealed that "a system that is not secure cannot be save" (David Strickland, chief Administrator for the National Highway Traffic Safety Administration (NHTSA). Fortunate, they did not really endanger persons, but were done for demonstration purposes only. The paper describes security analysis according to automotive cybersecurity guidelines of the Japanese standardization organization (similar to SAE in the US and now developed in ISO/SAE JWG1 as ISO 21434 standard "Road vehicles – Cybersecurity engineering".

The last session of the day is about **Collaborative and Autonomous Systems**, a topic of increasing interest in industry, automotive, railways, drones and aircraft, and robotics:

(1) "Systematic Composition of Services from Distributed Systems for Highly Dynamic Collaboration Processes" is about collaboration processes of systems in open and dynamically changing environments, which is a challenge to shared services. Platooning of vehicles is an example – what to do if environmental conditions change in a manner influencing e.g. control (braking on wet road surface etc.), which needs adaptation to degraded conditions. "Dynamic safety contracts" are presented as a potential solution, being executed at runtime and adapting to environmental conditions, which extends the existing concept of run-time certification (which results afterwards in a stable configuration, but does not adapt system behavior continuously), which was already presented at recent workshops.

(2) "Safety Assurance for Autonomous and Collaborative Medical Cyber-Physical Systems" – this paper refers to medical CPSoS which collaborate in a flexible

manner at run-time, thus providing a higher level of functionality. Since predictability can no longer be assumed, so new models and approaches are required to meet the new challenges, e.g. safety contracts, dynamic risk assessment etc. Some thoughts and a coherent taxonomy will be discussed.

(3) "Safety-Aware Control of Swarms of Drones" – this paper proposes a novel approach to ensuring safety while planning and controlling an operation of a swarm of drones, using evolutionary algorithms for safety-aware mission planning at run-time; autonomy of each drone is not assumed, it is a more centralized approach.

As chairpersons of the workshop, we want to thank all authors and contributors who submitted their work, Friedemann Bitsch, the SAFECOMP Publication Chair, and the members of the International Program Committee who enabled a fair evaluation through reviews and considerable improvements in many cases. We want to express our thanks to the SAFECOMP organizers, who provided us the opportunity to organize the workshop at SAFECOMP 2017 in Trento. Particularly we want to thank the EC and national public funding authorities who made the work in the research projects possible. We do not want to forget the continued support of our companies and organizations, of ERCIM, the European Research Consortium for Informatics and Mathematics with its Working Group on Dependable Embedded Software-intensive Systems, and EWICS, the creator and main sponsor of SAFECOMP, with its working groups, who always helped us to learn from their networks.

We hope that all participants will benefit from the workshop, enjoy the conference and accompanying programs and will join us again in the future!

Acknowledgements. Part of the work presented in the workshop received funding from the EC (ARTEMIS/ECSEL Joint Undertaking) and the partners National Funding Authorities through the projects ARROWHEAD (332987), EMC2 (621429), CRYSTAL (332830) and SafeCer (295373). Other EC funded projects are in FP7 DREAMS (610640) and OPENCOSS (289011), and in Horizon 2020 CP-SETIS (645149). Some projects received national funding only (see individual acknowledgements in papers). The ECSEL JU and nationally ("tri-partite") funded projects recently started and contributing to the work areas described here are AMASS (grant agreement 692474), ENABLE-S3 (692455), IoSENSE (692480), SemI40 (692466), ENABLE-S3 (692455), AQUAS (737475), Productive4.0 (737459) and AutoDrive (737469).

International Program Committee