Number 102 July 2015

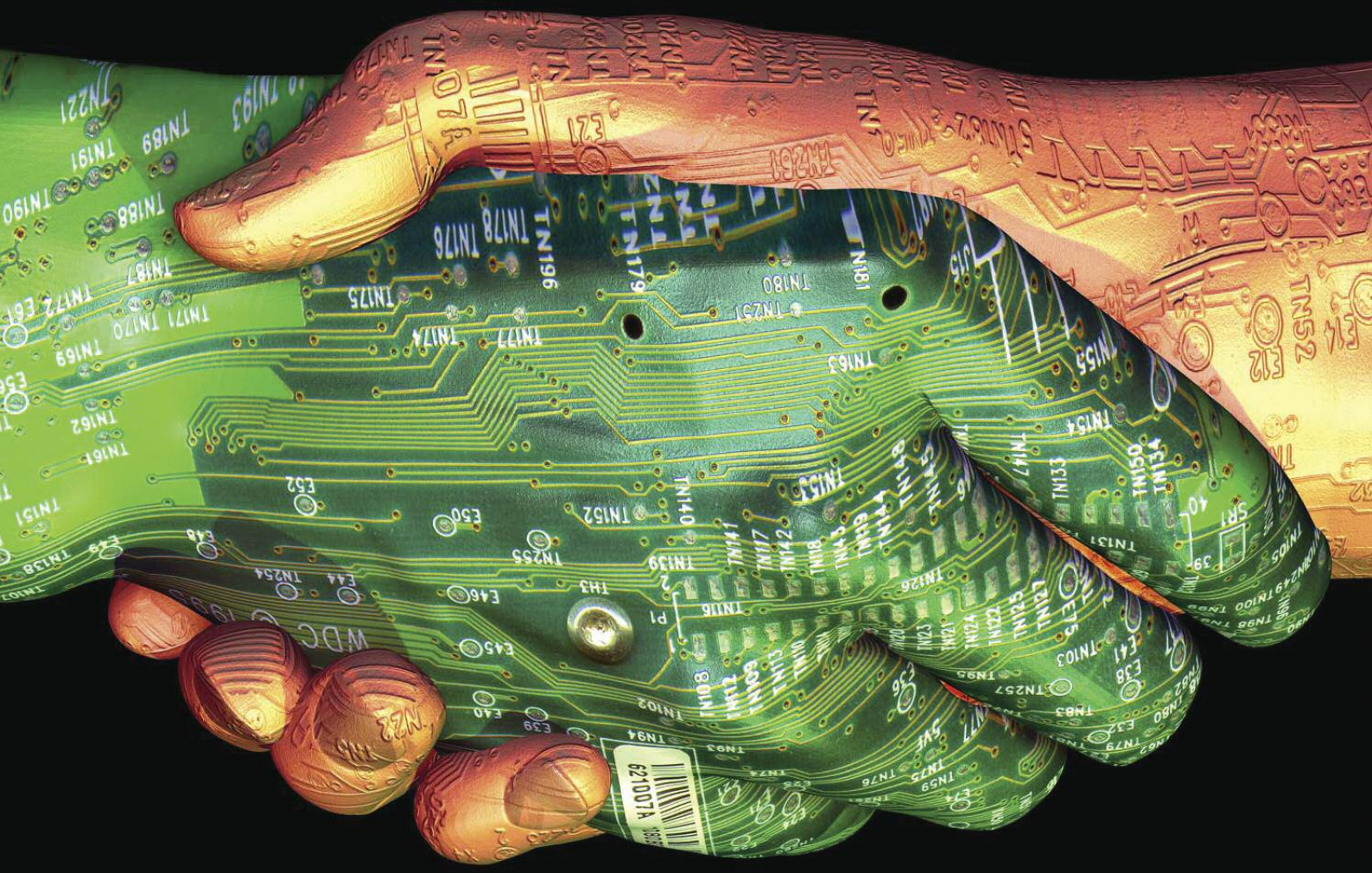
ERCIM NEWS

www.ercim.eu

Special theme:

Trustworthy Systems of Systems

Safety & Security Co-engineering



Also in this issue:

ERCIM News is the magazine of ERCIM. Published quarterly, it reports on joint actions of the ERCIM partners, and aims to reflect the contribution made by ERCIM to the European Community in Information Technology and Applied Mathematics. Through short articles and news items, it provides a forum for the exchange of information between the institutes and also with the wider scientific community. This issue has a circulation of about 6,000 printed copies and is also available online.

ERCIM News is published by ERCIM EEIG
BP 93, F-06902 Sophia Antipolis Cedex, France
Tel: +33 4 9238 5010, E-mail: contact@ercim.eu
Director: Jérôme Chailloux
ISSN 0926-4981

Contributions
Contributions should be submitted to the local editor of your country

Advertising
For current advertising rates and conditions, see http://ercim-news.ercim.eu/ or contact peter.kunz@ercim.eu

ERCIM News online edition
The online edition is published at http://ercim-news.ercim.eu/

Subscription
Subscribe to ERCIM News by sending an email to en-subscriptions@ercim.eu or by filling out the form at the ERCIM News website: http://ercim-news.ercim.eu/

Next issue
October 2015, Special theme: Augmented Reality

Cover: source GoGraph.com

Trustworthy Systems of Systems – A Prerequisite for the Digitalization of Industry

by Werner Steinhögl

In our modern world, with all aspects of our lives becoming increasingly digitalized, Systems of Systems will play a crucial role. As the embedded world meets the Internet world there will be an increasing number of interacting systems with strong connectivity in both society and in industry. The growing overall complexity of systems has triggered a paradigm shift and the need to enhance the classical view of Systems Engineering towards Systems of Systems (SoS) Engineering. SoS describes the large scale and dynamically varying integration of many independent, self-contained systems to satisfy needs for services that can only be provided by the system as a whole. Examples of SoS include the electrical grid, a large processing plant with many process units, multimodal traffic control, and combined heat and power generation.

Connectivity between embedded systems and computing devices is predicted to experience massive growth over the coming years. For instance, the consultancy Gartner estimates that by 2020 there will be 26 billion connected devices (excluding PCs, tablets and smartphones) in operation worldwide. This equates to a global market value of $1.9 trillion, of which 80% is expected to come from services. Mastering SoS will be imperative for companies to be successful, because connectivity provides value only if the information is used for improved services, productivity, resource efficiency, and user satisfaction, i.e. if additional functionality is offered and the systems as a whole operate reliably and securely in a SoS.

The field of SoS deals with how to engineer and manage such large interconnected and continuously evolving systems, and is thus fundamental to the realization of this market potential. The EU funded coordination action CPSOS has compiled a state of the art report and identified the challenges for this field. Methods from different domains need to be combined with systems and domain engineering such as control theory for continuous systems, discrete models from computer science for verification/testing and contract-based assertions, structure formation from physics and market mechanisms and evolution of beliefs from economics and social science. Modelling and simulation are crucial in this effort. Promising results have been obtained in some relatively controlled envi-

Werner Steinhögl, Programme Officer at the European Commission, Components and Systems, Directorate General CONNECT

ronments, such as chemical plants and traffic management. Yet in general the application of model-based methods in SoS engineering is still at the beginning and needs to find its way from research labs into practice.

Trust in Systems of Systems

Cyber-security is a very important element in Systems of Systems and must be addressed at all system and component levels. A specific SoS challenge is the recognition of obstructive injections of signals or takeovers of components in order to cause malfunctions, suboptimal performance, shutdowns or accidents, e.g. power outages. The detection of such attacks requires taking into account both the behaviour of the physical elements and the computerized monitoring, control and management systems. In the case of the detection of unsecure states, suitable isolation procedures and soft (partial) shut-down strategies must be designed. Needless to say, SoS must also be safe and must comply with relevant safety standards which necessitates a rethinking of certification approaches.

The European Situation

Europe has a strong position in the systems market with an ecosystem of world leading suppliers and systems integrators. The embedded systems industry alone creates 50,000 new jobs every year and Europe accounts for 30% of world production of embedded systems with particular strengths in the automotive sector, aerospace and health. There is fierce competition within the existing €850 billion embedded ICT market with strong players in the US aiming to capitalize on the expanding market. Europe needs to capitalize on its expertise via successful exploitation of ICT in Systems of Systems: there are opportunities to provide efficient, environmentally friendly, autonomous and safe mobility; greater efficiency in management and operations for process automation and smart grids; greater benefits to citizens via smart, safe and secure cities, energy efficient buildings and green infrastructure; and smart devices and services for smart home functionality and assisted living.

However, today's platforms for systems are often vertically oriented and proprietary which makes it difficult to link heterogeneous subsystems into a SoS. The vision is that a group of autonomously managed subsystems are coordinated and optimized to deliver a joint service. This includes, for instance, seamless and dynamic integration of new incoming subsystems into a SoS even when they come from different suppliers. Hence work on making platforms more open and interoperable is required.

EU support for trustworthy Systems of Systems

The European Union supports collaborative research and innovation in the area of Systems of Systems with an investment of 30 million Euros. In the wider area of Embedded Systems, Cyber-Physical Systems, Security and Internet of Things circa 150 million Euros per year are earmarked in the Horizon 2020 work programme and the Joint Technology Initiative ECSEL. As a flanking measure, the EU supports networks of competence centres to enable access to digital technologies for any industry in Europe.

Acknowledging the importance of digital platforms for industry, the EU and its member states have jointly launched large-scale innovation projects to demonstrate open, integrated and secure technology and operational platforms for product development, process automation and associated services in the ECSEL JTI programme. This will continue, and in addition large scale pilots for Internet of Things platforms are planned. These actions will also contribute to the design, development, demonstration and testing/validation of platforms for SoS and contribute to standardization and stimulation of the related ecosystem and marketplaces.

Links:

CPSOS coordination action:
http://www.cpsos.eu
Cyber-Physical Systems in Horizon 2020:
https://ec.europa.eu/digital-agenda/en/cyberphysical-systems-0
ECSEL Joint Technology Initiative:
http://www.ecsel-ju.eu
Internet of Things in Horizon 2020:
https://ec.europa.eu/digital-agenda/en/internet-things

KEYNOTE

JOINT ERCIM ACTIONS

EVENTS, IN BRIEF

SPECIAL THEME

The special theme section "Trustworthy Systems of Systems" has been coordinated by Poul Heegaard, NTNU and Erwin Schoitsch, AIT.

RESEARCH AND INNOVATION

This section features news about research activities and innovative developments from European research institutes

All photos by G. Scagnelli © Inria

20 years celebration of W3C Europe in the Paris city hall.

Michel Cosnard, former Inria CEO and ERCIM President

W3C Celebrated 20 Years in Europe

ERCIM and Inria organized W3C Europe's 20th anniversary event in the salons of the Paris City Hall, on Tuesday 5 May 2015.

Twenty years ago, the Web, born in Europe, was just taking off and the first cracks of browser fragmentation began to appear. To heal the cracks, a small group launched the World Wide Web Consortium, a big name for an even bigger project. This year, we celebrated the 20th anniversary of the European branch of W3C which played a key role in keeping the Web free, open and accessible to everyone.

Tim Berners-Lee, W3C director and Web inventor, together with a panel of Web luminaries, shared his vision of the future Web. The symposium speakers included Emmanuel Grégoire, Deputy Mayor of Paris; Michel Cosnard, former Inria CEO and ERCIM President; Axelle Lemaire, French Ministry of State for Digital Affairs; Isabelle Falque-Pierrotin, President of CNIL; Mário Campolargo, Director for "Net Futures" - DG CONNECT, European Commission; Inmaculada Placencia Porrero, Deputy Head of Unit for Rights of Persons with Disabilities, European Commission; Nicolas Colin, co-founder and partner, TheFamily, and Jean-François Abramatic, senior scientist at Inria, former W3C chairman and CEO.

Standardization, accessibility, privacy and the Web of Things were in the focus of the symposium. "We made a good a job, but we are far from having finished" concluded Tim Berners-Lee.

The Web is incredibly innovative, incorporating all manner of user experiences, business models, audio and video, data, programming paradigms, and hardware. W3C Europe can be proud of having achieved a lot during its 20 years of existence. Remaining and emerging topics are numerous and challenging, but the Web community's passion for building the Web helps us keep pace with the rapid changes in our field.

The event was sponsored by Inria and ERCIM, former and current W3C Europe hosts, and by Hachette Livre, as W3CEurope@20 supporter.

Link:
http://www.w3.org/20/Europe/

Axelle Lemaire, French Ministry of State for Digital Affairs

Isabelle Falque-Pierrotin, President of CNIL

Inmaculada Placencia Porrero, European Commission

Tim Berners-Lee, W3C director and Web inventor

PaaSage and OW2 Announced Platform Availability on the AppHub Marketplace

PaaSage, a large scale European research initiative for developing an open and integrated platform to support model based lifecycle management of Cloud applications for software and service providers, led by ERCIM, and OW2, the Open Source community for infrastructure software, announced a strategic partnership in June 2015. This partnership will open up access to the PaaSage platform through the AppHub European Open Source Market Place and accelerate the building of a wide community around the PaaSage technology.

As of today, Cloud solutions are still insufficient and in particular require from developers, operators and providers a high level of expertise to properly exploit the capabilities offered by Cloud technologies. Cloud infrastructures are not standardised and porting an existing application to a Cloud platform is still a very challenging task, leading to strong dependencies between the client application and the Cloud platform. Developing once and deploying on many Clouds is what the PaaSage platform enables.

PaaSage is an integrated open source platform to support both design and deployment of Cloud applications, together with an accompanying methodology that allows model-based development, configuration, optimisation and deployment of existing and new applications independently of the existing underlying Cloud infrastructures. The first version of PaaSage will be easily deployable from AppHub, the European Open Source Market Place, as soon as it is progressively published during the second half of 2015.

"We are delighted to partner with OW2 in order to provide PaaSage with the widest audience and community in Europe and beyond. This will help us to maximise the impact of our investment in the PaaSage platform", said Geir Horn, from University of Oslo, technical coordinator of the PaaSage platform.

Launched in October 2012, PaaSage is a research project carried out by 19 European partners. The PaaSage technology and the AppHub market place will be showcased at the major ICT event organised by the European Commission in Lisbon, Portugal, in October 2015 (ICT 2015, Innovate, Connect, Transform, @ICT2015eu).

PaaSage software source code is now hosted on the OW2 community forge.

Links: http://www.paasage.eu
http://www.apphub.eu.com
http://www.ow2.org

Please contact:
Pierre Guisset, ERCIM Office
E-mail: pierre.guisset@ercim.eu

"Big Data Europe" to Empower Communities with Data Technologies

ERCIM EEIG / W3C is partner in a new European project that develops a platform to facilitate big data usage.

The "BigDataEurope" project aims at developing a Big Data platform based on requirements identified with stakeholders from the seven H2020 societal challenges: Climate, Energy, Health, Transport, Social sciences, Food and Security. The consortium, led by Fraunhofer IAIS will engage with these communities to identify their big data technology needs, to design and realise the required ICT infrastructure and support the use and deployment of the platform.

With this platform,the project will provide companies and institutions with an integrated and ready-to-use palette of Big Data tools that is adapted to their particulary needs. Small and medium-sized companies who do often not have the resources for hiring specialized data scientists will especially benefit from the lowered entrance bar into the Big Data world as they are offered the opportunity to easily understand and use state-of-the-art data science tchniques for their business.

The project tackles two keyaspects. First, BigDataEurope will build up a network between stakeholders of the key European societal sectors. Interest groups modelled afte the W3C scheme will then be launched to discuss the particular needs of each sector in a series of workshops that will cover the whole process of data usage; from data collection, processing, storage, and visualization to the development of data services. The second aspect of the project will see tha the requirements collected in the workshops are used to guide the technical development and implememtation of the open BigDataEuurope Platform.

The first workshop, focussing on the health and demographic change societal challenge was held in Brussels on 21 May 2015. The second workshop wil focuses on "smart, green and integrated transport". Participants to this workshop will have the opportunity to influence the design, and ultimate benefit from the Big Data platform that the BigDataEurope project will deliver.

BigDataEurope started in January 2015, and will last three years.

Link:
http://www.big-data-europe.eu

Please contact:
Sören Auer, Fraunhofer IAIS, Germany
E-mail: soeren.auer@iais.fraunhofer dot de

Introduction to the special theme

Trustworthy Systems of Systems

Safety & Security Co-engineering

by Poul Heegaard and Erwin Schoitsch

In a highly interconnected world, a finite number of independently operable and manageable systems are networked together to achieve a higher goal as constituent systems of a 'System-of-Systems' (SoS), also referred to as a 'Digital Ecosystem'. Systems of Systems - characterized by self-organization, autonomous constituent systems, continuous evolution, scalability and sustainability - provide both economic and social value. Examples of SoS include: the smart power grid with power plants and power distribution and control, smart transport systems (rail, traffic management with V2V and V2I facilities for highly automated or autonomous driving, air traffic control systems), advanced manufacturing systems (industry 4.0), mobile co-operating autonomous robotic systems or vehicles, health-care systems, smart buildings and neighbourhoods - from local communities through to smart cities.

The main purpose of Systems-of-Systems (SoS) is to provide new services, but with highly interacting and interdependent ICT systems relying on critical infrastructures, new threats and challenges arise. Very often constituent systems are legacy systems not designed for integration into a system-of-systems which is another challenge for achieving and proving trustworthiness. Services delivered involve a chain of stakeholders that share the responsibility for providing robust and secure services with stable and good performance. The interacting relationship between the stakeholders is agreed upon in Service Level Agreements (SLAs), which gives guarantees on the non-functional properties of the services. How can we trust the services of such Systems-of-Systems? How can safe, reliable and secure interoperability of critical services be guaranteed? How should they be designed, implemented, deployed, operated and managed?

One crucial challenge is the operation of the SoS. To make optimal use of available resources, the complexity of the (sub-)systems and their operation will increase owing to increased interconnectedness and complexity. The support system itself contributes to the complexity, as do the public ICT services, which rely on cooperation between multiple stakeholders and an overall system that is not engineered. Consequently, there is no aggregated insight into the design and operation of SoS. Coordinated management would require co-operation between multiple network domains and various technologies and stakeholders.

In this context, the constituent systems to be considered are not only the complex ICT systems themselves, but also Cyber-physical systems (CPS), i.e. embedded ICT systems with strong relationship to physics, mechatronics and the notion of interaction with each other and with an unpredictable environment. The result may be 'emergent properties' - unforeseen or unpredicted behaviour that may have critical effects. Cyber-physical Systems-of-Systems (CPSoS) must be adaptable, reconfigurable and extendable during their lifetime, since the classical predictability assumptions of safety and cyber-security assessment and certification no longer hold [2].

The society strongly depends on ICT and CPSoS services, which have to be trustworthy since the negative impact of a failure or cyber attack might have considerable consequences for the society. Thus, the system and service dependability (safety, security, reliability, availability, maintainability, etc.), as well as resilience, robustness, and sustainability, must be evaluated in a holistic manner [1]. Therefore, European research programmes and complementary national research programmes are targeting CPSoS as a research topic. In-

dividuals and economies are becoming increasingly dependent on these systems – but how can we achieve trust in their dependability, performance, safety, security and privacy [3]? Several challenges and questions arise:

- How can we achieve trust in SoS?
- How to conduct safety and cyber-security co-assessment, co-engineering and certification/qualification?
- What are the challenges in resilience, robustness, sustainability – and how may we achieve these properties?
- What are the challenges of dependable services and interoperability of systems and services?
- Which safety and security standards should we apply? Which gaps should be covered? What are the recent developments in this area?
- How can reliable, safe and secure interoperability of systems and services be achieved? (frameworks and standards)
- Which design, development and verification and validation, and certification/qualification paradigms have to change? What are the recent developments in this area?
- How can we manage the complex requirements of constituent systems (multi-role, multi-multi-actor, multi-user and requirements, multi-technology) and the interaction with each other and other critical systems (e.g. power-systems, health care, transportation, financial systems)?
- What are some examples of challenges from different domains and how are these challenges being addressed?
- How can highly interdependent systems be run optimally without knowing the finer details of all systems involved?
- Can such SoS be operated and managed by multiple entities with only a business agreement (e.g. SLA) between them?
- How can responsibilities and liabilities be managed when these are many third party suppliers?
- How can during lifetime evolutionary processes, changes, reconfigurations and adaptations be managed, and trust be guaranteed and maintained over time?

This ERCIM News issue features a keynote by Werner Steinhögl, Programme Officer at the European Commission, Components and Systems, Directorate General CONNECT, highlighting the importance of trustworthiness of systems of systems for the digitalization of industry and European competitiveness in the industrial systems market and industrial production. This implies widespread support of collaborative research and innovation in the area of systems of systems, embedded/cyber-physical systems, safety and security, Internet of Things in Horizon 2020 in the JTI ECSEL.

In the special theme section, the keynote is complemented by an invited article by Andreas Wild, Executive Director of the ECSEL (Electronic Components and Systems for European Leadership) JU (Joint Undertaking) on strategic activities in the context of the ECSEL Joint Technology Initiative and its predecessors, the ARTEMIS and ENIAC JUs. Here, selected projects are outlined to illustrate the areas of power electronics and electric mobility.

The 17 regular articles of the special section are clustered into subsections comprising three or four articles according to their main messages and subtopics:

- Overview articles, networks and cross-cutting projects,
- Safety & Cybersecurity co-engineering,
- Building and verifying trustworthy SoS,
- Methods, techniques and tools,
- Applications, emergency recovery.

This clustering will help the reader navigate the wide area of safe, secure and reliable (dependable) engineering of systems of systems. Most of the aforementioned challenges and questions are tackled in these articles.

Links:

https://ec.europa.eu/digital-agenda/en/system-systems

AMADEOS: Architecture for Multi-criticality Agile Dependable Evolutionary Open System-of-Systems:
http://amadeos-project.eu/

System of Systems Overview, SEI, Carnegie Mellon University:
http://www.sei.cmu.edu/sos/

References:

[1] J-C. Laprie: "Resilience for the Scalability of Dependability", 4th International IEEE Symposium on Network Computing and Applications, IEEE CPS 2005, Cambridge, MA, p. 5-6, ISBN 0-7695-2326-9.

[2] D. Schneider, E. Schoitsch, E. Armengaud: "Towards Trust Assurance and Certification in Cyber-Physical Systems"; in Computer Safety, Reliability and Security, 33rd International Conference, SAFECOMP 2014, Springer, LNCS 8696, pp. 180- 191. 2014 ISBN: 978-3-319-10505-5.

[3] C. Schmittner et al.: "A Case Study of FMVEA and CHASSIS as Safety and Security Co-Analysis Method for Automotive Cyber-physical Systems", in Proc. of 1st ACM Workshop on Cyber-Physical System Security (pp. 69-80), ACM, 2015.

Please contact:

Erwin Schoitsch
Austrian Institute of Technology, Austria
E-mail: Erwin.Schoitsch@ait.ac.at

Poul Heegaard
NTNU, Norway
E-mail: poul.heegaard@item.ntnu.no

ECSEL JU Launches Research and Innovation Actions Strengthening European Competitiveness

by Andreas Wild

Less than one year since its inception, the ECSEL (Electronic Components and Systems for European Leadership) Joint Undertaking (JU) is launching six research and innovation actions and six innovation actions arising from its 2014 calls, investing €708 million in electronic components and systems. The ECSEL JU is established by the European Council with the aim to keep "Europe at the forefront of technology development, bridging the gap between research and exploitation, strengthening innovation capabilities and creating economic and employment growth in the Union".

Over the last five years, two organizations preceding ECSEL JU under FP7 (ENIAC and ARTEMIS JUs) pioneered a new type of project: "pilot line" or "innovation pilot" projects, positioned at higher technology readiness levels in order to bridge the "valley of death" separating the scientific discovery from its economic valorisation. Using open and competitive calls for proposals and a transparent evaluation and selection process, the JUs succeeded in concentrating investments on high priority, strategic topics. In fact, leading European companies engaged their ecosystems, assigned sizable research and innovation budgets, and used their best specialists in preparing convincing proposals that succeeded exclusively based on their merits. The JUs run a transparent evaluation and selection process performed by independent experts and public authorities.

The following examples illustrate two important areas (among others) in which a sequence of projects attracted significant private and public funding, commensurate with the global investments in the field, to advance the state of the art and generate industrial impact.

Power electronics

In power electronics, a sequence of proposals selected for funding address the societal challenge of energy efficiency:

- *EPT300:* Enabling Power Technologies on 300mm Wafers (April 2012- March 2015) introduced unique 300mm diameter substrates thinner than paper, processing equipment, handling and automation concepts creating world's most efficient and most affordable devices.
- *EPPL:* Enhanced Power Pilot Line (April 2013- March 2016) is setting up a pilot line for high reliability devices of the next generations, and chip-to-package 3D integration to optimally serve industrial, medical and mobility applications.
- *eRAMP:* Excellence in Speed and Reliability for More than Moore Technologies (April 2014- March 2017) accelerates yield learning and uses cloud based design technology and heterogeneous integration to demonstrate highest energy efficiency in motor drives, healthcare equipment and LED lighting applications.

ECSEL JU launches now a new Innovation Action taking these concepts to the next level:

- *PowerBase:* Enhanced Substrates and GaN Pilot Lines Enabling Compact Power Applications (May 2015 – April 2018) using innovative silicon and gallium nitride substrates combined with embedded chip assembly technologies to achieve unparalleled efficiency in compact power applications.

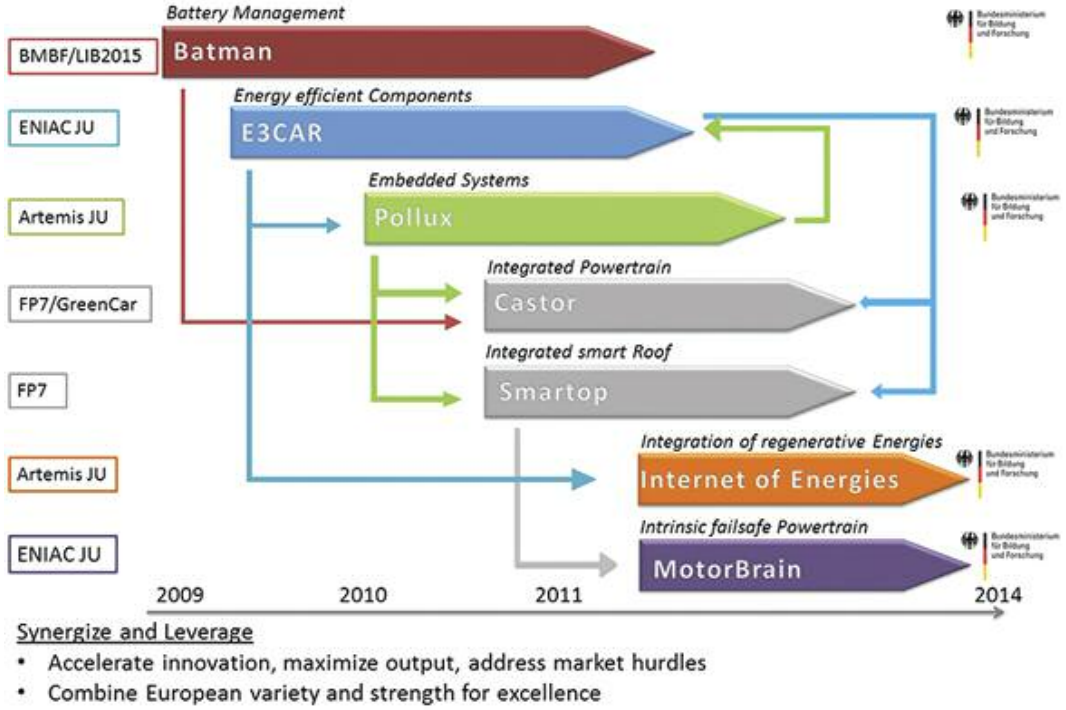


Figure 1: Convergence of European Electric Vehicle projects.

The 130 participations from 12 countries engaged €270 million, and have been awarded €76 million national and €48 million EU grants to position Europe as the leader in power electronics.

Electric mobility

European companies are world leaders in automotive innovation and sales. Together with their suppliers of electronic components and systems, they have proposed ambitious actions to establish leadership in electric mobility.

- *E3Car:* Nanoelectronics for an Energy Efficient Electrical Car (Jan 2009 – Jan 2012) achieved a breakthrough in nanoelectronic technologies, devices and miniaturised subsystems achiev-ing 35% energy savings for the same performance.
- *Pollux:* Process Oriented Electrical Control Units for Electrical Vehicles Developed on a Multi-system Real-time Embedded Platform (Mar 2010 - Feb 2013) generated the first platform concept for electric vehicles architecture, electronics, communication and embedded systems.
- *IoE:* Internet of Energy for Electric Mobility (May 2011 - Apr 2014) enabled seamless connectivity and created middleware to achieve interoperability of the Internet applications addressing the electric mobility infrastructure.
- *Motorbrain:* Nanoelectronics for Electric Vehicle Intelligent Failsafe Powertrain (Apr 2011 – Mar 2014) introduced radical innovation in component and subsystems resulting in unparalleled energy efficiency of the drive-train and safe exit from traffic even in case of failure.

ECSEL JU is now launching a new research and innovation action, taking these concepts to the next level:

- *3CCAR:* Integrated Components for Complexity Control in Affordable Electrified Cars (Apr 2015 – Apr 2018) shall introduce innovative approaches at all levels (vehicle architecture, sub-systems, components) to increase the affordability of the electric vehicles and accelerate their market penetration.

One hundred and fifty one participations from 16 countries engaged €175 million , and were awarded €49 million national and €37 million EU grants to defend Europe's leading position in the global competition.

Conclusion

The ECSEL JU three-way funding model (private sector, Member States and EU) is proven as compelling. It succeeds in leveraging significant private and public investments and concentrating them on strategic priorities. The ECSEL JU offers a fertile collaborative environment for large and small companies, academic and institutional researchers from all around Europe, together developing and implementing high impact industrial strategies, which are beneficial for Europe in general.

Link:
http://www.ecsel-ju.eu/

Please contact:
Andreas Wild, Executive Director of the ECSEL Joint Undertaking
E-mail: Alun.Foster@ecsel.europa.eu

Core Research and Innovation Areas in Cyber-Physical Systems of Systems

by Michel A. Reniers, Sebastian Engell and Haydn Thompson

The CPSoS project (http://www.cpsos.eu) is developing a European roadmap for future research activities in Cyber-Physical Systems of Systems (CPSoS), which are large complex physical systems that interact with and are controlled by a considerable number of distributed and networked computing elements and human users [1]; see Figure 1. Examples include automotive systems [2], rail systems, electric grids, smart buildings, and large production facilities.

To date, research activities on CPSoS have largely been performed by individual domains, e.g. computer science, simulation technology and systems and control, with little cooperation and exchange between the different areas. To capture the views of industry and academia and from different communities, the CPSoS project has set up three working groups:

- Systems of Systems (SoS) in Transportation and Logistics,
- Physically Connected Systems of Systems,
- Tools for Systems of Systems Engineering and Management.

The working groups currently comprise 36 members, leading specialists from industry and academia, and include delegates from ongoing EU-funded projects in the area of SoS to ensure that as many views as possible are represented. Members of the working groups are listed at http://www.cpsos.eu.

By means of three industry/academia working groups, public workshops and consultations and interviews with over 100 practitioner experts in the field from large companies, mid-caps, SMEs and academia, the project has produced a comprehensive view of the state-of-the-art in transport and logistics, electric grids, smart buildings, industrial production systems and in supporting tools and techniques (see http://www.cpsos.eu/state-of-the-art/). The discussions in the working groups and the consultations have been summarized in a working paper on the core research and innovation areas (see http://www.cpsos.eu/roadmap/). Three key research topics, described below, have been identified:

Challenge 1: Distributed, reliable and efficient management of Cyber-Physical Systems of Systems

Owing to the scope and complexity of CPSoS as well as the ownership or man-

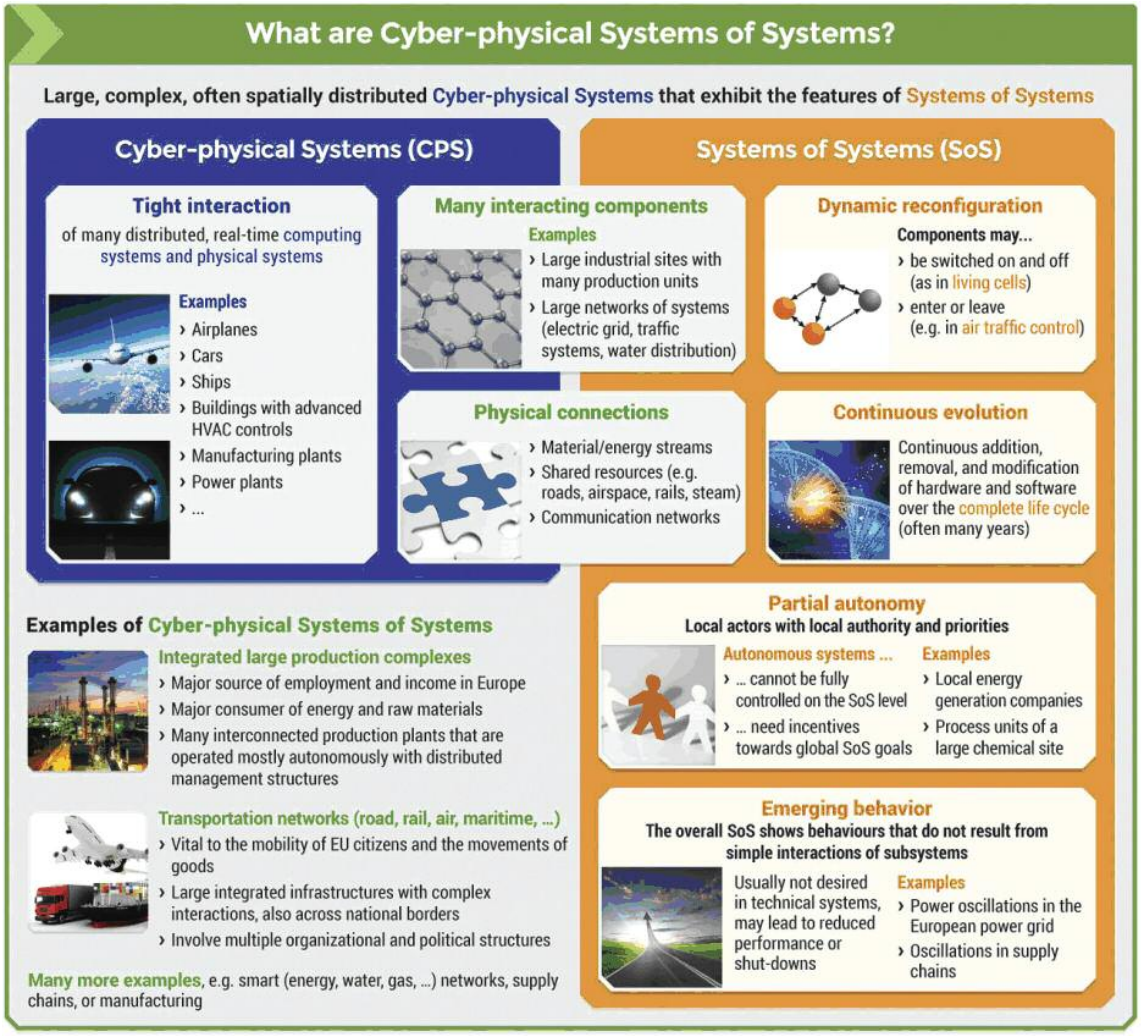


Figure 1: Explanation of Cyber-Physical Systems of Systems, from [3].

agement structures, the control and management tasks in such systems cannot be performed in a centralized or hierarchical top-down manner with one authority tightly controlling all subsystems. In CPSoS, there is a significant distribution of authority with partial local autonomy [3]. The design of such management systems for reliable and efficient management of the overall systems poses a key challenge in the design and operation of CPSoS.

The following sub-topics should be addressed:

- Decision structures and system architectures,
- Self-organization, structure formation, and emergent behaviour in technical systems of systems,
- Real-time monitoring, exception handling, fault detection and mitigation of faults and degradation,
- Adaptation and integration of new components,
- Humans in the loop and collaborative decision making,
- Trust in large distributed systems.

Challenge 2: Engineering support for the design-operation continuum of Cyber-Physical Systems of Systems

While model-based design methods and tools have been established in recent years in industrial practice for traditional embedded systems, the engineering of CPSoS poses key challenges that go beyond the capabilities of existing methodologies and tools for design, engineering, and validation. These challenges result directly from the constitutive properties of CPSoS, such as their process of continuous evolution and the high degree of heterogeneity and partial autonomy of CPSoS.

The efficient design and operation of such systems requires new design support methodologies and software tools in the following areas:

- Integrated engineering of CPSoS over their full life-cycle,
- Modelling, simulation, and optimization of CPSoS, and
- Establishing system-wide and key properties of CPSoS.

Challenge 3: Cognitive Cyber-Physical Systems of Systems

SoSs by their very nature are large, distributed and extremely complex, presenting a myriad of operational challenges. To cope with these challenges there is a need for improved situational awareness. Gaining an overview of the entire SoS is inherently complicated by the presence of decentralized management and control. The introduction of cognitive features to aid both operators and users of complex CPSoS is seen as a key requirement for the future to reduce the complexity management burden from increased interconnectivity and the data deluge presented by increasing levels of data acquisition. Research in a number of supporting areas is required to allow vertical integration from the sensor level to supporting algorithms for information extraction, decision support, automated and self-learning control, dynamic reconfiguration features and consideration of the sociotechnical interactions with operators and users.

The following subtopics have been identified as being necessary to support a move to Cognitive CPSoS:

- Situation awareness in large distributed systems with decentralized management and control,
- Handling large amounts of data in real time to monitor the system performance and to detect faults and degradation,
- Learning good operation patterns from past examples, auto-reconfiguration and adaptation,
- Analysis of user behaviour and detection of needs and anomalies.

A public consultation process on the roadmap was undertaken in April-June 2015 (results: http://www.cpsos.eu/public-consultation/).

The research topics listed above provide a strategic long-range research agenda. The working groups of CPSoS will complement this strategic research agenda by sector-specific medium-term research and innovation topics that should be tackled by cooperative research projects in the near future.

Further information will be provided in the CPSoS newsletter which is available via http://www.cpsos.eu/news-events/news/.

The CPSoS project has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 611115.

Link: http://www.cpsos.eu

References:

[1] M. A. Reniers, Sebastian Engell: "A European Roadmap on Cyber-Physical Systems of Systems", ERCIM News 2014 (97), 2014.

[2] R. Boagey: "Automotive Cyber-physical systems: the next computing revolution", Automotive Megatrends, Q3, pages 104-106, 2014.

[3] S. Engell, J. Lygeros, S.Grammatico: "The emergence of systems of systems", Pan European Networks: Science & Technology, Vol 14, pages 79-81, 2015, http://www.paneuropeannetworkspublications.com/ST14/#78

Please contact:
Michel Reniers, TU/e, The Netherlands
E-mail: m.a.reniers@TUE.nl

GT SoS: Research Network on Trustworthy Software-intensive Systems-of-Systems

by Flavio Oquendo, Axel Legay and Khalil Drira

This French initiative in the framework of the CNRS GDR GPL establishes an open research network for tackling the emerging domain of software-intensive systems-of-systems. It focuses on bringing together researchers and practitioners, in a national effort, to discuss and enable the development of novel and sound theories, languages, methods, processes, and tools for architecting and engineering trustworthy software-intensive systems-of-systems.

Since the dawn of computing, the complexity of software and the complexity of systems reliant on software have grown at a staggering rate. In particular, software-intensive systems have rapidly evolved from being stand-alone systems in the past, to be part of networked systems in the present, to increasingly become systems of systems in the future.

With networks becoming increasingly pervasive, it is now possible to interconnect systems that were independently developed, operated, managed, and evolved, yielding a new kind of complex system, i.e. a system that is itself composed of systems, the 'System-of-Systems' (SoS). SoSs are evolutionarily developed from systems to achieve missions that cannot be achieved by a system alone.

Trustworthy SoSs are of paramount necessity since various aspects of our lives and livelihoods are becoming progressively dependent on some sort of SoS. SoSs are relied upon in areas as diverse as aeronautics, the automotive industry, energy, healthcare, manufacturing, and transportation; and applications that address societal needs, such as environmental monitoring, emergency coordination, traffic control, smart grids, and smart cities.

Complexity is intrinsically tied to SoSs, since SoSs by definition result in emergent behaviour: missions are achieved in SoSs through emergent behaviour drawn from the local interaction among constituent systems.

Therefore, the endeavor of conceiving and constructing trustworthy systems has evolved from engineering complicated systems in the last century, to architecting trustworthy SoSs in this century [1]. Trustworthy SoSs, by their very nature, have intrinsic properties that are hard to address.

Indeed, trustworthiness is a holistic property that calls for the co-engineering of safety and cyber-security, among other qualities. It is not sufficient to address one of these attributes in isolation, nor is it sufficient simply to assemble constituent systems that are themselves trustworthy (composing trustworthy constituent systems may imply an untrustworthy SoS). Integrating the constituent systems and understanding how the trustworthiness dimensions interact as well as how these interactions create emergent behaviour influencing safety and security is a central issue in architecting a trustworthy SoS.

A grand research challenge is presented by the unique characteristics of SoSs, namely: the operational and managerial independence of their constituent systems, as well as their geographic distribution (they are not all in one place), and the evolutionary development and emergent behaviours that emerge.

Additionally, the environment in which an SoS operates is only partially known at design-time, i.e. it is too unpre-

dictable to be summarized within a fixed set of specifications, thus there will inevitably be novel situations to deal with at run-time. Hence, the challenge is to architect and engineer an SoS in a way that it can dynamically accommodate to new situations acting only in the way it constructs coalitions of systems while continuing to act to fulfill its own mission.

Overall, the grand challenge raised by SoSs calls for a novel paradigm and novel scientific approaches for architecting and engineering trustworthy software-intensive SoSs [2] deployed in unpredictable environments while assuring their continuous trustworthiness, taking into account their unique characteristics.

Source: https://ec.europa.eu/digital-agenda/en/system-systems/

Systems-of-Systems - A digital agenda for Europe.

Roadmaps

The importance of developing novel theories, languages, methods, processes, and tools for architecting and engineering trustworthy software-intensive SoSs is highlighted in several roadmaps targeting year 2020 and beyond (Figure 1).

In France, a report prepared by the French Ministry of Economy explicitly targets SoSs as one of the key technologies for the period 2015-2025 (étude prospective sur les technologies clés à 2015-2025, Direction Générale de la Compétitivité, de l'Industrie et des Services du Ministère de l'Economie). This technology is also explicitly targeted in the studies developed by the initiative of the European Commission, in particular ROAD2SoS (Development of Strategic Research and Engineering Roadmaps in Systems-of-Systems) and T-Area-SoS (Trans-Atlantic Research and Education Agenda in Systems-of-Systems).

These roadmaps highlight the importance of progressing from the current situation, where SoSs are developed in ad-hoc way, to a scientific approach providing rigorous theories and technologies for mastering the complexity of software-intensive SoSs, in particular for achieving trustworthy SoSs.

The GT SoS, a French initiative in the framework of the CNRS GDR GPL, brings together researchers and practitioners in a national effort to discuss and enable the development of novel and sound theories, languages, methods, processes, and tools for architecting and engineering trustworthy software-intensive systems-of-systems.

Composition of the GT SoS

The GT SoS is composed of 28 founding members representing 16 academic groups and 12 institutional and industrial partners.

The sixteen academic groups are: ACADIE, ARCHWARE, CPR, DIVERSE, ESTASYS, ISC, MACAO, MAREL, MODALIS, MOVIES, RSD, SARA, SOC, SPADES, SPIRALS, and TEA. Fourteen of these groups are distributed in nine research units of CNRS, of which eight are UMR (CRISTAL, I3S, IRISA, IRIT, LIRIS, LIRMM, LIX, and VERIMAG), one 1 UPR (LAAS), and in three research centres of INRIA (Rennes Bretagne Atlantique, Lille Nord Europe, and Grenoble Rhône-Alpes). The last two are host teams from MENESR (CEDRIC and LIUPPA).

These groups bring together 146 researchers working on topics related to software-intensive systems-of-systems, of which 71 are academics, 59 are PhD students, and 16 are post-docs.

To these academic groups are added two Initiatives of Excellence: LabEx M2ST and IRT SystemX.

The industrial participation includes key players of the domain of systems-of-systems: AIRBUS, CAP GEMINI, CS, DCNS, SEGULA, THALES Group, THALES Alenia Space, THALES Communications et Sécurité, THALES Recherche & Technologie; as well as the French Association for Systems Engineering (AFIS).

This GT being an open initiative, it is open to new members according to the GDR GPL procedures.

Links:
http://gdr-gpl.cnrs.fr/
https://ec.europa.eu/digital-agenda/en/system-systems/

References:
[1] M. Jamshidi (Ed.): "System-of-Systems Engineering: Innovations for the Twenty-First Century", Wiley, November 2008.
[2] F. Oquendo et al. (Eds): "Software Engineering for Systems-of-Systems", ACM, July 2013.

Please contact:
Flavio Oquendo
IRISA (UMR CNRS, Inria & Universities of Rennes and South-Brittany), France
E-mail: flavio.oquendo@irisa.fr
http://people.irisa.fr/Flavio.Oquendo/

Axel Legay
Inria and IRISA, France
E-mail: axel.legay@inria.fr
http://people.irisa.fr/Axel.Legay/

Khalil Drira
LAAS-CNRS, France
E-mail: khalil@laas.fr
http://homepages.laas.fr/khalil/

Operational Trustworthiness Enabling Technologies - The OPTET Project

by Costas Kalogiros, Vasilis Tountopoulos, Sotiris Ioannidis, Sebastien Keller and Pascal Bisson

OPTET introduces a trustworthiness-by-design methodology for the development of socio-technical systems. It defines a unified model of trust and trustworthiness to describe the processes of such systems, and delivers a set of generic enablers on trustworthiness that will complement large-scale ICT platforms and contribute to achieve better trust distribution.

OPTET, an EU-funded project under the 7th Framework Programme, adopts a unique approach designed to cover all relevant trust aspects of a software development and operation life cycle. The project has developed a unified cross-disciplinary model of trust and trustworthiness, which is used to represent and quantify the trust of all stakeholders and the trustworthiness of socio-technical systems.

The multidisciplinary project team, consisting of social scientists, economists, legal experts and computer scientists, has been motivated by the eroding nature of trust in the Internet and in Internet-based applications to work on a European level and deliver research strength results, through both methods and tools to reverse this erosion and substantially increase the trust and confidence in future internet systems, applications and services. The work identifies processes to manage the trustworthiness of these systems with respect to user concerns, and develops technologies to facilitate evidence-based trustworthiness management.

OPTET plans to cover the whole life cycle of trustworthy ICT systems (from requirements right through to production, via the stages of implementation, validation and integration), with a multidisciplinary approach and by taking into account the drivers of stakeholders' trust. Thus, it defines its own engineering-based development approach, which describes different phases for the trust and trustworthiness attributes lifecycle in a custom software development methodology [1]. This OPTET lifecycle identifies additional activities to the typical development lifecycle processes and verifies that trust and trustworthiness are adequately addressed, both at design time, deployment time and runtime. The OPTET lifecycle evolves in the following phases.

The Design Phase involves the development of a Trustworthy by design process (TWbyD) in the form of a handbook, listing the potential capability patterns that can be used to follow a trustworthiness approach in the development of Future Internet applications. In this phase, OPTET envisions the depiction of the domain knowledge, in which experts in a specific socio-technical domain can introduce the trust and trustworthiness concepts and build a Design Time Trustworthiness Model (DTTM). The latter governs the interactions between system actors and their associated abstract assets in this specific domain of knowledge. Furthermore, the model is enriched with the corresponding threats that impact the trustworthiness of the involved system assets, and the respective controls for mitigating the risks related to these threats.

The Design Phase concludes with the calculation of the Trustworthiness Profile (TW profile), including the expected end-to-end trustworthiness value of the socio-technical system following a candidate topology of systems assets. This profile is based on metrics, describing the defined trustworthiness attributes of the model, and the end-to-end formation of the system workflow.

In the Development Phase, OPTET addresses the implementation and verification steps. It exploits the capability patterns, the DTTM and the available TW profiles of the Design Phase to drive the development of secure software for trustworthy socio-technical systems and applications. This phase includes static and dynamic verification steps for measuring trustworthiness evidences, based on the associated trust and trustworthiness attributes [2].

Figure 1: The Optet Lifecycle.

The Certification Phase defines a relevant certification process, which results in the Digital Trustworthiness Certification (DTWC), characterizing the system development under certification. This DTWC depicts the compilation of the trustworthiness attributes as they have been expressed in the Design Phase, and their compliance to the selected TW profile.

During the Distribution and Deployment Phase, the certified system is announced to a TW Software Marketplace, along with the DTWC and is ready to be instantiated for runtime use. At this point, a service provider can decide on the exact deployment configuration in the selected deployment plat-

form, according to the end-to-end trustworthiness of system asset compositions.

Finally, the Maintenance Phase uses the provisions of the DTWC to properly monitor the normal operation of the running trustworthy application and/or socio-technical system. Thus, this phase takes advantage of the dynamics of the execution environment to verify that provisions of the DTWC are met at runtime. When specific offerings of the DTWC are not adequately addressed, this phase activates trust and trustworthiness management procedures to derive alternative controls [3].

Future steps include the evaluation of the OPTET methodologies and enabling technologies by means of two business use-cases, namely Ambient Assisted Living (AAL) and Cyber Crisis Management (CCM). The evaluation approach will follow an iterative mode, which will allow initial models and prototype tools to be empirically evaluated and, if necessary, adjusted to the specific requirements of stakeholders' requirements, thus contributing to the success of the OPTET mechanisms.

Links:
http://www.optet.eu
http://www.fiware.org

References:
[1] S. Paulus, N. G. Mohammadi, T. Weyer: "Trustworthy software development", in Proc. of the 14th IFIP CMS 2013 Conference Berlin, Springer, pp. 233-247.
[2] Z. Zhioua, S. Short, Y. Roudier: "Static Code Analysis for Software Security Verification: Problems and Approaches", in Proc. of the 38th IEEE COMPSAC Workshop, 2014, pp.102-109.
[3] C. Kalogiros et al.: "Profit-maximizing trustworthiness level of composite systems", in Proc. of the 17th Conference HCI 2015, Los Angeles, USA.

Please contact:
Sebastien Keller
Thales Group, France
Tel: +33 1 69 41 60 16
E-mail:
sebastien.keller@thalesgroup.com

Five Major Reasons Why Safety and Security Haven't Married (Yet)

by Tiago Amorim, Daniel Schneider, Viet Yen Nguyen, Christoph Schmittner and Erwin Schoitsch

Cyber-Physical Systems (CPS) offer tremendous promise. Yet their breakthrough is stifled by deeply-rooted challenges to assuring their combined safety and security. We present five major reasons why established engineering approaches need to be rethought.

All relevant safety standards assume that a system's usage context is completely known and understood at development time. This assumption is no longer true for Cyber-Physical Systems (CPS). Their ability to dynamically integrate with third-party systems and to adapt themselves to changing environments as evolving systems of systems (CPSoS) is a headache for safety engineers in terms of greater unknowns and uncertainties. Also, a whole new dimension of security concerns arises as CPS are becoming increasingly open, meaning that their security vulnerabilities could be faults leading to life-endangering safety hazards.

Despite this, there are no established safety and security co-engineering methodologies (or even standardization). In fact, their respective research communities have traditionally evolved in a disjointed fashion owing to their different roots: namely embedded systems and information systems. With CPSoS, this separation can no longer be upheld. There are five major hurdles to a healthy safety-security co-engineering practice. The EMC² project investigates how these may be overcome.

Reconciliation points

Safety is commonly defined as the absence of unacceptable risks. These risks range from random hardware failures to systematic failures introduced during development. Security is the capacity of a system to withstand malicious attacks. These are intentional attempts to make the system behave in a way that it is not supposed to. Both safety and security contribute to the system's dependability, each in its own way. The following issues, in particular, are intrinsically in conflict:

1. *Assumed User Intention:* Safety deals with natural errors and mishaps, while security deals with malice from people (i.e., attacks). Thus, safety is able to include the user in its protection concept, whereas security distrusts the user.
2. *Quantifying Risks:* Safety practices utilize hazard probability when defining the acceptable risk and required safety integrity level of a system function. In security, measuring the likelihood of an attack attempt on a system in a meaningful way is impossible. Error and mishaps can, to a certain degree, be quantified statistically, whereas it is unfeasible to estimate the occurrence of an attack. An attacker's motivation may change over time.
3. *Protection Effort:* Safety is always non-negotiable. Once an unacceptable risk has been identified, it must be reduced to an acceptable level, and the reduction must be made evident based on a comprehensive and convincing argument. Security, in contrast, is traditionally a trade-off decision. Specifically in the information systems domain, where a security issue is associated with a monetary loss (in some form), the decision about how much effort to

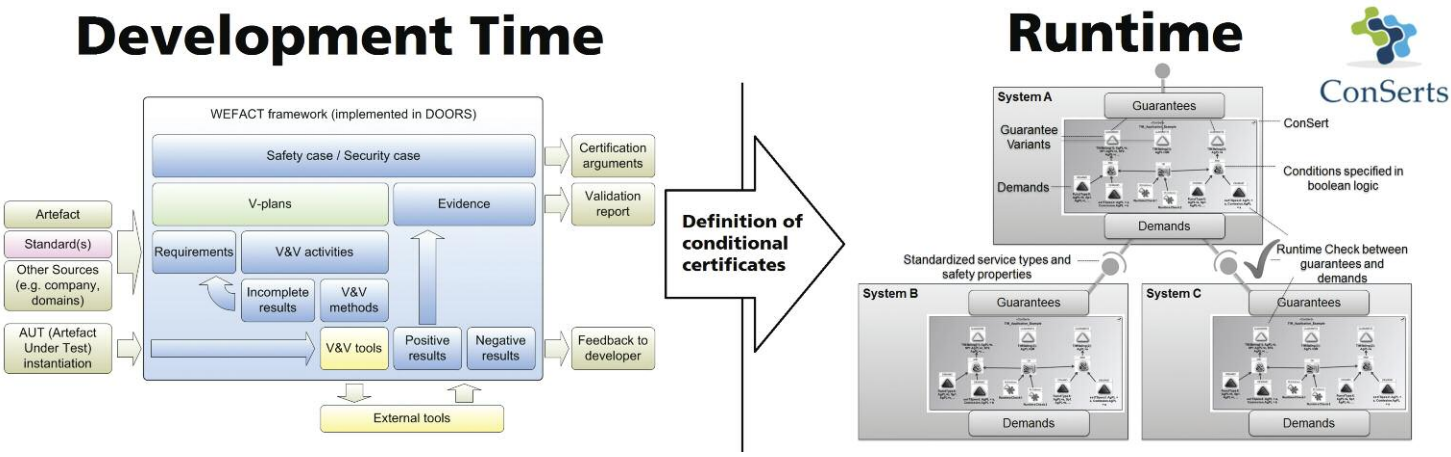


Figure 1: WEFACT addresses safety and security co-engineering at development time and ConSerts addresses CPS certification at Runtime. Both come together in the EMC² project.

invest into protection is largely a business decision.

4. *Temporal Protection Aspects:* Safety is a constant characteristic of a static system which, ideally, is never changed once deployed. Security requires constant vigilance through updates to fix newly discovered vulnerabilities or improve mechanisms (e.g. strengthening a cryptographic key). Security depreciates as a result of increases in computational power, development of attack techniques, and detection of vulnerabilities. This is such a huge issue that a system might require a security update the day after it goes into production. Consequently, effort for ensuring safety is mainly concentrated in the design and development phases. In the case of security, the effort is divided among design, development, and operations and maintenance, the latter requiring higher effort.

5. *COTS:* Safety-critical systems benefit from COTS. In such widely used and tested components, design flaws and failure probabilities are known. In terms of security, COTS can be detrimental since the design of these components is usually publicly available and found vulnerabilities can be exploited wherever the component is used.

EMC²: Safety and security co-Engineered

Current research performed in WP6 [1] of the project EMC² (ARTEMIS Joint Undertaking project under grant agreement n° 621429) aims to bridge the gap between safety and security assurance and certification of CPS-type systems. In EMC² we are looking at overlaps, similarities, and contradictions between safety and security certification, for example between the ISO 26262 safety case and the security target of ISO/IEC 15408 (Common Criteria). Both are aimed at assuring a certain level of trust in the safety or security of a system. Certain parts, such as the Hazard and Risk Analysis, which considers the effects in different driving situations, are relatively similar in intention to the security problem definition with its description of threats.

In addition, there is also some overlap between a security target for which part of the security concept depends on security in the operational environment, and a safety element out of context where the final safety assessment depends on the evaluation of assumptions about the system context. As one of the most prominent traits of CPS is their ability to integrate dynamically, EMC² also strives to develop corresponding runtime assurance methodologies. Formalized modular conditional certificates can be composed and evaluated dynamically at the point of integration to determine valid safety and security guarantees of the emerging system composition.

This work has been partially funded by the European Union (ARTEMIS JU and ECSEL JU) under contract EMC² (GA n° 621429) and the partners' national programmes/funding authorities.

References:

[1] D Schneider, E Armengaud, E Schoitsch, "Towards Trust Assurance and Certification in Cyber-Physical Systems", In Proc. of Workshop on Dependable Embedded and Cyber-physical Systems and Systems-of-Systems (DECSoS'14) - Computer Safety, Reliability, and Security, SPRINGER LNCS 8696, Springer International Publishing, pp. 180-191, 2014, ISBN 978-3-319-10556-7.

Please contact:

Tiago Amorim, Viet Yen Nguyen, Daniel Schneider
Fraunhofer IESE, Germany
Tel: +49 631 6800 3917
Email:
Tiago.Amorim@iese.fraunhofer.de,
VietYen.Nguyen@iese.fraunhofer.de,
Daniel.Schneider@iese.fraunhofer.de

Christoph Schmittner, Erwin Schoitsch
Austrian Institute of Technology, Austria
E-mail:
Christoph.Schmittner.fl@ait.ac.at,
Erwin.Schoitsch@ait.ac.at

CyPhySec: Defending Cyber-Physical Systems

by Johanna Ullrich and Edgar Weippl

The CyPhySec project (Framework to Cyber-Physical System Security) is embedding security in safety control for protecting Cyber-Physical Systems in the presence of adversarial behaviour.

CyPhySec addresses security threats to physical infrastructure operated by information technology (IT), such as water treatment or power plants. Although security incidents of this kind date back as far as the 1980s, attacks on cyber-physical systems (CPS) have been more frequent since the early 2000s [1]. Common targets include transport systems, power and utilities. The metal working industry has also been under attack: last year a steel mill in Germany was compromised when attackers gained access to the relevant networks by means of spear phishing, and ultimately sabotaged physical components of the plant [2]. Also in 2014, numerous European and U.S. energy companies were victims of a hacking group known as 'Dragonfly'; although the methods were similar (e-mail attacks, malware), cyberespionage seems to have been the main goal [3] – however, in cyber-physical systems it's just a small step from data theft to damaging physical components or whole infrastructures. Therefore, CPS must be protected as comprehensively as possible.

IT is a fast-evolving field in which new vulnerabilities are constantly emerging. Currently, the most common approach to cyber-security is to reuse existing IT solutions, such as: access control, patching, firewalls and encryption; which mainly defend against known attack vectors. The physical component of a cyber-physical system is not necessarily taken into account by these countermeasures, and so, in the absence of further protection, remains vulnerable. Even without this additional challenge, it can be difficult for system operators to keep up with innovations and hazards, and given the complexity and size of cyber-physical systems, this security issue should be addressed urgently. In addition, the possibility of attacks exploiting the dynamic of a system's physical parts must be considered.

CyPhySec faces the challenge of combining the two diverging points of view of control engineers and computer scientists. The former can predict a system's reaction to an event, while the latter are able to analyse such events in terms of their security issues. Consequently, CyPhySec aims to develop a multidisciplinary and consistent framework, which focuses on the impact that sophisticated attacks may have on a system's physical components. We have three specific goals:

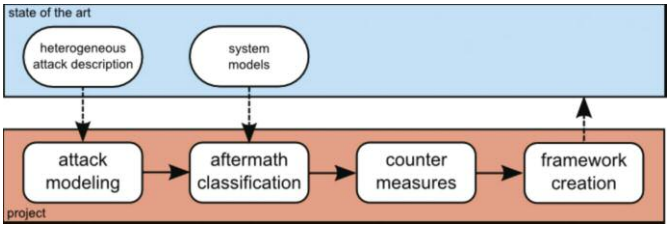


Figure 1: Methodology of the CyPhySec project.

1. *Attack Modelling:* This topic has not been comprehensively addressed, and a mutual and consistent method for describing attacks and their aftermaths is still lacking. We aim to bring together the respective fields and systematically determine probable consequences of cyber-launched attacks on physical systems.

2. *Countermeasures:* Current measures for the protection of cyber-physical systems consist either of IT security solutions or of traditional control engineering approaches. We aim to acquire an in-depth understanding of existing countermeasures and include new alternatives that might enable cyber-physical system protection. Such alternatives go beyond traditional IT protection, and aim at integrating defences within the control algorithms themselves towards protecting the CPS from adversarial behaviour that exploits IT weaknesses.

3. *Consistent notation:* Since this is a multidisciplinary project, the documentation has to be understandable by all parties involved to preserve the gained insights and to accelerate their spread within the related fields. Therefore, we are developing a consistent notation, including mathematical, textual and graphical explanations.

The CyPhySec project has been running since January 2014 and is funded by the BRIDGE Early Stage program (a funding scheme of the FFG, the Austrian Research Promotion Agency). The project is carried out by SBA Research in collaboration with Theobroma Systems, both located in Vienna, Austria.

Currently a group of four researchers – electrical engineers and computer scientists – is working on this project and has created a sophisticated collection of software, hardware and mathematical attacks that can be launched against cyber-physical systems; work on a multidisciplinary description of these attacks is also in progress.

Links:
https://www.sba-research.org/research/projects/cyphysec/
https://www.sba-research.org/
https://www.theobroma-systems.com/

References:
[1] RISI – The Repository of Industrial Security Incidents, http://www.risidata.com/Database/event_date/desc
[2] R.M. Lee, M.J. Assante, T. Conway: "SANS ICS Defense Use Case (DUC) Dec 30, 2014: ICS CP/PE case study paper – German Steel Mill Cyber Attack", https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf
[3] J. Langill, E. Zambon, D. Trivellato: "Cyberespionage campaign hits energy companies", available at http://www.secmatters.com/sites/www.secmatters.com/files/documents/whitepaper_havex_US.pdf

Please contact:
Johanna Ullrich, SBA Research, Austria
E-mail: jullrich@sba-research.org

Combining Safety and Security Engineering for Trustworthy Cyber-Physical Systems

by Christoph Schmittner, Zhendong Ma and Thomas Gruber

Networked cyber-physical systems introduce new challenges for safety, security, and dependability of such systems. Addressing them requires unified approaches towards safety and security co-analysis, design, implementation and verification in a holistic way. The researchers and engineers at the Austrian Institute of Technology develop concepts, techniques and tools for combining safety and security engineering for different domains.

Interconnected embedded systems integrated into the physical surroundings are known as Cyber-physical Systems (CPS). CPS are the driving force for many technological innovations to improve efficiency, functionality, and reliability of products, services, and infrastructures. Consequently, our society is becoming dependent on these 'intelligent' or 'smart' systems; from smart home appliance to industrial control, smart city, and intelligent transport. Owing to the scale, complexity, and connectivity of these systems, it is very challenging to ensure their safety, security, and resilience. Faults and malfunctions as well as malicious attacks can cripple a system and lead to devastating consequences in the physical world, eliminating all the advantages technology brings. Since system features increasingly depend on computation, network, and information processing, safety and security become tightly coupled in CPS. Safety cannot be guaranteed without security, and security is only as long as system safety holds. Many CPS are open systems, which are the target of cyberattacks. Interconnectivity removes boundaries and the need for physical presence to gain access. Complexity and time-to-market lead to the introduction of vulnerabilities and flaws and new ways of failure that can be very hard to analyse and cannot be easily addressed in development.

In the past, safety and security were treated as separate issues. Different methodologies, techniques, processes, certifications, and standards exist for system safety and security. Technological development and the challenges facing CPS require a combined approach. In a continuous effort with its partners, the Austrian Institute of Technology (AIT) has conducted research on safety and security co-engineering in the context of a series of EU projects including ARROWHEAD, EMC², and CARONTE in domains such as connected industrial systems, automotive, railway, and land transport. The research includes safety and security co-analysis, co-design, verification and validation, and certification.

One outcome of this research, 'Failure Mode, Vulnerabilities and Effect Analysis' (FMVEA) [1], is a combined analysis of failures and attacks and their effects on system dependability. The method has been applied to interconnected industrial, automotive [2] and railway systems. A system is divided into subsystems and parts. Potential failure and threat modes for each part are identified, and the consequences on a local and system level are determined. Through a semi-quantitative approach, the likelihood for the threat modes is determined. Results are safety motivated security goals and an improved coordination between safety and security goals.

To include safety and security considerations and to coordinate their interactions at each phase of the development lifecycle, a combined development lifecycle is proposed [3]. Based on lifecycle models in existing standards and best practices, the approach is a unified lifecycle with a balanced set of measures for mitigating both safety and security risks during development. In the requirement specification, security effects to ensure safety are considered during the Hazard, Risks and Threat analysis. At the beginning of the design phase, a consolidation is made for the definition of safety and security goals. In the development phase, safety and security measures are considered to fulfil the design goals. For example, the design can use tamper-resistant hardware for robustness against environmental influences. In the implementation/realization phase, safety coding standards that restrict the usage of dynamic elements can reduce the number of buffer overflow exploits. Safety and security development should be a continuous

Figure 1:Connected critical systems.

process beyond the release. As a part of the incident response, new vulnerabilities require the re-consideration of the safety and security concept and an impact analysis on other system quality attributes. Besides maintaining the necessary safety levels during a decommission process, one needs also to consider if potential attackers can gain insight about potential vulnerabilities from the disposed system.

To deepen the impact of our research results, AIT is actively involved in standardization activities to foster safety and security co-engineering and to promote joint approaches in the evolving editions of IEC 61508 and ISO 26262. AIT is a member of the recently founded ad hoc group 1 of IEC TC65 on "Framework towards coordination of safety and security". AIT is also a member of IEC TC65 WG 10 and the national counterpart, which works jointly with ISA 99 to develop IEC 62443 "Industrial communication networks - Network and system security - Security for industrial automation and control systems", a standard as a reference for cybersecurity in industrial systems and several other functional safety standards.

Links:
http://www.ait.ac.at/departments/digital-safety-security/?L=1
http://www.arrowhead.eu/
http://www.emc2-project.eu/
http://www.caronte-project.eu/

References:
[1] C. Schmittner et al.: "Security application of failure mode and effect analysis (FMEA)," in Computer Safety, Reliability, and Security, Sep. 2014, Springer, pp. 310–325.
[2] C. Schmittner et al.: "A Case Study of FMVEA and CHASSIS as Safety and Security Co-Analysis Method for Automotive Cyber-physical Systems", in Proc. of 1st ACM Workshop on Cyber-Physical System Security, 2015, pp. 69-80.
[3] C. Schmittner, Z. Ma, E. Schoitsch: "Combined Safety and Security Development Lifecylce", in IEEE INDIN, July 2015, IEEE (to appear).

Please contact:
Christoph Schmitter, Ma Zhendong, Thomas Gruber, AIT, Austrian Institute of Technology, Austria
E-mail: ,
christoph.schmittner.fl@ait.ac.at,
zhendong.ma@ait.ac.at,
thomas.gruber@ait.ac.at

Trustworthy and High Assurance Cyber-Physical Systems – A Research Agenda

by Markus Tauber, Christian Wagner and Andreas Mauthe

In the frame of the European ARTEMIS (Advanced Research and Technology for Embedded Intelligence and System) Inno-vation Pilot Project "Arrowhead" we address safety and security analysis methods as a part of 'safety and security co-engineering'. This is being combined with other research activities in e.g. the FP7 Project SECCRIT (Secure Cloud Computing for Critical Infrastructure IT) in which we investigate how to assure security properties in complex (cloud based) systems which are derived from safety and security analysis results. The goal is to create a uniform point of view for Sys-tems-of-Systems high-level security properties and assurance.

The latest ICT trends (e.g. the Internet of Things (IoT), Industry version 4 or smart-*) will result in systems integrating sensors and embedded devices within one infrastructure collecting huge amounts of data. The amount of data generated is somewhat unpredictable, being dependent on factors such as environmental conditions and human behaviour patterns. Cloud based systems would seem a logical place to store and process this data. Since these systems are also used together with control utilities, they form part of the critical infrastructure, and trust is of utmost importance. To introduce trustworthiness into such systems, transparency through enhanced monitoring is a key factor. However, deciding what to monitor is very complex. Established audit approaches or methods for analysing safety and security of systems can be used as a basis. However, such approaches typically focus on safety in the peripheral domain (e.g. sensors) or on security in the backend (e.g. Cloud). Hence, combined approaches are required.

Today's ICT systems include IoT infrastructures such as smart grids, smart cities and smart buildings (including private households as well as public buildings such as schools), they are often composed of traditionally isolated systems, now forming part of smart systems-of-systems (SoS). They consist of environmental sensor networks or manufacturing devices. The amount of data and its complexity (i.e. interdependencies) depends on usage patterns - for instance, electricity usage in a specific segment of a power grid, or on environmental conditions when controlling heating in public buildings. Resources for processing and storing such data need to be scalable and flexible. Thus, the Clouds represent an enabling factor for such systems. Such systems span from the peripheral domain (with sensor networks and embedded devices with some potential fluctuation of constituent components) to scalable and flexible Cloud backends (in which constituent components are contributing resources on demand).

To accept such technologies, users must be able to understand how their data is being treated and how the system protects data and operates in a safe and secure manner. Transparency is of utmost importance to achieve trustworthiness. It is hard to decide which parameters to monitor and how to represent the monitoring information in an aggregated form.

To address these issues our research agenda is twofold. First, we investigate established audit, security and safety analysis methods to extract the relevant high level security properties. Safety analysis methods are typically used in the peripheral domain and security analysis methods in the backend. These need to be combined as 'safety and security co-engineering' to create a uniform point of view for SoS high-level security properties. This work is conducted in the Artemis project ARROWHEAD and contributed to the ARROWHEAD framework [1]. Second, we investigate how to represent aggregated information in our assurance approaches [2], in the FP7 project SECCRIT (Secure Cloud Computing for Critical Infrastructure IT).

A first publication [3] related to safety and security co-engineering presents an evaluation of the methods in isolation. For succeeding activities the security analysis an approach based on the ISO 27005 and ETSI TS 102 165-1 standards is used in recent work in ARROWHEAD. For the safety and reliability analysis the IEC 60812 standard is used. Both include an identification of unsatisfactory situations (threats and failure modes) and a method for identifying those with the highest risks. The system is modelled using a dataflow diagram for identifying threats and to motivate decisions when extracting failure modes from an existing catalogue. We have performed an applicability analysis on the resulting threats and failure modes to filter out the relevant ones. In the end the risks of the remaining threats and failure modes were evaluated in detail. The elicitation of threats was supported by a series of workshops and interviews. Results have been applied to current design of one of the project's pilots. So far we have conducted safety and security analysis individually, and will extend the range of methods. The next step will involve modelling the process and investigating how to describe results to conduct a combined analysis to develop safety and security co-engineering, the fundamentals of which will be contributed to the ARROWHEAD framework.

We have systematically modelled security metrics for Cloud systems to contribute to our assurance model (as introduced in [2]). I.e. ISO27002, defines 'high-level' security metrics such as strong passwords. This can be measured by checking if corresponding tools (e.g. PAM (see Link) are available in the constituent components. A catalogue of high level security metrics is being developed and corresponding tool-support will be provided.

Promising initial results have already been published, and form a basis of our research agenda. They will be extended in future projects (e.g. H2020 CREDENTIAL).

Link:
http://www.linux-pam.org/Linux-PAM-html/Linux-PAM_MWG.html
http://www.arrowhead.eu/
http://www.seccrit.eu

References:
[1] S. Plosz, M. Tauber, P. Varga: "Information Assurance System in the Arrowhead Project", ERCIM News No. 97, pp 29, April 2014.
[2] A. Hudic et al.: "Multi-layer and multi-tenant cloud assurance evaluation methodology, in International Conference on Cloud Computing Technology and Science (CloudCom-2014), 2014.
[3] S. Plósz et al.: "Security Vulnerabilities And Risks In Industrial Usage Of Wireless Communica-tion", ETFA 2014, September 2014.

Please contact:
Markus Tauber, AIT, Austrian Institute of Technology, Austria
E-mail: markus.tauber@ait.ac.at

Communication and Compatibility in Systems of Systems: Correctness-by-Construction

by Maurice ter Beek, Josep Carmona and Jetty Kleijn

Society is still trying to catch up with technology in the wake of the digital revolution of the last twenty years. Current systems need to be both heterogeneous and able to deal with enormous volumes of data coming from uncertain environments; consequently it is essential to be able to automatically assess the correctness of interactions. To guarantee that a system of systems, comprising a conglomerate of cooperating reactive components, can be trusted, and that the system as a whole behaves as intended, requires a thorough understanding of its communication behaviour. Once local interactions are identified, abstractions can support the identification of incompatibility of systems that should cooperate within a larger system.

In an increasingly smart, connected world in which digital communications outnumber all other forms of communication, it is important to understand the complex underlying interconnections in the numerous systems of systems that govern our daily life. This requires a deep understanding of all kinds of different communication and collaboration strategies (e.g. client-server, peer-to-peer and master-slave) used in embedded or multi-component systems and the risk of failures they entail (e.g. message loss and deadlocks can have severe repercussions on reliability, safety and security).

A project involving ISTI-CNR and Leiden University (the Netherlands) considers fundamental notions paramount for the development of correct-by-construction multi-component systems. Basic building blocks are reactive components that interact with each other via shared (external) actions; in-

ternal actions are never shared. External actions can be input or output to the components to which they belong. Components can be added in different phases of construction allowing for hierarchically composed systems of systems. To establish that components within a system or a system and its environment always interact correctly, a concept of compatibility is needed. Compatibility represents an aspect of successful communication behaviour, a necessary ingredient for the correctness of a distributed system. Compatibility failures detected in a system model may reveal important problems in the design of one or more of its components that must be repaired before implementation.

In [1] a definition is given for compatibility of two components that should engage in a dialogue free from message loss and deadlocks. Message loss occurs when one component sends a message that cannot be received as input by another component, whereas deadlock occurs when a component is indefinitely waiting for a message that never arrives. The aim of the ideas developed in [1] is to provide a formal framework for the synthesis of asynchronous circuits and embedded systems. There the approach is restricted to two components and a closed environment, i.e. all input (output) actions of one component are output (input) actions of the other component.

In [2] this approach is generalized to distributed systems which consist of several components, and within which communication and interaction may take place between more than two components at the same time (e.g. broadcasting). These multi-component systems are represented by team automata [3], originally introduced to model groupware systems. Team automata represent a useful model to specify intended behaviour and have been shown to form a suitable formal framework for lifting the concept of compatibility to a multi-component setting. They resemble the well-known I/O automata in their distinction between input (passive), output (active) and internal (private) actions, but an important difference is that team automata impose fewer a priori restrictions on the role of the actions and the interactions between the components [3]. In [2] emphasis is on team automata with interactions based on mandatory synchronized execution of common actions.

Together with the Universitat Politècnica de Catalunya (Barcelona, Spain) we plan to continue the approach of [2] by investigating other composition strategies and, in particular, focusing on how to handle compositions based on master-slave collaborations. In such collaborations, input (the slave) is driven by output (the master) under different assumptions ranging from slaves that cannot proceed on their own to masters that should always be followed by slaves. Thus we address questions such as "how is compatibility affected when slaves are added?" and "in what way does compatibility depend on the collaboration among slaves?" Practical solutions to these answers may have strong impacts in various fields, such as services computing and security.

Composition and modularity are common in modern system design. So compatibility checks considering varying strategies significantly aid the development of correct-by-construction multi-component systems. Hence the ideas in this project should serve the development of techniques supporting the design, analysis and verification of systems of systems.

References:

[1] J. Carmona and J. Cortadella: "Input/Output Compatibility of Reactive Systems", Formal Methods in Computer-Aided Design, LNCS 2517 (2002) 360-377

[2] J. Carmona and J. Kleijn: "Compatibility in a multi-component environment", Theoretical Computer Science 484 (2013) 1-15

[3] M.H. ter Beek and J. Kleijn: "Modularity for Teams of I/O Automata", Information Processing Letters 95, 5 (2005) 487-495

Please contact:

Maurice ter Beek
ISTI-CNR, Italy
E-mail: maurice.terbeek@isti.cnr.it

Safety Analysis for Systems-of-Systems

by Jakob Axelsson

The introduction of systems-of-systems (SoS) necessitates the revision of common practices for safety analysis. In the case of vehicle platooning, for instance, this means that an analysis has to be carried out at the platoon level to identify principles for the safety of the SoS, and these principles then have to be translated to safety goals and requirements on the individual trucks.

The term systems-of-systems (SoS) started to become relevant some 20 years ago, and accelerated as a research area around 10 years ago. Although some people tend to take SoS as a synonym for large and complex systems, the research community has arrived at a fairly precise characterization of the term: in an SoS, the elements, or constituent systems, exhibit an operational and managerial independence, meaning that they can operate outside the SoS context, and have different owners. They choose to collaborate in order to achieve a common goal, manifested as an emergent property of the SoS, i.e. a property that does not exist in any of its parts in isolation. A recent literature review [1] shows that the field, so far, has been dominated by US researchers focusing on military and space applications. Key topics include: architecture, communications, interoperability, modelling and simulation, and also a number of properties where dependability attributes, such as safety, play an important role.

From its origins in the government driven sectors, SoS are now spreading

Photo: Scania

Figure 1: In the case of truck platooning, an analysis has to be carried out at the platoon level to identify principles for the safety of the SoS, and then these principles have to be translated to safety goals and requirements on the individual trucks.

to civilian and commercial usage. One example of this is the current efforts in vehicle platooning (see Figure 1), where a lead truck is followed by a number of other trucks that are driven more or less autonomously at a very short distance between each other. The trucks communicate using short-range radio to synchronize their movements to keep the right distance.

The motivator for platooning is primarily to improve fuel consumption by reducing aerodynamic drag, which is good both for the economy of the truck operator and for the environment. However, due to the automation and the short distances between the trucks, safety becomes an issue. Clearly, the platoon is an SoS, since each truck can also operate outside the platoon, and the trucks have different producers and owners.

The automotive industry has a long tradition in improving safety, and the best practices have recently been standardized as ISO 26262. In this standard, hazards are classified at different safety integrity levels based on the associated risk, and this classification is then used to derive requirements on components and on the product life-cycle processes. The focus in applying the standard is for a vehicle manufacturer to ensure that their product is safe to use.

However, when the product is to become a part of an SoS, carrying out the safety analysis on the product alone is not sufficient. As stated in [2], safety is an emergent property that has to be dealt with at the level of the SoS. In the case of the vehicle platoon, this means that an analysis has to be carried out at the platoon level to identify principles for the safety of the SoS, and then these principles have to be translated to safety goals and requirements on the individual trucks.

The challenge in this lies in the SoS characteristics of operational and managerial independence. Since no one owns the platoon, all safety requirements have to be agreed upon by potential participants, who must then take measures to implement these requirements in their products while making the best trade-offs with other requirements on the individual trucks not related to their use in the platooning SoS.

At SICS, we are investigating suitable safety analysis techniques for SoS. The first application is platooning, in co-operation with the Swedish truck industry. The approach is based on systems thinking, applied to safety as described in [3]. In the process, appropriate feedback loops are identified to devise a safety scheme based on constraining the behaviour of the constituent systems, i.e. the trucks in the platoon. In this process, additional requirements on the technical implementation can be identified, including new sensors and added communication between the constituent systems. The result is a set of safety goals and requirements on each constituent system, which can then be implemented using ISO 26262 and other standard procedures.

References:

[1] J. Axelsson: "A systematic mapping of the research literature on system-of-systems engineering", in Proc. of IEEE Intl. Conf. on Systems-of-Systems Engineering, 2015.
[2] N. Leveson: "The drawbacks in using the term 'system of systems'", Biomedical Instrumentation & Technology, March/April 2013.
[3] N. Leveson: "Engineering a safer world", MIT Press, 2012.

Please contact:

Jakob Axelsson
SICS Swedish ICT
Tel: +46 72 734 29 52
E-mail: jakob.axelsson@sics.se

Open, Autonomous Digital Ecosystems – How to Create and Evolve Trustworthy Systems of Systems?

by John Krogstie, Dirk Ahlers and Bjarne Helvik

Digital ecosystems encompass both ICT services and digital infrastructures, and their interactions with their surroundings. Prime challenges in such systems are the lack of coordinated engineering and management which, if not properly handled, can threaten the trustworthiness of the overall system. A holistic view of services and infrastructures is required, focusing on the relationships and dependencies between communication networks, data storage, service provisioning, and management of services and infrastructure.

New ICT-solutions are not created from scratch, but are based on building upon a large number of existing and evolving systems and services – 'systems of systems'. Since the sub-systems are not under any centralized control and exhibit emergent features, the term 'digital ecosystems' was proposed to describe such systems. Digital ecosystem is a metaphor inspired by natural ecosystems to describe a distributed, adaptive, and open socio-technical system. A wide range of individuals and organizations use and provide data, content and services to the digital ecosystem, as shown in Figure 1. Such systems are ideally characterized by self-organization, autono-mous subsystems, continuous evolution, scalability and sustainability, aiming to provide both economic and social value. On the other hand, as these systems grow organically, it also opens them up for a number of threats to the overall dependability and thus trustworthiness of the system.

There are three partly related variants of digital ecosystems: software ecosystems, data-oriented ecosystems, and infrastructure ecosystems.

Software ecosystems are "a set of businesses functioning as a unit and interacting with a shared market for software and services, together with relationships among them. These relationships are frequently underpinned by a common technological platform and operate through the exchange of information, resources, and artifacts" [2]. For instance, within open source systems (OSS), hundreds of thousands of co-evolved software 'components' are freely available. Their quality and documentation is rather variable. Yet, OSS components are integrated into many applications, and some also contribute back [1]. Traditional customers – such as municipalities – cooperate to provide improved e-services for their inhabitants. And end-users, even children, are becoming developers of components for the potential use of others.

Data-oriented ecosystems: In recent years, an increasing amount of data and meta-data has been made available for common use, representing the basis for an ecosystem of services being developed based on the shared online data. Of particular interest is the explosion of linked open data that makes it possible to access, interpret, and share heterogeneous and dynamically changing data across the Web with limited knowledge of how the data was produced. Since applications don't need to have any ownership to this data or to have access to an appropriate infrastructure for local management of large-scale data, the provision of linked open data enables a new breed of data-driven applications which are more cost-effective to develop and can combine data in new and innovative ways. Moreover, anyone can contribute to the total data model by publishing their own definitions, making sure that the data model is dynamically adapted and is relevant for outside use. It is in the nature of such data to be both heterogeneous and distributed. This creates new challenges, as this data often cannot be transferred owing to volume or legal constraints.

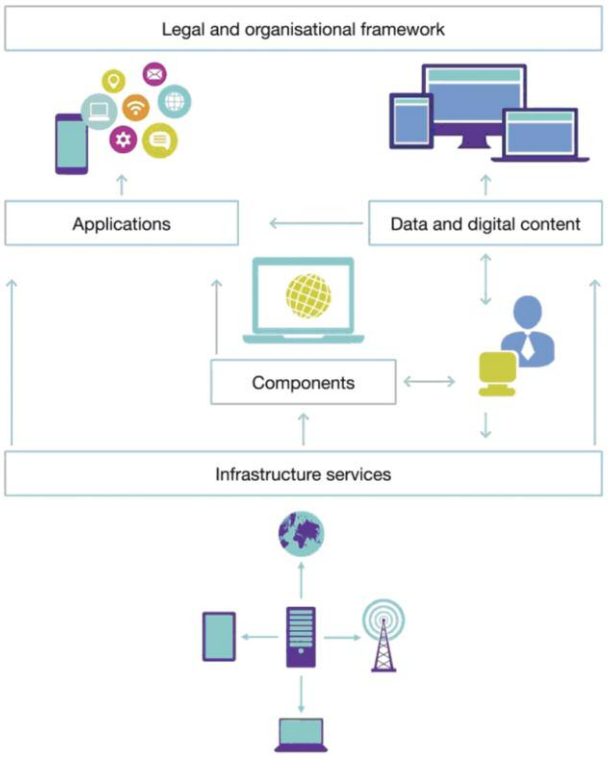


Figure 1: Types of actors and interactions in digital ecosystems.

A variant of data-oriented ecosystems are content ecosystems - networks that deal with creation and sharing of artistic or intellectual artifacts. The Web allows for highly visual and multimodal inter-

actions, and these interactions will become represented through richer means.

The third eco-system, and critical with respect to trustworthiness, is the *ICT infrastructure ecosystem*. It consists of a huge number of interconnected networks, computing and storage facilities, owned and operated by a number of autonomous market actors [3]. In addition, it has infrastructure services, such as positioning, and infrastructure information, such as maps, that a range of end user services rely on. The organization of these systems is mostly based on bilateral commercial agreements between market actors, and hence, it is a techno-economic eco-system rather than an engineered system. There may be regulations that put requirements on these systems and their interworking, but these are of a general kind.

In summary, there is no entity that has a global view of how this system of systems is organized and has an ability to deal with events 'across systems' that may threaten the ecosystem's role as the critical infrastructure our modern societies to an increasing degree rely on. It is a research challenge to understand the behaviour of this eco-system and to develop technology that ensures robustness to random failures, attacks, mistakes, natural disasters, etc. as well as combinations of these threats.

To address the trustworthy application of combined digital content, software and infrastructure ecosystems, there must be substantial and concerted improvements of the state-of-the-art in five traditionally unrelated and partially isolated research areas:

1. Open innovation
2. Software engineering
3. Enterprise architecture and enterprise modelling
4. (Big) Data management
5. Quantitative modelling of ICT infrastructure.

In complex digital ecosystems, such as those underlying Smart Cities or Smart Grids, aspects from all of these areas interplay, and to understand how to design, implement, manage, and operate trustworthy systems on top of the digital ecosystem, we need to be able to look at the different aspects in concert. How can we exploit the innovative opportunities arising by the digital ecosystems, whilst maintaining the overall trustworthiness and resilience of the total system? OADE – Open, Autonomous Digital Ecosystems, is a research program at NTNU, coordinating resources from computer science, information systems, telecommunications, and power engineering to address this versatile problem. We are looking at these issues from an interdisciplinary perspective to develop cross-cutting reliable solutions suited to flexible and autonomous digital ecosystems.

Link:
http://www.ntnu.edu/ime/oade

References:
[1] Ø. Hauge, C. Ayala, R. Conradi: "Adoption of Open Source Software in Software-Intensive Industry - A Systematic Literature Review", Information and Software Technology, 52(11):1133-1154, 2010.
[2] S. Jansen, A. Finkelstein, S. Brinkkemper: "A sense of community: A research agenda for software ecosystems", ICSE 2009, New and Emerging Research Track - Companion Volume, 2009.
[3] A. F. v. Veenstra et al.: "Infrastructures for public service delivery: Complexities of governance and architecture in service infrastructure development, e-services Journal, 2012.

Please contact:
John Krogstie, NTNU, Norway
Tel: +47 93417551
E-mail: krogstie@idi.ntnu.no

Formal Architecture Description of Trustworthy Systems-of-Systems with SosADL

by Flavio Oquendo and Axel Legay

Over the last 20 years, considerable research effort has been put into conceiving Architecture Description Languages (ADLs), resulting in the definition of different languages for formal modelling of static and dynamic architectures of single systems. However, none of these ADLs has the expressive power to describe the architecture of a trustworthy System-of-Systems (SoS). SosADL is a novel ADL specifically conceived for describing the architecture of Software-intensive SoSs. It provides a formal language that copes with the challenging requirements of this emergent class of complex systems that is increasingly shaping the future of our software-reliant world.

The importance of developing sound languages and technologies for architecting SoSs is highlighted in several roadmaps targeting year 2020 and beyond, e.g. ROAD2SoS and T-Area-SoS. They show the importance of progressing from the current situation, where SoSs are basically developed in ad-hoc ways, to a rigorous approach for mastering the complexity of Software-intensive SoSs. Complexity is inevitable in SoSs since missions in SoSs are achieved through emergent behaviour drawn from the interaction among constituent systems. Hence, complexity poses the need for separation of concerns between architecture and engineering: (i) architecture focuses on reasoning about interactions of parts and their emergent properties; (ii) engineering focuses on designing and constructing such parts and integrating them as architected.

A key facet of the design of any software-intensive system or system-of-systems is its architecture, i.e. its fundamental organization embodied in the components, their relationships to each other, and to the environment, and the principles guiding its design and evolu-

tion, as defined by the ISO/IEC/IEEE Standard 42010 [1].

Therefore, the research challenge raised by SoSs is fundamentally architectural: it is about how to organize the interactions among the constituent systems to enable the emergence of SoS-wide behaviours/properties derived from local behaviours/properties (by acting only on their interconnections, without being able to act in the constituent systems themselves).

Trustworthiness is thereby a global property directly impacted by emergent behaviours - which may be faulty, resulting in threats to safety or cyber-security.

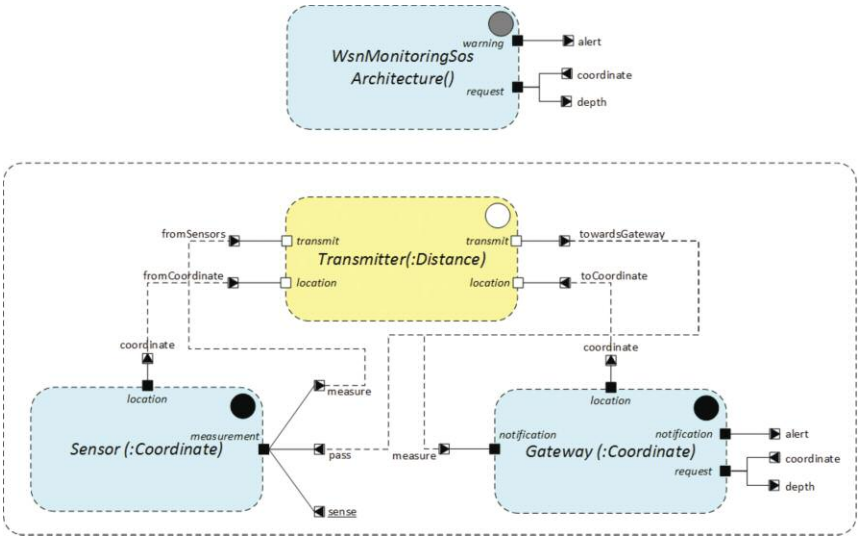


Figure 1: Abstract architecture of a flood monitoring SoS.

Various recent projects have addressed this challenge by formulating and formalizing the architecture of software-intensive SoSs. A systematic literature review revealed that 75% of all publications addressing the architecture of software-intensive SoSs appeared in the last five years, and approximately 90% in the last 10 years. Much of the published research describes open issues after having experimented with existing systems approaches for architecting or engineering SoSs.

Actually, although different Architecture Description Languages (ADLs) have been defined for formally modelling the architecture of single systems, none has the expressive power to describe the architecture of software-intensive SoSs [2][3].

To fill this gap, we have defined SosADL, a novel ADL specifically conceived for formally describing the architecture of trustworthy software-intensive SoSs.

Formally defined in terms of the π-calculus with concurrent constraints, SosADL provides architectural concepts and notation for describing SoS architectures. The approach for the design of SosADL is to provide architectural constructs that are formally defined by a generalization of the π-calculus with mediated constraints. Both safety and cyber-security are addressed.

Using SosADL, an SoS is defined by coalitions that constitute temporary alliances for combined action among systems connected via mediators. The coalitions are dynamically formed to fulfil the SoS mission through emergent behaviours under safety and cyber-security properties. The SoS architecture is defined intentionally in abstract terms (Figure 1) and is opportunistically created in concrete terms (Figure 2).

A major impetus behind developing formal languages for SoS architecture description is that their formality renders them suitable to be manipulated by software tools. The usefulness of an ADL is thereby directly related to the kinds of tools it provides to support ar-

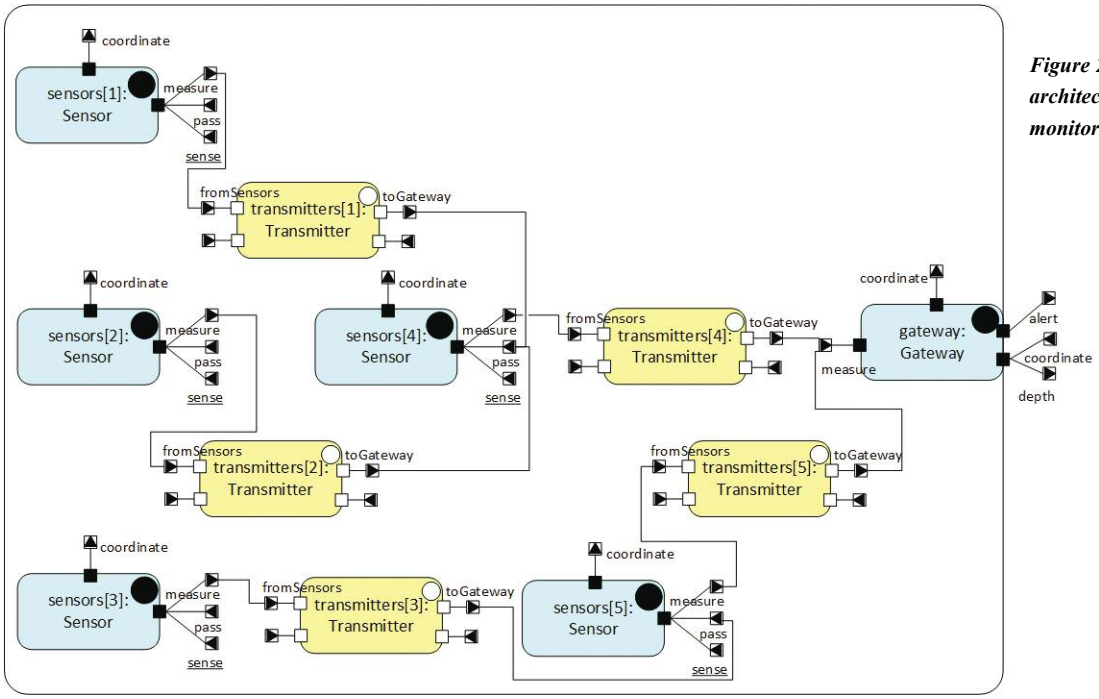


Figure 2: Concrete architecture of a flood monitoring SoS.

chitecture description, but also analysis and evolution, in particular in the case of SoSs.

We have developed an SoS architecture toolset for supporting architecture-centric formal development of SoSs using SosADL. This toolset, 'SoSmart', is constructed as plugins in Eclipse Luna. It provides a Model-Driven Architecture software environment where the SosADL meta-model is transformed to different meta-models and converted to input languages of external tools, of which we have selected: UPPAAL for model checking, PLASMA-Lab for statistical model checking, DEVS and FMI (Functional Mockup Interface)/FMU (Functional Mockup Unit) for simulation.

In our approach for co-engineering safety and cyber-security supported by SoSmart, we are extending techniques applied for safety analysis to address cyber-security evaluation. This promising approach tackles different open issues, largely due to fundamental differences between the accidental nature of the faults appearing in safety analysis, and the intentional, human nature of cyber-attacks.

SosADL, supported by its SoSmart toolset, has been applied in various case studies and pilot projects for architecting SoSs, including a pilot project of a real SoS for architecting a novel flood monitoring and emergency response SoS to be deployed in the Monjolinho River. This SoS is based on different kinds of constituent systems: sensor nodes (for measuring river level depth via pressure physical sensing), a gateway and base station (for analyzing variations of river level depths and warning inhabitants of the risk of flash flood), UAVs (Unmanned Aerial Vehicles for minimizing the problem of false-positives), and VANETs (Vehicular Ad-hoc Networks embedded in vehicles of rescuers). In addition to the deployment in the field, this SoS (via the gateway system) has access to web services providing weather forecasting used as input of the computation of the risk of flash flood.

In the context of this pilot project, the SosADL met the requirements for describing trustworthy SoS architectures. As expected, a key identified benefit of using SosADL was the ability, by its formal foundation, to validate and verify the studied SoS architectures very early in the SoS lifecycle with respect to trustworthiness, including analysis of uncertainties in the framework of safety and cyber-security.

Future work will address the application of SosADL in industrial-scale pilot projects, feeding back the research work on the ADL. This will include joint work with DCNS for applying SosADL to architect naval SoSs, and IBM in which SosADL will be used to architect smart-farms in cooperative settings.

Link: http://www-archware.irisa.fr/

References:

[1] ISO/IEC/IEEE 42010:2011: Systems and Software Engineering – Architecture Description, December 2011.
[2] I. Malavolta, et al.: "What Industry Needs from Architectural Languages: A Survey", IEEE Transactions on Software Engineering, vol. 39, no. 6, June 2013.
[3] M. Guessi, E.Y. Nakagawa, F. Oquendo: "A Systematic Literature Review on the Description of Software Architectures for Systems-of-Systems", 30th ACM Symposium on Applied Computing, April 2015.

Please contact:

Flavio Oquendo
IRISA (UMR CNRS, INRIA & Universities of Rennes and South-Brittany, France)
E-mail: flavio.oquendo@irisa.fr
http://people.irisa.fr/Flavio.Oquendo/

Axel Legay, INRIA and IRISA, France
E-mail: axel.legay@inria.fr
https://team.inria.fr/estasys/

Quantitative Modelling of Digital Ecosystems

by Tesfaye A. Zerihun, Bjarne E. Helvik, Poul E. Heegaard and John Krogstie

In a world where ICT systems are everywhere and are critical for the well being, productivity and in fact the survivability of our society, it is crucial that they are resilient to all kinds of undesired events, random failures, mistakes, incompetence, attacks, etc. To deal with this challenge, a thorough understanding of the nature of their complexity and inter-dependencies is needed. A quantitative model of a digital ecosystem can offer insights into how management and operations can be conducted within, and coordinated across the different autonomous domains that constitute the global, complex, digital ecosystems.

Interworking ICT systems have become critical infrastructure for society, and are a prerequisite for the operation of critical infrastructures – e.g. payment systems, electricity grids and transportation. The challenges posed by these highly interwoven infrastructures were addressed in the FutureICT initiative [1], [2]. Modern society depends on the robustness and survivability of ICT infrastructure; but to achieve these qualities, we must address several challenges posed by the evolution of this technology:

- The public ICT service provisioning infrastructure can viewed as an ecosystem; the result of cooperation between many market actors. The overall ecosystem is not engineered, and there is no aggregate insight into its design and operation.
- There is no coordinated management that may deal with issues involving several autonomous systems, in spite of such issues being a likely cause of extensive problems and outages.
- It is necessary to prepare for restoration of service after a major event such as common software breakdown, security attacks or natural disasters. This preparation must include technical, operational as well as organizational and societal aspects.

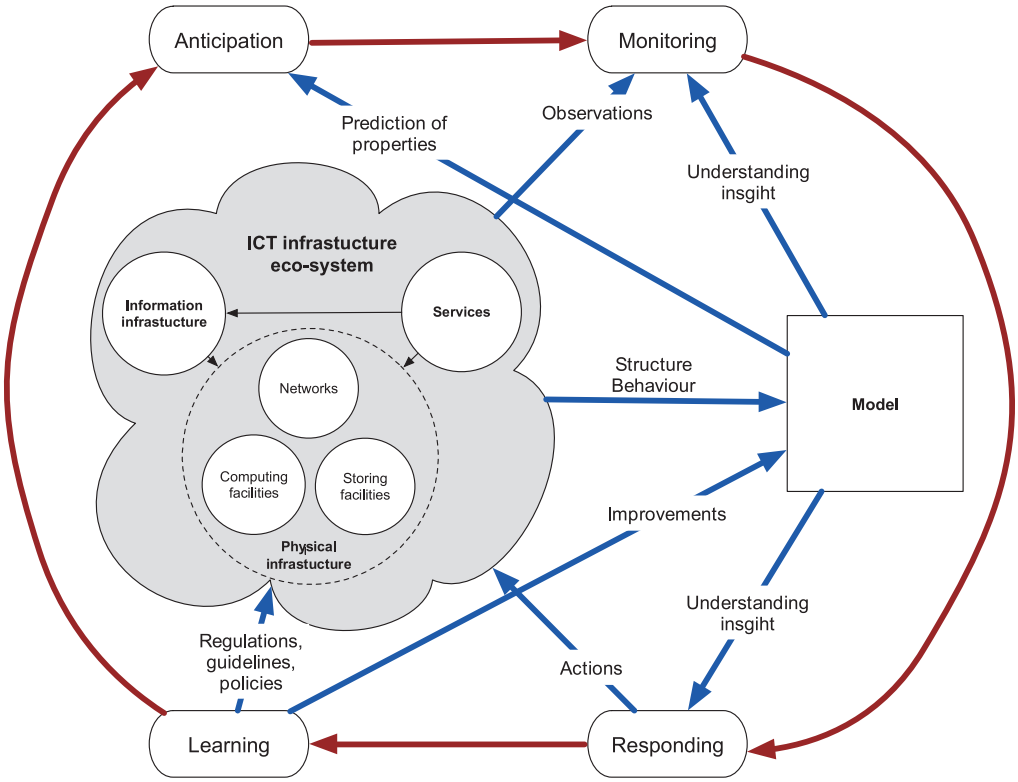


Figure 1: Conceptual sketch for a resilience engineering approach to improve ICT infrastructure robustness.

- There are currently no theoretical foundations to control the societal and per service dependability of this infrastructure, neither from a public regulatory position, nor from groups of autonomous (commercially) co-operating and partly competing providers.

The objective of the Quantitative Modelling of Digital Ecosystems project is to establish a quantitative model for a digital ecosystem. The model should form the basis for a resilience engineering oriented approach [3] to deal with robustness and survivability challenges in the ICT infrastructure.

The model of an ICT infrastructure must describe the structure and behaviour of the physical and logical information and network infrastructure, including the services provided. Through the modelling phases it should also describe how resilience engineering [3] can be applied to manage the robustness and survivability of the ICT infrastructure. The simplest resilience approach is simply to monitor the system's state and react to anomalies. This might work well when failure events are infrequent and the response to one event can be completed before the next occurs. The modelling should help us determine how to monitor and react to anomalies.

A more realistic approach is to have both reactive and proactive responses, and to learn from the experiences. Again the modelling should help achieve the insight and understanding necessary to define and take actions that will improve the resilience of the ICT system. The learning includes regulations, management guidelines, and policies, which will influence the properties of the system and therefore also refine the model. The last and very crucial step in resilience engineering is to anticipate known and unknown events so it is possible to be proactive as well as reactive. The predictions that can be learnt from the modelling provide very important input to the assessment of the risk of being too early; i.e. proactive measures that are considered to be a waste of time and money, in contrast to being too late, which implies that the events escalate with larger consequences and much higher cost of recovery than necessary. The holistic model of the ICT infrastructure and the resilience engineering applied to it, is illustrated in Figure 1.

This work is still at an early stage. Among the outcomes we aim to achieve are:

- A basis for a continuous monitoring, anomaly detection and handling, system improvement cycle, according to the Resilient Engineering approach.
- Better prediction of risks and vulnerabilities incurred by ICT services provided by a heterogeneous eco-system like infrastructure.
- A basis for setting guidelines for regulation by public authorities.

Links:

NTNU/IME: Open and Autonomous Digital Ecosystems (OADE): http://www.ntnu.edu/ime/oade

NTNU QUAM Lab: Quantitative modeling of dependability and performance: http://www.item.ntnu.no/research/quam

References:

[1] D. Helbing: "Globally networked risks and how to respond", Nature, 497(7447):51–59, 05 2013.

[2] S. Bishop: "FuturICT: A visionary project to explore and manage our future", ERCIM News, (87) p.14, October 2011.

[3] E. Hollnagel, D. D Woods, N. Leveson: "Resilience engineering: Concepts and precepts", Ashgate, 2006.

Please contact:

Bjarne E. Helvik
NTNU, Norway
E-mail: bjarne.helvik@item.ntnu.no

Workflow Engine for Analysis, Certification and Test of Safety and Security-Critical Systems

by Christoph Schmittner, Egbert Althammer and Thomas Gruber

Certification and Qualification are important steps for safety- and security-critical systems. In Cyber-Physical Systems (CPS), connected Systems of Systems (SoS) and Internet of Things (IoT), safety and security certification should be done in a holistic and unified way. Assurance that a system is safe needs to include evidence that the system is also secure. WEFACT is a workflow tool originally developed for guidance through the safety certification and testing process, which is now extended towards holistic safety and security assurance.

Mission-critical Cyber-Physical-Systems (CPS) often need to follow well-defined safety and qualification standards. Most safety standards demand explicitly or implicitly a safety case, which contains evidence and assurance that all safety risks have been appropriately identified and considered. To generate such a safety argumentation, requirements tracking and workflow support are important. The Workflow Engine for Analysis, Certification and Test (WEFACT) has been developed as a platform for safety certification and testing in the ARTEMIS/ECSEL projects SafeCer, MBAT and CRYSTAL. The final result of the WEFACT supported workflow is the safety case (Figure 1).

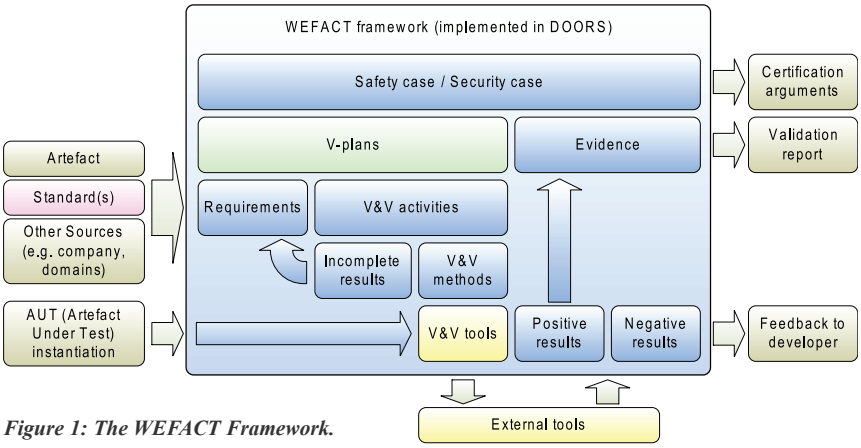


Figure 1: The WEFACT Framework.

WEFACT's requirements tracking, testing and certification support is based on a workflow derived from the requirements of functional safety standards, but other domain-specific requirements and company-specific practices can also be included. These requirements, together with functional and non-functional requirements defined for the individual application, are stored in a DOORS© database; 'V-plans' (validation plans) are defined for these requirements, and their successful execution proves that the requirements are fulfilled. Recently, WEFACT is being developed in the ARTEMIS/ECSEL project EMC² towards a framework for supporting a general assurance case covering all relevant dependability attributes, including safety, security and performance (see Figure 2).

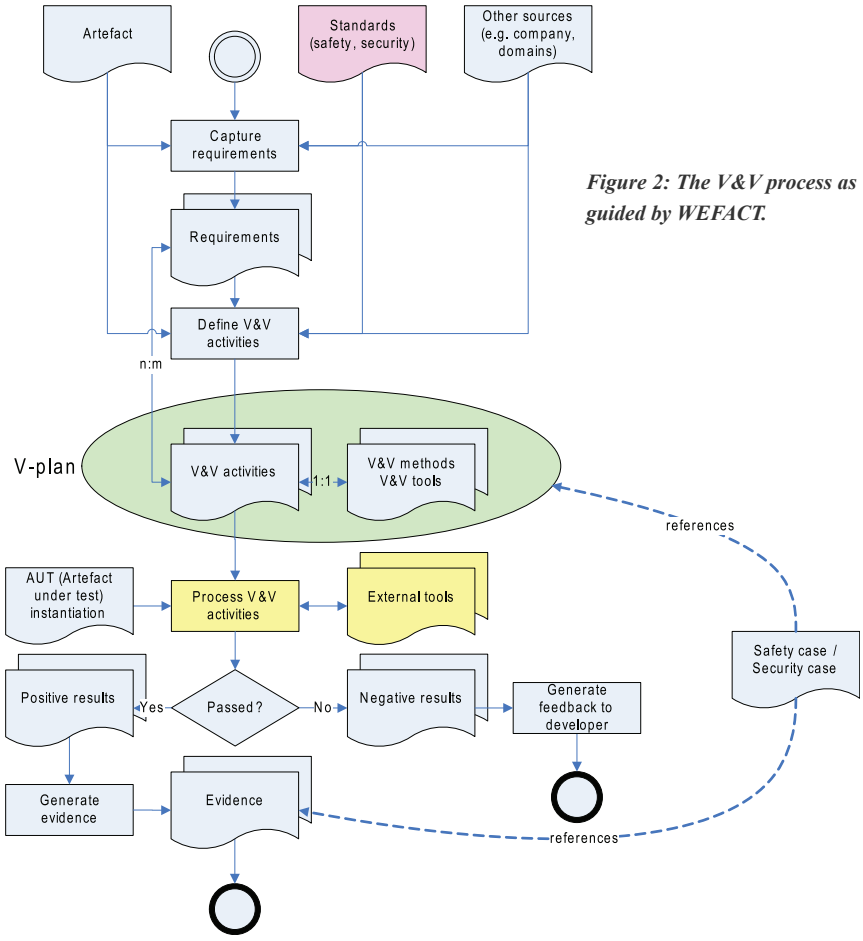


Figure 2: The V&V process as guided by WEFACT.

With increasingly interconnected and networked critical systems, a safety case needs to be aware of security risks because security threats have to be considered as a potential cause for hazards. A security aware safety case includes security assurance in order to demonstrate that a system is safe and

secure. The security assurance part of WEFACT is based on the ISO/IEC 15408 (Information technology - Security techniques - Evaluation criteria for IT security (Common Criteria)) and IEC 62443 (Industrial communication networks - Network and system security - Security for industrial automation and control systems). ISO/IEC 15408 defines Security Assurance Requirements (SAR) for different parts of the Artefact under test (AUT). A system is evaluated based on the assigned Evaluation Assurance Level (EAL), which describes a set of SAR. There are seven EAL with increasing requirements on formalism and thoroughness of the evaluation. The V-plan for the AUT describes the responsibilities and activities, based on safety and security standards as well as other sources such as domain-specific and company-specific practices. WEFACT guides the combined process of achieving certification according to safety and security standards. In addition, activities for verification and validation (V&V) are connected to external tools which can be integrated into the workflow engine. WEFACT supports automated tool integration over Open Services for Lifecycle Collaboration (OSLC), an interoperability standard for the cooperation of lifecycle management tools. Depending on the level of integration, i.e. whether the V&V tool can be called directly via OSLC or command line interface, or a V&V activity needs manual interaction with external tools, WEFACT will be able to conduct the V&V activity more or less automatically and change the requirement status according to the result (<pass> or <fail>). After all V&V activities of the V-plans are conducted successfully, and all requirements are therefore fulfilled, a holistic safety and security case is generated. This so called dependability or assurance case uses an argument notation - for instance, the Goal Structuring Notation (GSN) to demonstrate the assurance that a system is safe and secure.

This work was partially funded by the European Union (ARTEMIS JU and ECSEL JU) under contracts MBAT, nSafeCer, CRYSTAL, ARROWHEAD and EMC² and the partners' national programmes/ funding authorities.

Links:
http://www.ait.ac.at/wefact
http://open-services.net
http://www.goalstructuringnotation.info/
http://www.ecsel-ju.eu

References:
[1] J. Spriggs: "GSN-The Goal Structuring Notation: A Structured Approach to Presenting Arguments", Springer Science & Business Media, 2012.
[2] E. Althammer, et al.: "An Open System for Dependable System Validation and Verification Support – The DECOS Generic Test Bench", in Proc. of the INDIN 2007, Vienna, ISBN 1-4244-0864-4, p. 965 – 969.
[3] E. Schoitsch: "An E&T Use Case in a European project", special session TET-DEC (Teaching, Education and Training for Dependable Embedded and Cyber-physical Systems); in Proc. of SEAA 2015, IEEE CPS, to appear.

Please contact:
Egbert Althammer
AIT Austrian Institute of Technology GmbH
E-mail: egbert.althammer@ait.ac.at

Consequences of Increased Automation in Smart Grids

by Jonas Wäfler and Poul E. Heegaard

The increased use of information and communication technology in the future power grid can reduce the most frequent types of failure and minimize their impacts. However, the added complexity and tight integration of an automated power grid brings with it new failure sources and increased mutual dependencies between the systems, opening the possibility for more catastrophic failures.

The power grid plays a crucial role in modern society; the whole economy relies on a dependable power supply. In order to provide this, modern power grids rely heavily on information and communication technology (ICT) for monitoring and controlling. In the next few years, even more ICT devices and systems will be deployed in the power grid, making the system smarter and creating the 'smart grid' [1], which will allow a more precise monitoring of the system state and a finer granularity of control.

New systems and services like preventive failure detection and automated failure mitigation come with the aim to utilize the power grid more efficiently and increase the overall reliability. In theory, the automation of processes can reduce the frequency of failures and their severity. When implementing automation of power grids, the primary focus is usually on the most frequent types of failures; those that occur daily, weekly and monthly. A beneficial side effect of automation is a reduction of human effort needed in normal operation.

However, automation brings with it its own challenges. First, the new systems contain more sophisticated software and more configuration possibilities. This makes development, configuration, operation and maintenance more complex and error-prone [2]. Second, the power grid and its supporting ICT systems have mutual dependencies: the ICT systems depend on power supply and the power grid depends on information channels and systems for monitoring and controlling. Such systems are both more complex to analyze and manifest different failure patterns [3]. These failures may not happen in every day operation; they have a low frequency but potentially very serious consequences.

Figure 1 depicts the risk curve of a specific system, showing the consequences for incidents with different frequencies. Generally, a high frequency incident has low consequences, but a low frequency (rare) event may have catastrophic con-

sequences. The introduction of ICT focusses on reducing the consequences for high frequency incidents, as shown on the right side of the figure. Automation reduces human effort for these incidents because of a reduction in the number of incidents, and possibly also because of automatic restoration processes. However, there is also a change on the other end of the plot. In the absence of preventative measures, automation can lead to larger consequences in low frequency incidents.

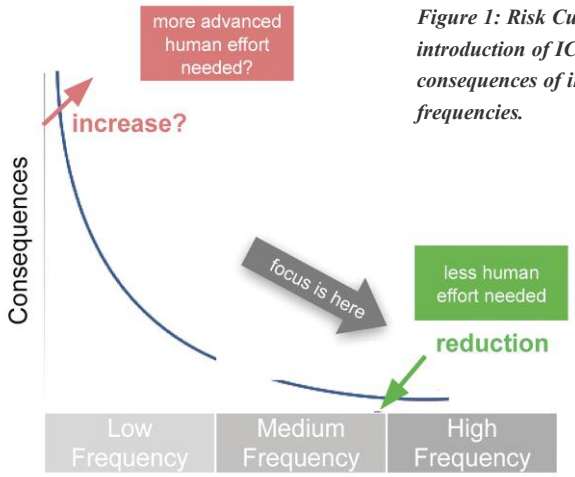


Figure 1: Risk Curve showing how the introduction of ICT may change the consequences of incidents, depending on their frequencies.

The introduction of ICT focusses on reducing the consequences for high frequency incidents, as shown on the right side of the figure. Automation reduces human effort for these incidents because of a reduction in the number of incidents, and possibly also because of automatic restoration processes. However, there is also a change on the other end of the plot. In the absence of preventative measures, automation can lead to larger consequences in low frequency incidents.

This can be illustrated through an example of the restoration process after a power grid failure. More monitoring and controlling devices allow a fast automatic detection and isolation of a failure. The devices also send diagnostics about the precise failure reason and location, which dramatically accelerates the restoration process. Automation reduces the human effort needed to monitor the system. It reduces the required skill set for the repair crews since the system gives more detailed information about its failure. Additionally, it might also reduce the number of repair crews, as the restoration times are shorter, and owing to better monitoring, a proactive maintenance scheme reduces the number of failures.

However, if the monitoring system fails, the restoration process has to be handled manually again. With a reduced and less skilled repair crew, the consequences of the same outage are bigger. And even more importantly, programming, configuration and operational failures, which are dominant in ICT systems, add additional failures and may lead to very unpredictable states of the system and are more difficult to locate and restore.

In summary, the introduction of automation may have unwanted effects for low frequency incidents. This can be circumvented by the following endeavors: first, by using the saved human effort in normal operation to cover less frequent incidents; second, by increasing the skill set for operational staff to cover new failures and rare events; third, by keeping the staff trained to a high standard and having efficient and well-established processes to deal with rare events.

References:
[1] International Energy Agency (IEA), "Technology roadmap: Smart grids," http://www.iea.org/publications/freepublications/publication/smartgrids_roadmap.pdf, 2011.
[2] P.Cholda et al.,"Towards risk-aware communications networking," Rel. Eng. & Sys. Safety, vol. 109, pp. 160–174, January 2013.
[3] S. Rinaldi et al., "Identifying, understanding, and analyzing critical infrastructure interdependencies," IEEE Control Systems, vol. 21, no. 6, pp. 11–25, Dec. 2001.

Please contact:
Jonas Wäfler, Poul E. Heegaard
NTNU, Norway
E-mail: jonas.waefler@item.ntnu.no, poul.heegaard@item.ntnu.no

Layered Thinking in Vertex Centric Computations

by Emanuele Carlini, Patrizio Dazzi, Alessandro Lulli and Laura Ricci

The Telos framework eases the transition to a vertex-centric approach in the high performance and distributed programming of BigData analytics targeting large graphs. Telos represents a paradigm shift, from 'think like a vertex' to 'think like a network'.

The recent proliferation of mobile devices and Internet usage has resulted in huge amounts of data. For instance, in 2012, 2.5 exabytes of data were created, every day. This data comes from many heterogeneous sources, including social networks, business transactions and diversified data collections. Industries and academics frequently model this data as graphs in order to derive useful information.

However, it is not always possible to process graphs of such large volumes of data on a single machine. Many different frameworks for large graph processing, mainly exploiting distributed systems, have been proposed in recent years to overcome this limitation.

In order to ease the distribution of the computation across many computers, the vast majority of the proposed solutions exploit a vertex-centric view of the

graph [1]. In this approach, the algorithms are implemented from the perspective of a vertex rather than a whole graph. Unfortunately, this shift in the perspective of programmers does not come free-of-charge. Two main issues are identified: performance and adoption.

Performance can be affected by the software design of the programming framework. Moving the viewpoint to a per-vertex perspective needs a careful design of the platform enabling data and computation distribution [2][3].

The second problem is that programmers may be reluctant to embrace a new paradigm because it will be necessary to adapt classic algorithms to a vertex-centric approach: most of the existing algorithms must be re-thought or even re-conceived. Solutions targeting this problem aim at providing new tools to help to construct new algorithms.

The Telos framework addresses the adoption issue. Underpinning this framework is the similarity between vertex-centric models and massively distributed systems, for instance P2P. Massively distributed systems commonly rely on a multi-layer overlay network. An overlay can be thought of as an alternative network, built upon the existing physical network, where logical links follow a defined goal. According to Telos, vertices of the graphs can be seen as nodes of the network and edges as links.

We have taken advantage of this similarity to develop three main strategies for large graph processing:

Local knowledge: algorithms for overlays are based on local knowledge. Each node maintains a limited amount of information and a limited neighbourhood. During computation, it relies only on its own data and the information received from its neighbourhood.

Multiple views: the definition of multi-layer overlays has been a successful trend. These approaches build a stack of overlays, each overlay is characterized by a ranking function that drives the node neighbourhood selection according to a specific goal.

Approximate solutions: since overlays are usually based on an approximated knowledge on the graph, algorithms running on them are conceived to deal with approximated data and to find approximated solutions.

Specifically, Telos provides high level API to define multiple overlay views. Telos has been developed on top of Apache Spark. Computation is organized by means of different views of the graph, called Protocol. Some of the most popular massively distributed systems algorithms have been implemented as built-in protocols within Telos. The main task requested to a protocol is to provide a compute function. This function takes as input the messages received by the vertex and the previous vertex state. The contract is to return a new vertex state and messages that must be dispatched to other vertices.

A relevant aspect of Telos is that not only the context of a vertex but also its neighbourhood can change. This functionality is a key part of the Telos framework because it lets users adapt the neighbourhood according to requirements and allows convergence to a graph topology targeted for the problem.

To exploit communication within the neighbourhood of each vertex, three different kinds of communication pattern occur within Telos: (i) intra-vertex to let a vertex access the state of all its layers, (ii) intra-protocol to let a vertex communicate to another vertex on the same layer, (iii) extra-protocol to request the state of another vertex in a protocol different from that operating.

The layered architecture of Telos is shown on the left in Figure 1. A different protocol is executed on each layer. Each vertex has a different state for every layer, as shown in the Telox vertex view on the right.

Telos has been used successfully to improve a state-of the-art algorithm for the balanced k-way problem and to dynamically adapt the vertices neighbourhood targeting specific problems, for instance, to find similar vertices or for leader election mechanisms.

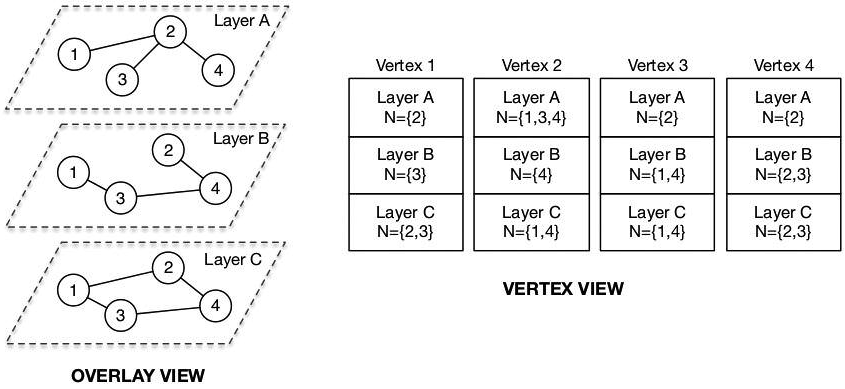


Figure 1: Layered architecture and interactions.

Links:
Telos API:
https://github.com/hpclab/telos

References:
[1] R. R. McCune, T. Weninger, G. Madey: "Thinking Like a Vertex: a Survey of Vertex-Centric Frameworks for Large-Scale Distributed Graph Processing."
[2] E. Carlini, et al.: "Balanced Graph Partitioning with Apache Spark, in Euro-Par 2014: Parallel Processing Workshops (pp. 129-140). Springer, 2014.
[3] A. Lulli, et al.: "Cracker: Crumbling Large Graphs Into Connected Components", 20th IEEE Symposium on Computers and Communication, ISCC2015.

Please contact:
Emanuele Carlini, Patrizio Dazzi
ISTI-CNR, Italy
E-mail: emanuele.carlini@isti.cnr.it, patrizio.dazzi@isti.cnr.it

Alessandro Lulli, Laura Ricci
University of Pisa, Italy
E-mail: lulli@di.unipi.it, ricci@di.unipi.it

Cross-functional Teams Needed for Managing Information Security Incidents in Complex Systems

by Maria Bartnes Line and Nils Brede Moe

Recent attacks and threat reports show that industrial control organizations are attractive targets for attacks. Emerging threats create the need for a well-established capacity for responding to unwanted incidents. Such a capacity is influenced by organizational, human, and technological factors. A response team needs to include personnel from different functional areas in the organization in order to perform effective and efficient incident response. Such a cross-functional team needs to be self-managing and develop a shared understanding of the team's knowledge.

We conducted a case study involving ten Distribution System Operators (DSOs) in the electric power industry in Norway. As they control parts of critical infrastructures, they need to be well prepared for responding to information security incidents, as consequences of such might be significant for the society. Our aim was to identify current incident management practices and pinpointing ways to improve them. We interviewed representatives from three different roles in the DSOs:

- IT manager
- IT security manager
- Manager of control room/power automation systems.

In addition, we observed preparedness exercises for IT security incidents as performed by three of the DSOs.

Current practices for incident management

We identified three main factors affecting current practices for incident management: risk perception, organizational structure, and resources. We found that in light of current threats, the detection mechanisms in use will not be capable of detecting all incidents. As long as no major incidents are experienced, the perceived risk is unlikely to increase significantly, thus there will be little incentive to improve the current detection mechanisms. The risk perception is further affected by: (i) the size of the organization, and (ii) whether IT operations are outsourced. Organizations that outsource their IT operations tend to place a great deal of confidence in their supplier and put less effort into planning and preparatory activities compared with those that do not outsource. Size matters, too: small organizations have a lower risk perception than large organizations owing to the belief that they are not attractive targets for attacks, as well as their ability to operate the power grid without available control systems.

In addition to organizational and technical factors, human factors have been found to be important for incident management. Different personnel (e.g. business managers and technical personnel) have different perspectives and priorities when it comes to information security. In addition, there is a gap between how IT staff and control system staff understand information security. This finding is in agreement with Jaatun et al. [1], who studied incident response practices in the oil and gas industry. All perspectives need to be represented in the team handling a crisis. Therefore, an organization needs to rely on cross-functional teams. Relying on cross-functional teams will ensure a holistic view during the incident response process.

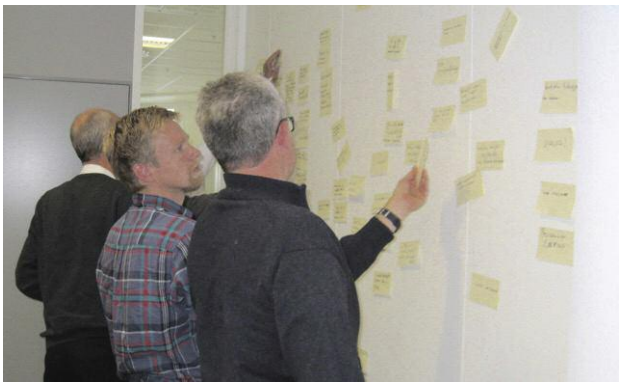


Figure 1: A team evaluating the preparedness exercise.

Cross-functional teams

Incident response is a highly collaborative activity and requires cooperation of individuals drawn from various functional areas, with different perspectives, to make the best possible decisions [2]. To create good cross-functional response teams, it is important to acknowledge that the team members might have conflicting goals. Different functional areas within an organization possess complementary goals that are derived from a set of general, organization-wide goals. Consequently, in order for one functional area to achieve its goals, another functional area may be required to sacrifice, or at least compromise, its primary goals. Therefore, the cross-functional team needs superordinate goals. Superordinate goals will have a positive and significant direct effect on cross-functional cooperation. The team further needs to be able to update its initial superordinate goals if the initial conditions change during the incident response process.

Not only does the cross-functional team need participants from various functional areas within the organization, it also needs participation from, or communication with, suppliers. The organizations in our study assumed that collaboration with suppliers functioned well, but acknowledged that this should be given more attention, as common plans were rare and collaborative exercises were not performed.

In addition to a cross-functional team having the right competence, the team members need a shared understanding of who knows what is needed to solve a task, such as a crisis, effectively [3]. Ex-

ercises provide a means for growing shared understanding of the team knowledge. The organization needs to perform exercises for a broad variety of incidents. Different incidents will require different configurations of the cross-functional team. Frequent training is important because these teams exist only when an incident occurs.

Training for responding to information security incidents is currently given low priority. Evaluations after training sessions and minor incidents are not performed. Learning to learn would enable the organizations to take advantage of training sessions and evaluations, and thereby improve their incident response practices.

The project was carried out at NTNU, in close cooperation with SINTEF and the Norwegian Smart Grid Centre. The project period was 2011-2015.

Link:
http://www.item.ntnu.no/people/personalpages/phd/maria.b.line/start

References:
[1] M. G. Jaatun, et al.: "A framework for incident response management in the petroleum industry", International Journal of Critical Infrastructure Protection, vol. 2, pp. 26–37, 2009.
[2] M. B. Line, N. B. Moe: "Understanding Collaborative Challenges in IT Security Preparedness Exercises", International Conference on ICT Systems Security and Privacy Protection (IFIP SEC) 2015, Hamburg, Germany.
[3] K. Lewis and B. Herndon: "Transactive Memory Systems: Current Issues and Future Research Directions," Organization Science, vol. 22, no. 5, pp. 1254–1265, Sep. 2011. [online], available: http://dx.doi.org/10.1287/orsc.1110.0647

Please contact:
Maria Bartnes Line
NTNU, Norway
Tel: +47-45218102
E-mail: maria.b.line@item.ntnu.no

Goal-Oriented Reasoning about Systems of Systems

by Christophe Ponsard, Philippe Massonet and Jean-Christophe Deprez

Reasoning about Systems of Systems has proved difficult, not only because it is difficult to combine heterogeneous system models, but more fundamentally because of complex interactions that make it difficult to exactly predict the emerging behaviour. Goal-oriented requirements engineering techniques can help to drive the analysis and design of systems-based techniques, combining semi-formal reasoning with more focused quantified analysis carried out through the filter of specific goals.

A System of Systems (SoS) can be defined as "an integration of a finite number of constituent systems which are independent and operatable, and which are networked together for a period of time to achieve a certain higher goal" [1]. Such higher level goals are key properties either explicitly sought when designing SoS such as airport systems (e.g. smooth management of passenger and aircraft flows), emergency disaster recovery systems (e.g. fast evacuation and securing a disaster area), defence systems (e.g. coordinate land/airborne/naval forces to achieve mission), or manufacturing complex systems (especially in circular economy and Industry 4.0 contexts) [2].

The interacting systems comprising an SoS may be very different in nature, each being described, analysed, and simulated using specific languages/techniques/tools - for example, differential equations (control systems), graph theory (e.g. road networks), Petri Nets (resources, workflows). This heterogeneity makes it difficult to build a full-scale and fine grained SoS-level model. An alternative approach is to focus on properties. Over the years, Goal Oriented Requirement Engineering (GORE) has developed powerful notations, methods and tools [2] that can be applied to this area by:

- Connecting SoS goals with properties of the interacting systems based on a rich and possibly quantified/formalized relations such as refinement, contribution, obstacle or conflict.
- Recognizing organizational-level patterns across those systems such as case-based delegation, rely/guarantee, chain of command, etc.
- Enabling hazard/impact analysis and run-time monitoring from the evolving ecosystem in order to ensure the continuity of global SoS goals.
- Or conversely 'slicing' on specific SoS goal to conduct a focused analysis on composite systems involved in achieving that given SoS goal..

For example, an emergency disaster recovery system cannot rely on an existing state emergency system to deliver care to injured people, owing to inadequate numbers of trained staff to deal with the potential volume of patients (Figure 1). The existing infrastructure should be able to globally adapt its operation mode to cope both with the emergency, and with a flow of critically injured patients coming from other areas. This requires a special plan to summons medical staff and reschedule hospital operation in an area relevant to the assessed importance of the disaster (city; district; nation-wide; or possibly international - in the case of big earthquakes, for instance). Figure 1 illustrates an excerpt of a SoS model built with the Objectiver tool. Starting from strategic SoS goals (in blue at the top), major obstacles are identified (in red) and specific goals are then added to mitigate them (in blue at the bottom), along with extra systems able to cope with them in the global SoS (yellow filled elements transitively connected to orange

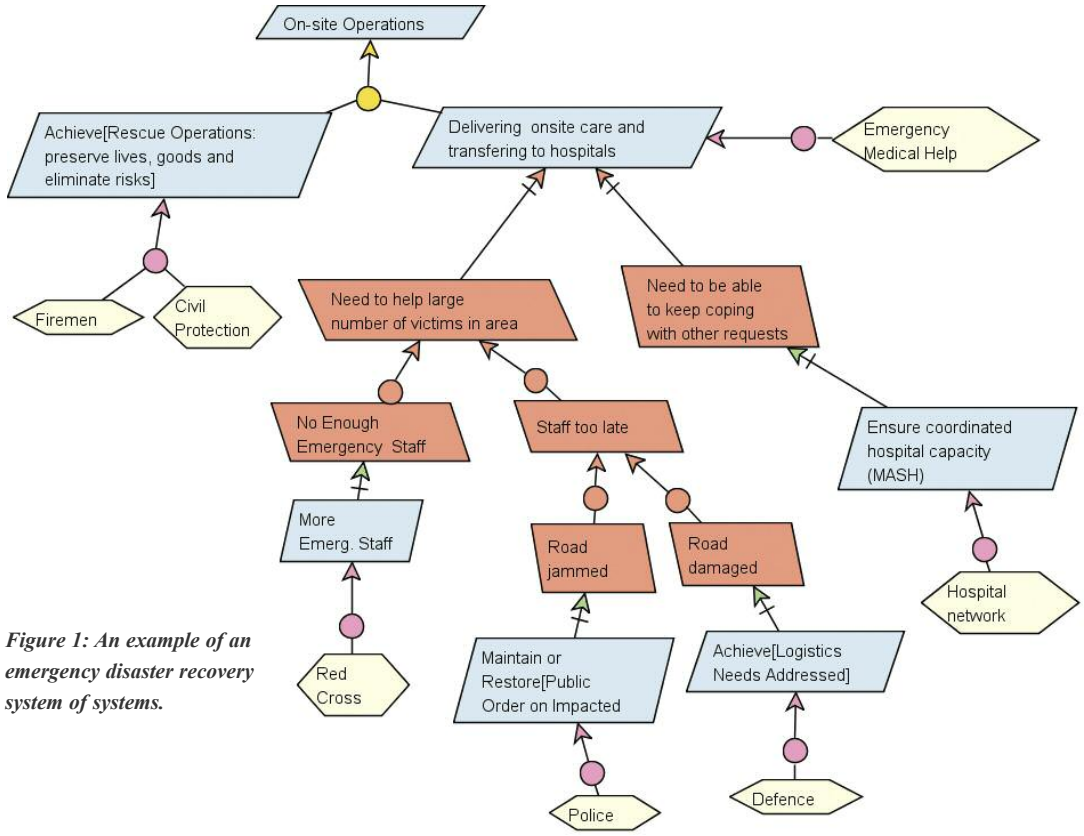


Figure 1: An example of an emergency disaster recovery system of systems.

ones). For example, the police to maintain order on the roads or defence in a specific support role to repair damaged infrastructure.

Starting from this global SoS goal-model, it is then possible to analyse how the satisfaction of goals can be achieved by carrying out a focused analysis on the relevant systems for each goal, possibly driven by specific scenarios (a typical case are SEVESO risk-class sites). This can be achieved using generic models (e.g. road intervention times can be predicted based on road graph models taking into consideration known congestion issues) or specific models (e.g. hospital capacity is related to a specific mobilization plan). In addition to what-if scenarios, such models can also support decision making at intervention time.

Our current work is precisely to extend GORE notation to better cope with SoS concepts, in particular to abstract away complexity and retain the capacity to zoom into each system, which in turn can appear as a collection of collaborating entities (which may be systems, humans playing a specific role, or software/hardware components). We are currently focusing on SoS in the emergency crisis domain and Industry 4.0 sectors, respectively in the scope of the REDIRNET and SimQRI projects where specific tools are being developed.

Links:
REDIRNET - Emergency Responder Data Interoperability Network:
http://www.redirnet.eu
SimQRI - Simulative quantification of procurement induced risk consequences and treatment impact in complex process chains:
http://www.simqri.com
Objectiver tool:
http://www.objectiver.com

References:
[1] M. Jamshidi: "System of Systems Engineering", Wiley, 2009.
[2] R. Berger: "INDUSTRY 4.0, The new industrial revolution - How Europe will succeed", 2014.
[3] A. van Lamsweerde: "Goal-Oriented Requirements Engineering: A Guided Tour", Fifth IEEE International Symposium on Requirements Engineering, 2001.

Please contact:
Christophe Ponsard
CETIC, Belgium
E-mail: christophe.ponsard@cetic.be

European Research and Innovation

Classification and Evaluation of the Extremely Low Frequency Electromagnetic Field Radiation Produced by Laptop Computers

by Darko Brodić and Alessia Amelio

We present an analysis of the extremely low frequency magnetic field radiation produced by laptop computers in normal conditions and under stress.

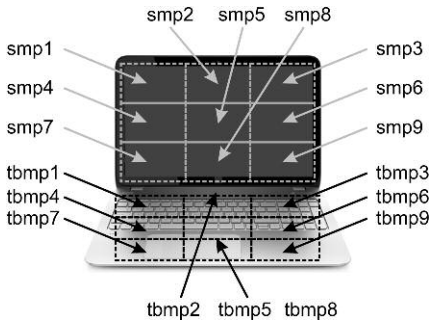
A laptop is a portable all-in-one computer powered by AC or battery. Owing to its portability, it is quite commonly used in close contact with the body, i.e. touching areas of skin, blood, lymph, bones, etc. It has been suggested that this might have negative effects on the user's health, due to the effect of the non-ionized electromagnetic radiation (EMR) characterized by extremely low frequency up to 300 Hz.

The risk of extremely low frequency magnetic exposure for laptop users has been partly analyzed [1], [2]. The World Health Organization has recognized the occurrence of hypersensitivity to electromagnetic radiation, including dermatological symptoms as well as neurasthenic and vegetative symptoms. The referent limit level is defined as the critical level of EMF radiation (extremely low frequencies), above which the environmental conditions can be unsafe for humans. This has been set as up to 0.3 μT [1], [2].

We address the problem of the magnetic field radiation to which users are exposed by their laptops. We have developed a new approach to measure and classify uniform extremely low frequency magnetic fields, produced in the laptop neighbourhood [3]. The intensity of the magnetic induction B in the direction of the Cartesian axes x, y and z is measured by Lutron EMF 828 devices. We propose 27 measurement points in the laptop neighbourhood, divided into three groups: screen measurement points, top body measurement points and bottom body measurement points.

The value of the magnetic field B around the laptop is measured under 'normal conditions' and under stress. The normal operating condition means that the laptop runs typical programs such as Word, Excel, Internet browsing, etc. The under stress laptop operations are introduced as a new approach to measurement. We consider extreme computer operations, when all parts of the laptop are under heavy load. This is achieved by running the 3DMark Vantage program, which represents the well-known computer benchmarking tool created to determine the performance of a computer 3D graphic rendering and CPU workload processing capabilities.

The results of the experiment are given for 10 laptops. They show that the level of EMF radiation in the laptop screen area is negligible or in the order up to 0.02 μT. Accordingly, only the results of EMF obtained at the top and bottom body part



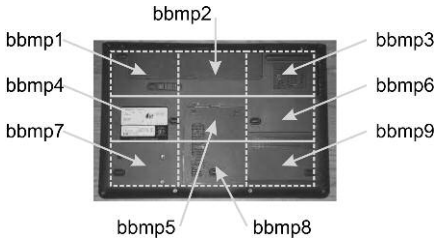


Figure 1. Measurement points in the laptop neighborhood: at the top part of a portable computer (left), at the bottom part of a portable computer (right).

of laptops are considered. Six out of ten laptops are tested in normal conditions and under stress, while the other four laptops are only tested under normal conditions. The experiment shows that the EMF values measured under stress are two to three times higher than those obtained in the normal operating condition. Furthermore, the level of EMF at the bottom part of the laptop is higher than at the top part.

In conclusion, extreme caution is needed when using a laptop. We advise: (i) connecting an external keyboard, (ii) connecting the mouse, and (iii) keeping the laptop out of the lap by putting it on a desk or table.

Finally, we measured the EMR for 10 different laptops under normal conditions. The EMF measurements are partitioned into classes leading to the establishment of different levels of dangerous and non-dangerous zones in the laptop neighbourhood. Furthermore, the areas of the laptop which are more or less dangerous when in direct contact with the user are defined. This information will provide valuable input for the design of computer inner components.

Future research will classify laptop EMF radiation under both normal and stress conditions.

The approach described is part of a project proposal which will consider the impact of the EMF radiation in the office. The bilateral research project, in collaboration with the National Research Council of Italy, will be carried out by the Technical Faculty in Bor at the University of Belgrade (Serbia). This work was partially supported by the Ministry of Education, Science and Technological Development of the Republic of Serbia TR33037.

References:

[1] S. A. Hanna, et al.: “Measurement Evaluations of Static and Low Frequency Magnetic Fields in the Near Field Region”, Measurement, 44(8):1412-1421, 2011.

[2] C. V. Bellieni, et al.: “Exposure to Electromagnetic Fields From Laptop Use of ‘Laptop’ Computers”, Archives of Environmental & Occupational Health, 67(1):31-36, 2012.

[3] D. Brodić: “The Impact of the Extremely Low Electromagnetic Field Radiations from the Portable Computers to the Users”, Revista Facultad de Ingenieria-Universidad de Antioquia, in press.

Please contact:

Alessia Amelio, ICAR-CNR, Italy
E-mail: amelio@icar.cnr.it

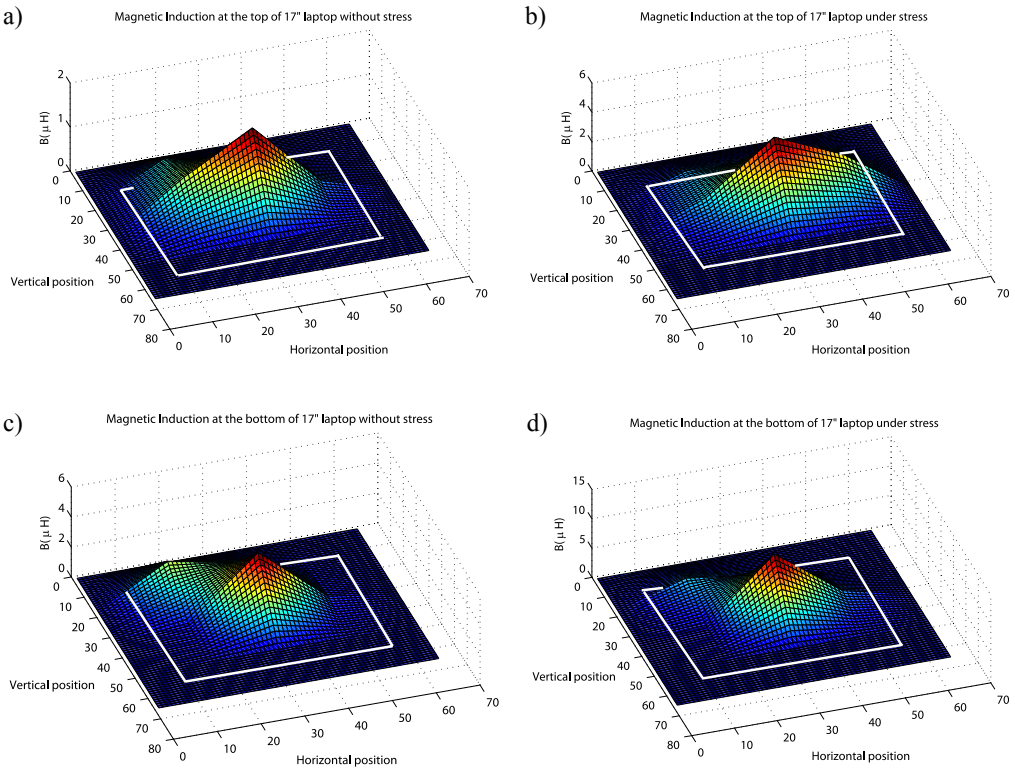


Figure 2. EMF measured values (white line represents the border of the laptop): (a) at the top part of a laptop (without stress), (b) at the top part of a laptop under stress, (c) at the bottom part of a laptop (without stress), (d) at the bottom part of a laptop under stress.

A Record-Setting Microserver: A Data-Centre in a Shoebox

by Matteo Cossale, Rolf Clauberg, Andreas Doering, Ronald Luijten, Bruno Michel and Stephan Paredes

A prototype of the world's first water-cooled 64-bit microserver, which is roughly the size of a smartphone, is part of the proposed IT roadmap for the Square Kilometer Array (SKA), an international consortium to build the world's largest and most sensitive radio telescope.

When it goes live (by 2024), the Square Kilometer Array (SKA) will collect a deluge of radio signals from deep space. Every day thousands of antennas located in southern Africa and Australia will collectively gather 14 exabytes, and store one petabyte, of data. The SKA has been described as the ultimate Big Data challenge. To solve this unprecedented challenge, in 2012, ASTRON and IBM scientists launched 'DOME', an initial five-year, 35.9 million euro collaboration, named after the protective cover on telescopes and the famous Swiss mountain [1].

Microservers integrate an entire server motherboard in a single Server-on-a-Chip (SoC), excluding main memory, bootROM and power conversion circuits. This technology has evolved to a 64bit-processor able to run server-class operating systems (OSs).

The 64-bit microserver uses a T4240 PowerPC based chip from Freescale Semiconductor running Linux Fedora and IBM DB2. At 139 × 55 mm2 the microserver contains all of the essential functions of today's servers, which are four to ten times larger in size.

Not only is the microserver compact, it is also very energy-efficient. One of its innovations is hot-water cooling, which keeps the chip's operating temperature below 85 Co. The copper plate used to transfer heat from the chips to the hot-water flow also transports electrical power by means of a copper plate. The concept is based on the same technology IBM developed for the SuperMUC supercomputer located outside of Munich, Germany[2]. IBM scientists hope to keep each microserver operating between 35–40 watts including the system on a chip (SOC) — the current design is 40 watts.

Details of the design of the microserver were presented at the 2015 IEEE International Solid-State Circuits Conference [3].

Links:

http://www.research.ibm.com/labs/zurich/sto/bigdata_dome.html
http://www.research.ibm.com/labs/zurich/microserver/#fbid=84Tir8LUSrp

References:

[1] T. Engbersen: "A Radio Telescope of the Superlative", ERCIM News, No. 92, January 2013, http://ercim-news.ercim.eu/en92/ri/a-radio-telescope-of-the-superlative
[2] G. Meijer, T. Brunschwiler, S. Paredes, and B. Michel: "Using Waste Heat from Data Centres to Minimize Carbon Dioxide Emission", ERCIM News, No. 79, October, 2009. http://ercim-news.ercim.eu/en79/special/using-waste-heat-from-data-centres-to-minimize-carbon-dioxide-emission
[3] R. Luijten, et al.: "Energy-Efficient Microserver Based on a 12-Core1.8 GHz 188K-CoreMark 28mm Bulk CMOS 64b SoC for Big-Data Applications with 159GB/s/L Memory Bandwidth System Density", ISSCC 2015, Paper 4.4, Feb.2015.

Please contact:

Ronald Luijten
IBM Research Zurich, Switzerland
E-mail: lui@zurich.ibm.com

	Memory	Peak Memory Bandwidth	Processing Speed	Simultaneous Processing Threads
Microserver Card 139mmx55mmx7.6mm	48GB	43 GB/S	200 GFlops	24
Drawer of 128 Microserver Cards	6 TB	5.5 TB/S	25.6 TFlops	3072

Table 1: Performance summary.

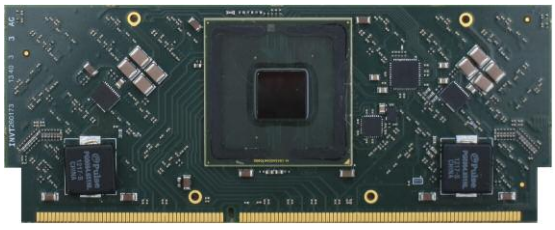


Figure 1: The Microserver.

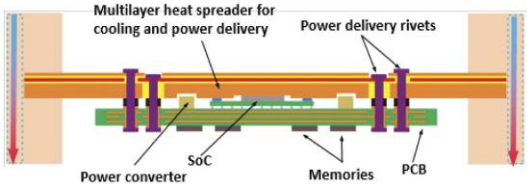


Figure 2: Cooling and power delivery for the microserver. The coolant flow can be seen on each side of the figure.

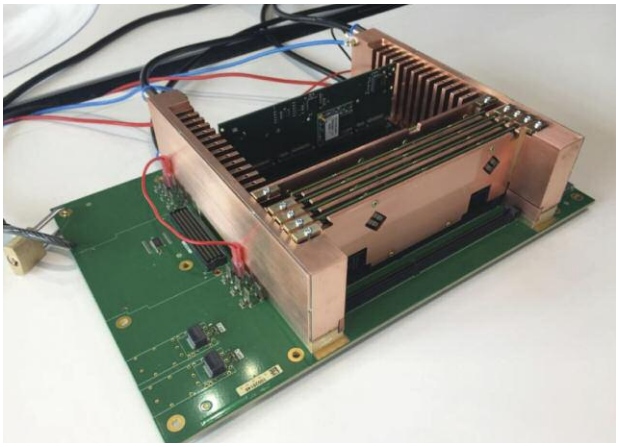


Figure 3: Microserver cluster demonstrator. Cooling water is delivered to the stack of cards via the manifolds on the left- and right-hand sides.

High Assurance Security Products on COTS Platforms

by Rolf Blom and Oliver Schwarz

With commodity operating systems failing to establish unbreakable isolation of processes, there is a need for stronger separation mechanisms. A recently launched open source project aims at applying virtualization to achieve such isolation on the widespread embedded ARM architectures. Strong assurance is established by formal verification and common criteria certification. Coexisting guest systems are able to run unmodified on the multicore platform, in a resource and cost efficient manner. The solution is rounded anchored in a secure boot process.

Governments, big organizations and authorities are increasingly starting to require independent verification (certification) of claimed security properties of deployed products and systems. For IT-solutions a well-established method is to use the Common Criteria (CC) (ISO 15408) framework and certify products according to defined and internationally recognized security requirements and assurance levels. The CC addresses protection of assets against unauthorized disclosure, modification, and loss of use.

The High Assurance Security Products on COTS (commercial of the shelf) Platforms project (HASPOC) is targeting a security solution for use in embedded systems, i.e. a trusted, cost and resource efficient virtualized commercial-off-the-shelf platform, which should have proven and Common Criteria certified security properties. The project, led by SICS Swedish ICT, is carried out together with a consortium including Ericsson Research and KTH, the Royal Institute of Technology. The key feature offered by the platform is guaranteed isolation between different users and services running on it and their associated information. The isolation is provided by a formally security verified boot and hypervisor solution. Background on the design of a hypervisor for isolation can be found in [1].

The COTS platform selected for HASPOC is an ARMv8-A based multicore system on a chip of the form indicated in Figure 1. The HASPOC developed hypervisor takes advantage of the available hardware virtualization support (MMU, S-MMU, etc.) and is in principle a bare metal solution running essentially unmodified guests. The hypervisor will support Linux as guest OS. The solution will be released as open source; the boot solution under a GNU GPL v.2 licence and the hypervisor code under an Apache v.2 licence.

The platform security solution is supported by trust anchoring and boot solutions developed by project partner T2 Data. The hypervisor builds on the SICS Thin Hypervisor (STH) for ARMv7, which in a joint KTH- SICS project PROSPER, has been studied regarding the formal verification of its security claims (isolation properties). These existing solutions will be enhanced and modified to cover the new technology offered by the ARMv8 platform, product requirements and requirements for achieving high assurance level (EAL 5/6) Common Criteria evaluations.

The project will also produce baseline documents needed for a formal CC evaluation at EAL 6, i.e. a Security Target and supporting documentation needed in the evaluation process. The idea is that these baselines documents can be used as a starting point when a product based on the HASPOC platform should be CC certified. The project itself will not perform a formal CC evaluation as it will not develop a specific product.

In the formal verification process we create a mathematical and machine checkable proof that guests executing in coexistence on the HASPOC platform behave in the same way as if each guest runs on its own machine. This guarantees isolation relaxed by desired and controlled inter-guest communication. With hardware increasingly taking over virtualization tasks, the formal verification of separation platforms departs from a pure software verification towards an integrated verification of hardware architectures, their isolation mechanisms and their interaction with software. The principles behind the formal verification work are described in [2].

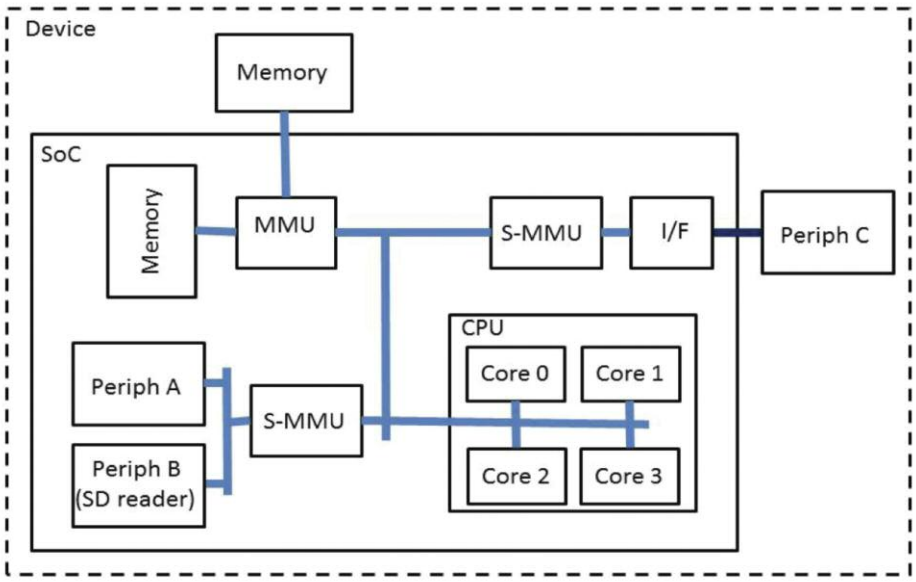


Figure 1: High level view of HASPOC compliant system on a chip.

Demonstrators in the secure communications area (encryption solutions with strict red/black separation) will be built within the project framework to test and demonstrate the efficiency and usability of the platform solution. This is an excellent test area as its security requirements are strict and

high, while at the same time there is an increasing demand for new generations of High Assurance security products with increased functionality resulting in a corresponding need to find tools to enable agile product revisions. By the introduction of trusted components such as the HASPOC platform in product development, a decrease in lead time from user requirement to developed, evaluated and deployed solution can be realized.

The developed technology will, in addition to specific security products such as crypto equipment, secure mobile phones and firewalls, be applicable in a wide range of areas like SCADA systems, mobile communication networks, vehicular, avionics and medical systems, and also for devices in the Internet of Things (IoT). Particularly interesting areas in the industrial sector are issues around mixing personal and business information in the same user device (e.g. a laptop), cloud computing (allowing tenants to share pooled resources) etc.

Links:
The HASPOC project:
https://haspoc.sics.se/
The PROSPER project:
http://prosper.sics.se
ARM Architecture:
http://www.arm.com/products/processors/instruction-set-architectures/index.php
CC; Common Criteria:
https://www.commoncriteriaportal.org/

References:
[1] O. Schwarz, C. Gehrmann, V. Do: "Affordable Separation on Embedded Platforms: Soft Reboot Enabled Virtualization on a Dual Mode System", in Proc. of Trust and Trustworthy Computing (TRUST) 2014.
[2] M. Dam, et al.: "Formal Verification of Information Flow Security for a Simple ARM-Based Separation Kernel", in Proc. of the 2013 ACM SIGSAC Conference on Computer & Communications Security (CCS'13).

Please contact:
Rolf Blom, SICS Swedish ICT
Tel: +46 70 3251906
E-mail: rolfb@sics.se

Real-Time Intelligent Monitoring and Operation Using Synchronized Wide Area Information

by Kaveri Bhuyan and Kjetil Uhlen

To meet the future challenges for sustainable energy systems, the operation and control of smart grids will require a System of Systems (SoS) approach, which takes into account the combined complexities of power grids and Information and Communication Technology (ICT) infrastructures. This encompasses a Wide Area Monitoring Systems (WAMS) approach. The basic building block of WAMS is the Phasor Measurement Units (PMUs). Based on wide area information from PMU, it is possible to monitor and observe the state of the power system in real-time. Applications utilizing PMU measurements are being developed for secure operation of power systems.

The smart grid is a complex system consisting of interdependent power grid and ICT components. This complex network is called cyber-physical system or system of systems (SoS) [1]. WAMS approach for monitoring, protection and control can help to address the future challenges in sustainable smart grid-based energy systems. The main purpose of WAMS is to improve the monitoring and observability of the power grid. WAMS will enable intelligent monitoring, protection and control of power systems using ICT.

PMUs have been extensively installed and used in many countries to stimulate development of WAMS. Our research activity concentrates on developing application of wide area information obtained from PMUs for monitoring, protection and control in smart grids. PMU measures time synchronized voltage and current phasors at any location in the power system through Global Positioning System (GPS) time stamping. The PMU measurements are collected, processed or stored in Phasor Data Concentrators (PDCs) for further use in protection and control systems. PMUs have high measurement frequency and the challenge is to secure and manage the enormous amounts of data that are available from the measurements. These aspects constitute vulnerabilities and call for robust ICT solutions and strong power grid considering interdependencies and interoperability. Thus, WAMS has to be able to provide more accurate, fast and reliable information for initiating control actions. Figure 1 shows the layout of a simple WAMS architecture [2]. It primarily consists of PMUs, PDCs, and PMU-based application systems.

State estimation is a key function in power system planning, operation and control [3]. Time synchronized PMU measurements at different locations makes it possible to have state estimates that can be utilized for control purposes in power systems. With the availability of phasor measurements, it is easier to obtain optimized power flow solutions, security/stability assessment enabling flexible operation of the system closer to its stability limit. As part of our research, we plan to

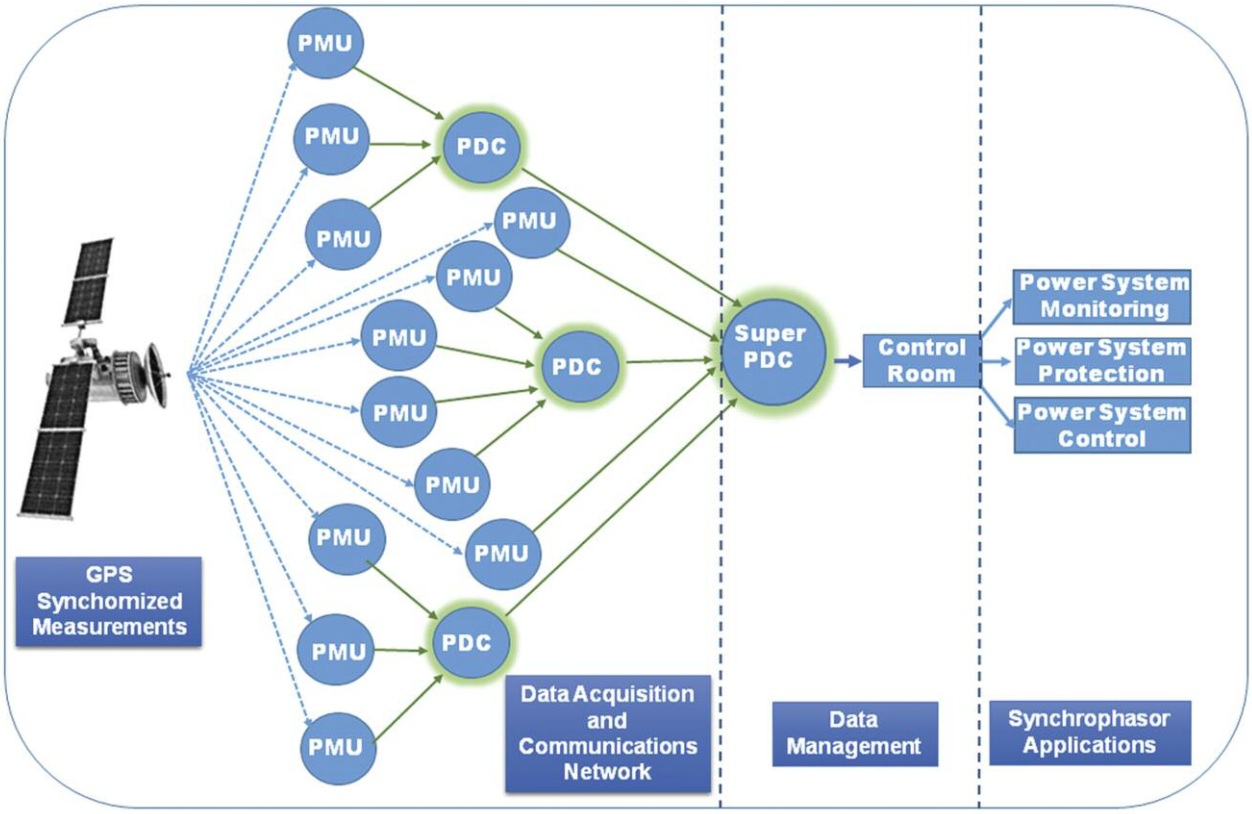


Figure 1: Basic layout of wide area monitoring systems [2]

develop formal methods to extract useful information - e.g. to help anticipate whether an operating point is potentially vulnerable (e.g. resulting in a voltage collapse or poorly damped inter-area oscillations). The PMUs are installed in the Smart Grid/ Renewable Energy Laboratory at Norwegian University of Science and Technology, Trondheim, Norway. The data regarding system frequency, power oscillation and voltage stability obtained from the PMU measurements at multiple locations could be used to identify possible vulnerabilities in the test system. The primary objective of our work is to develop, demonstrate and validate smart and robust solutions for power system operation and control in smart grids using PMUs. The eventual goal is to develop methods to extract and aggregate useful information from PMU data for power system state estimation to increase situational awareness, identify and analyze cyber-physical system vulnerabilities in real-time. The next-generation monitoring, and control centre will use PMU data to assess available transfer margins across transmission corridors, provide corrective actions to prevent cascading failures and blackouts, provide probabilistic risk assessment for N-x contingencies, and automatic protection and restoration.

References:

[1] J. Wäfler, P.E. Heegaard: "Interdependency modeling in smart grid and the influence of ICT on dependability", Adv Commun Networking, pp. 185–196, 2013.
[2] M. Chenine, et al.: "Implementation of an experimental wide-area monitoring platform for development of synchronized phasor measurement applications", IEEE Power and Energy Society General Meeting, pp.1-8, July 2011.
[3] Y.-F. Huang, et al.: "State estimation in electric power grids: Meeting new challenges presented by the requirements of the future grid," IEEE Signal Process. Mag., vol. 29, no. 5, pp. 33–43, Sept. 2012.

Please contact:

Kjetil Uhlen
NTNU, Norway
E-mail: kjetil.uhlen@ntnu.no

Kaveri Bhuyan
Post-doctorate researcher (ERCIM fellow)
NTNU, Norway
E-mail: Kaveri.Bhuyan@ntnu.no

Integrated Care Solutions

by Mariagrazia Fugini, Federica Cirilli and Paolo Locatelli

The Italian Project "Digital Support and Social Innovation in Controlled Environments - Attiv@bili", funded by the Region of Lombardy, proposes innovative organizational and ICT models for the care of frail individuals (e.g. the elderly and people with disabilities). These individuals require both health and social services (integrated care), preferably at home.

The number of frail individuals, in particular elderly people and people with disabilities, requiring assistance is increasing rapidly, creating a critical situation for health and social services management. As far as possible, these people should be cared for in their own homes. ICT tools and home automation devices can play an important role here, increasing the quality of life and promoting social inclusion.

The Attiv@bili project is developing tools that support the provision of health and social care services in the home. The focus is on process coordination between organizations and on integrated ICT solutions, both seen as key factors in achieving effective information exchange between all those involved (individuals and agencies) in care provision.

Attiv@bili

Attiv@bili aims at: (i) sustainability, requiring small investments in new technologies and few organizational changes; (ii) health and social care integration, through information systems and acquisition of data about health, behaviour, social activities and responsiveness of patients at home and in assisted residential living; (iii) end-to-end services for key groups of patients; (iv) flexible hardware and software solutions that can be personalized locally; (v) services that are scalable according to population demand; (vi) strengthened organizational initiatives, introducing process best practices to guide the project.

These targets are achieved through networked information systems and data acquisition devices in the home. End-to-end services and macro-classes of patients are taken into account; however, the proposed solutions aim at respecting specificities and individual levels of acceptance and need for privacy.

Attiv@bili begins by gathering data in the home in four distinct areas: (i) Ambient Intelligence; (ii) Interactive media (e.g. interactive television); (iii) Body Area Sensors; (iv) Smart assistance systems (e.g. voice recognition systems, automatic reminders and alert functions).

Attiv@bili fosters digital process support and the sustainable integration of different actors involved in social assistance and care through: (i) extension of the capabilities of existing solutions; (ii) sharing of dedicated systems between actors operating on care processes; (iii) integration of services and information within each process step, managed by different information systems.

The core of the integration model is a backbone platform conveying data from devices for ambient automation and orchestrating process components. The platform is designed to use limited resources and to support integrated care processes.

From an organizational viewpoint, Attiv@bili develops a set of Key Performance Indicators and coordination mechanisms through which operations of the various actors can be aligned dynamically.

Framework

The ICT solution in Attiv@bili is a service-oriented and event-driven platform [2], including an Orchestration and Integration System made of workflows and services for information sharing, alerts, ambient control commands and moni-

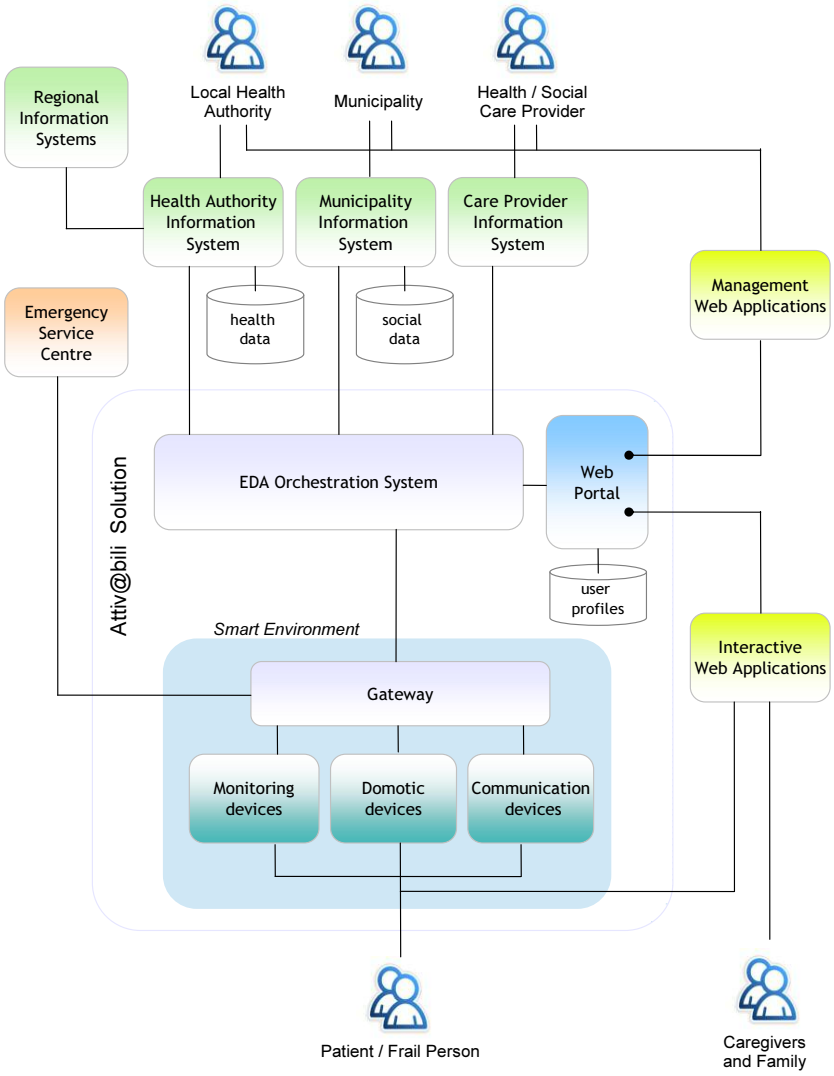


Figure 1: Collaborative software architecture in the Attiv@bili solution.

toring (see Figure 1). It acts as a flexible orchestrator across different actors connected through their information systems via software adapters. New actors/systems could be integrated by developing a suitable adaptor. Cooperation between different information systems occurs through signals and contextualized information, according to specific events. For example, the need for a new care plan by a Local Healthcare Authority is transmitted through an alert to a certified care provider via Attiv@bili: visits to the patient's home will automatically generate feedback via the information systems made interoperable via the Attiv@bili platform.

Integration between sensors and monitoring tools at patients' homes or in residential complexes guarantees continuity of care among care providers. The Gateway currently connects a smart watch, a number of domotic devices (totems) and communication devices (web browsers or smart devices). The Gateway will be connected to an Emergency Service Centre. The Web Portal shows administrative and advanced (smart care) services. Attiv@bili includes two types of application modules: applications for the actors of care service management processes, and applications providing interactive services to the assisted subjects/caregivers. The Portal interacts with the orchestration system to manage user profiles, and is an access point for third parties providing additional services (e.g. ordering medical supplies).

Prototype

The prototype is currently being activated by local public health authorities and care service providers. Meanwhile, pilot environments are being set up with home devices to cater for different kinds of patient needs and in different living settings, from private homes to residential complexes, both in rural and urban areas.

Attiv@bili is funded by the by the Region of Lombardy within the Smart Cities 2007-2013 Regional Development Structural Funds of the European Union. The project partners include Linea Com Srl, Politecnico di Milano, GPI Spa, Consoft Systems Spa, Fluidmesh Networks Srl, Ancitel Lombardia, Microdevice Srl, Studiofarma Srl and two non-profit organizations for health and social care services in Lombardy.

References:

[1] G. Okeyo, Li. Chen, H. Wang: "Combining ontological and temporal formalisms for composite activity modelling and recognition in smart homes", Future Generation Computer Systems, vol. 39, Oct. 2014, pp. 29-43.
[2] A. Mouttham, et al.: "Event-driven data integration for personal health monitoring", Journal of Emerging Technologies in Web Intelligence 1.2 (2009): 110-118.

Please contact:

Mariagrazia Fugini - Politecnico di Milano, Italy
Tel: +39-02-23993624
E-mail: mariagrazia.fugini@polimi.it

Predictive Analytics for Server Incident Reduction

by Jasmina Bogojeska, Ioana Giurgiu, David Lanyi and Dorothea Wiesmann

As IT infrastructures become more heterogeneous — with cloud and local servers increasingly intermingling in multi-vendor datacentre infrastructure environments — CIOs and senior IT decision makers are struggling to optimize the cost of technology refreshes. They need to be able to justify the cost of technology refresh, manage the risk of service disruption introduced by change and balance this activity against business-led IT changes.

The decision about when to modernize which elements of the server HW/SW stack is often made manually based on simple business rules. The goal of our project is to alleviate this problem by supporting the decision process with an automated approach. To this end, we developed the (Predictive Analytics for Server Incident Reduction (PASIR) method and service (conceptually summarized in Figure 1) that correlates the occurrence of incidents with server configuration and utilization data.

In a first step, we need to identify past availability and performance issues in the large set of incident tickets. This incident ticket classification, however, is a very challenging task for the following reasons:

- The number of tickets is very large (in the order of thousands in a year for a large IT environment), which makes their manual labelling practically impossible.
- Ticket resolution is a mixture of human and machine generated text (from the monitoring system) with a very problem-specific vocabulary.
- Different ticket types have very different sample abundances.
- The texts of the tickets from different IT environments are very different as they are written by different teams who use different monitoring systems and lingua, which renders the reuse of manually labelled tickets and knowledge transfer among different IT environments infeasible.

To address these challenges, we implemented an automatic incident ticket classification method that utilizes a small, preselected set of manually labelled incident tickets to automatically classify the complete set of incidents available from a given IT environment. In the first step, to select the training data for the supervised learning, we apply the k-means clustering algorithm to group the incident tickets into bins with similar texts and then sample tickets for training with the ratio of samples to be selected from each cluster being computed using the silhouette widths of the clusters. This results in an increased representation of incident tickets from rare classes in the training data. In the second step, we use the manually labelled set of incident tickets to train a gradient boosting machine (GBM), a powerful, flexible method that can effectively capture complex non-linear function de-

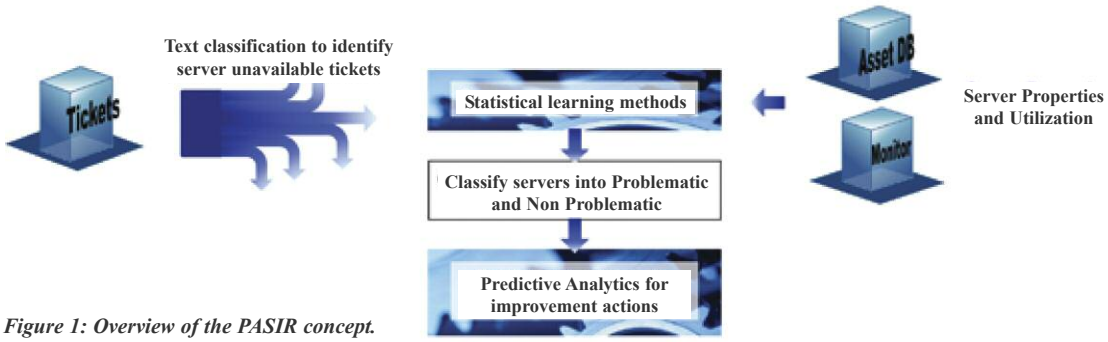


Figure 1: Overview of the PASIR concept.

pendencies and offers high quality results in terms of prediction accuracy and generalization.
Next, we define a threshold for incident tickets of a certain class to identify servers with problematic availability or performance. Based on the historic set, a Random Forest classifier is trained to identify and rank servers with problematic behaviour as candidates for modernization. Random Forest models are ensembles of classification or regression trees. While regular tree models are very attractive and widely used nonlinear models due to their interpretability, they exhibit high variance and thus have a lower capability for deducing generalizations. The Random Forest model reduces the variance by averaging a collection of decorrelated trees which provides performance comparable to that of support vector machines (SVMs) and boosting methods. Such a model can capture nonlinear relationships between the attributes of the server hardware, operating system and utilization and the server behaviour characterized by the corresponding incident tickets.

A summary of the procedure for training random forest models is given in Figure 2. Once trained, the predictive model is used to evaluate the impact of different modernization actions and to suggest the most effective ones. Each modernization action modifies one or several server features.

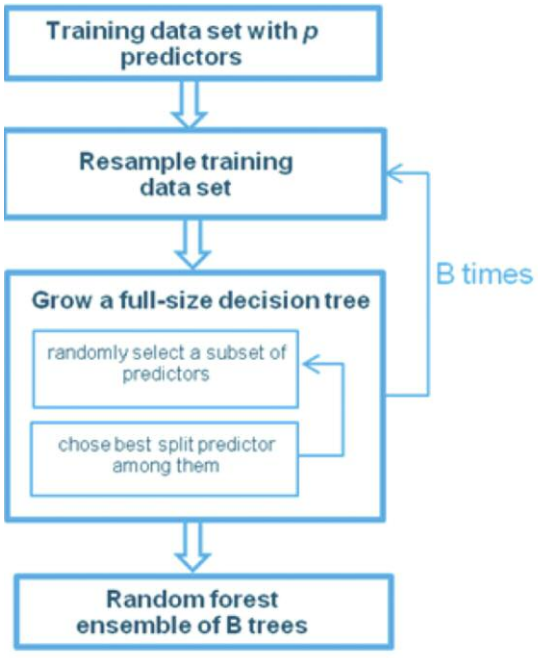


Figure 2: Overview of the training procedure for a Random Forest model.

Given a set of modernization actions, a random forest prediction model, and a target server, we quantify their improvement impact by taking the difference between the probabilities of the server being problematic before and after applying the actions considered. This enables us to rank all modernization actions based on their improvement impact and select the most effective ones.

The PASIR tool has been applied to over one hundred IT environments. The resultant modernization actions have resulted in significant reductions in the account incident volumes with a concomitant increase in the availability of the IT environment. The primary use cases of our tool are planning a refresh program, identifying an at-risk application environment, identifying servers for CLOUD migration, and contributing to cost penalty analyses for at-risk servers.

Link:
http://www.zurich.ibm.com/csc/services/textmining.html

References:
[1] J. Bogojeska et al.: "Classifying Server Behavior and Predicting Impact of Modernization Actions", in Proc. of the IFIP/IEEE 9th International Conference on Network and Service Management (CNSM), 2013.
[2] J. Bogojeska et al.: „Impact of HW and OS Type and Currency on Server Availability Derived From Problem Ticket Analysis", in Proc. of the IFIP/IEEE Network Operations and Management Symposium (NOMS), 2014.
[3] L. Breiman: "Random Forests", Machine Learning, 2001.

Please contact:
Dorothea Wiesmann
IBM Research Zurich, Switzerland
E-mail: dor@zurich.ibm.com

Fixing the Sorting Algorithm for Android, Java and Python

by Stijn de Gouw and Frank de Boer

In 2013, whilst trying to prove the correctness of TimSort - a broadly applied sorting algorithm - the CWI Formal Methods Group, in collaboration with SDL, Leiden University and TU Darmstadt, instead identified an error in it, which could crash programs and threaten security. Our bug report with an improved version, developed in February 2015, has led to corrected versions in major programming languages and frameworks.

Tim Peters developed the Timsort hybrid sorting algorithm in 2002. TimSort was first developed for Python, a popular programming language, but later ported to Java (where it appears as java.util.Collections.sort and java.util.Arrays.sort). TimSort is today used as the default sorting algorithm in Java, in Android (a widely used platform by Google for mobile devices), in Python and many other programming languages and frameworks. Given the popularity of these platforms this means that the number of computers, cloud services and mobile phones that use TimSort for sorting is well into the billions.

After we had successfully verified Counting and Radix sort implementations in Java [1] with a formal verification tool called KeY, we were looking for a new challenge. TimSort seemed to fit the bill, as it is rather complex and widely used. Unfortunately, we weren't able to prove its correctness. A closer analysis showed that this was, quite simply, because TimSort was broken and our theoretical considerations finally led us to a path towards finding the bug (interestingly, that bug appears already in the Python implementation). Here we sketch how we did it.

TimSort reorders the input array from left to right by finding consecutive (disjoint) sorted segments (called "runs" from here on). The lengths of the generated runs are added to an array named *runLen*. Whenever a new run is added to *runLen*, a method named mergeCollapse merges runs until the last 3 elements in *runLen* satisfies certain conditions , the most important one being *runLen[n-2] > runLen[n-1] + runLen[n]*.

This condition says that the sum of the last two runs is strictly smaller than the third last run and follows the pattern of the well-known Fibonacci sequence. The intention is that checking this condition on the top 3 runs in *runLen* in fact guarantees that all runs satisfy it (the "invariant"). At the very end, all runs are merged, yielding a sorted version of the input array.

For performance reasons, it is crucial to allocate as little memory as possible for *runLen*, but still enough to store all the runs. If the invariant is satisfied, the run lengths in reverse order grow exponentially (even faster than the Fibonacci sequence: the length of the current run must be strictly bigger than the sum of the next two runs lengths). Since runs do not overlap, only a small number of runs would then be needed to cover even very big input arrays completely.

However, when we tried to prove the invariant formally, we found out that it is not sufficient to check only the top 3 runs in *runLen*. We developed a test generator that builds an input array with many short runs – too short, in the sense that they break the invariant – which eventually causes TimSort to crash with an *ArrayOutOfBoundsException*.

We also succeeded to fix TimSort by checking the last 4 runs and formally verify this new version using a deductive verification platform for sequential Java and JavaCard applications, called KeY. It allows to statically prove the correctness of programs for any given input with respect to a given specification. Roughly speaking, a specification consists of a precondition (a condition on the input), also called requires clause and a postcondition (a condition on the output), also called ensures clause. Specifications are attached to method implementations, such as mergeCollapse() above.

The (simplified) mergeCollapse contract (Figure 1) illustrates these concepts.

```
/*@ private normal_behavior
  @ requires
  @   stackSize > 0;
  @ ensures
  @    (\forall int i; 0<=i && i<stackSize-2;
  @        runLen[i] > runLen[i+1] + runLen[i+2]);
private void mergeCollapse() {
```

Figure 1: The (simplified) mergeCollapse contract.

The precondition *stackSize > 0* means intuitively that *mergeCollapse()* should only be called when at least one run has been added. The two formulas in the postcondition (ensures) imply that after mergeCollapse completes, all runs satisfy the invariant. Without tool support and automated theorem proving technology it is hardly possible to come up with correct invariants for non-trivial programs. And in fact, it is exactly here that the designers of TimSort went wrong. So far, this was one of the hardest correctness proofs ever of an existing Java library. It required more than two million rules of inference and thousands of manual steps. With such an widely used language like Java, it is important that software does not crash. This result illustrates the relevance of formal methods, e.g., in Python our fix was quickly applied.

Other recent successful applications of formal methods are INFER, an automatic, separation-logic-based memory safety checker used in Facebook and the Temporal Logic of Actions (TLA). TLA is developed by Leslie Lamport, Recipient of the Turing Award 2013. It is in use by engineers at Amazon Web Services.The work was co-funded by the EU project Envisage.

Link:
http://envisage-project.eu/wp-content/uploads/2015/02/sorting.pdf

Reference:
S. de Gouw, F. de Boer, J. Rot: "Proof Pearl: The KeY to Correct and Stable Sorting", Journal of Autom. Reasoning 53(2), 129-139, 2014.

Please contact:
Stijn de Gouw, Frank de Boer, CWI, The Netherlands
E-mail: cdegouw@cwi.nl, f.s.de.boer@cwi.nl

Making the Internet of Things Fly

by Michael Baentsch and the IBM LRSC Team

The major challenges in turning the IoT (Internet of Things) vision into a reality are manifold: end-device power consumption, wireless range and penetration, coordination and control, and security. The Semtech LoRa(tm) modulation scheme enables extremely energy-efficient end devices that communicate wirelessly over distances of up to 40km in a single hop. The IBM Long-Range Signaling and Control (LRSC) software enables deploying and securely operating large-scale multi-tenant networks based on LoRa.

Over the next five years, Gartner estimates that more than 25 billion devices will be connected and become part of the IoT covering a broad range of applications from metering to environmental monitoring to waste management to tracking. This number strains the capability of current day technology: A large percentage of the envisioned applications further share some common characteristics that are not well served by the existing IoT infrastructure based on cellular networks. Most importantly, end devices must be able to live on a single set of batteries for extended periods, sometimes up to ten years or even longer. On the other hand, the communication requirements are rather moderate, typically sending a couple of bytes uplink every hour and receiving downlinks even far less often. From an infrastructure perspective, in turn, the challenge is to manage large numbers of end devices while utilizing the available bandwidth in the best possible way. On top, the challenge is to achieve this without sacrificing end-to-end data security and integrity between the end device and the application backend.

The key component for the solution to this problem is the use of a long-range, low-data-rate communications infrastructure that needs fewer base stations to serve simple end devices like smoke detectors, temperature sensors, or smart electrical heating controllers. While several radio technologies exist, one radio technology appears to be most promising: Semtech LoRa. The LoRa modulation scheme has ideal characteristics for many IoT applications by providing a robust, spread-spectrum modulation that can be used both in licensed and license-exempt (ISM) wireless spectrum between 70 MHz and 1GHz. This permits bi-directional low-power transmission using dynamically adaptable data rates from 300 bps up to 50 kbps over variable distances of up to 40 km. This modulation technique has significant advantages when compared with cellular networks and Wifi, including lower cost, good penetration of obstacles, greater coverage over longer distances, and better battery life. Based on the LoRa modulation, Semtech, Actility and IBM Research have created the LoRaWAN MAC specification for the just recently launched LoRa Alliance, an open, non-profit association of infrastructure providers, telecom operators and end-device manufacturers.

To deploy and operate a network of millions of connected sensors in a reliable, efficient, and secure way is a huge challenge, for which IBM Research has developed the IBM Long Range Signaling and Control (LRSC) system. This includes all the software components to deploy and manage a large-scale multi-tenant network of wireless devices using the LoRaWAN protocol. It comprises all functional and security logic distributed over the gateways to a central network server and multiple application routers as well as the corresponding end-device protocol software. End devices may be fixed or mobile and even roam across network boundaries and, according to LoRaWAN may send messages at their own discretion. For downlinks, end devices may fall into different classes according to LoRaWAN: end devices of Class A listen for a downlink only directly after an uplink; end devices of Class B further listen regularly to a network beacon for time synchronization according to some specific schedule; and end devices of Class C always listen when not sending.

In line with the LoRaWAN specification, the system further uses cryptographic authentication and end-to-end encryption of application payloads with device-specific AES128 keys. Most notably, and in line with the LoRaWAN specification, the architecture clearly separates the network operator from the users of the network. All cryptographic (session) keys are unique per end device (i.e., no network-wide keys exist) and the network operators are only enabled to do cryptographic integrity checking without gaining access to the actual user data.

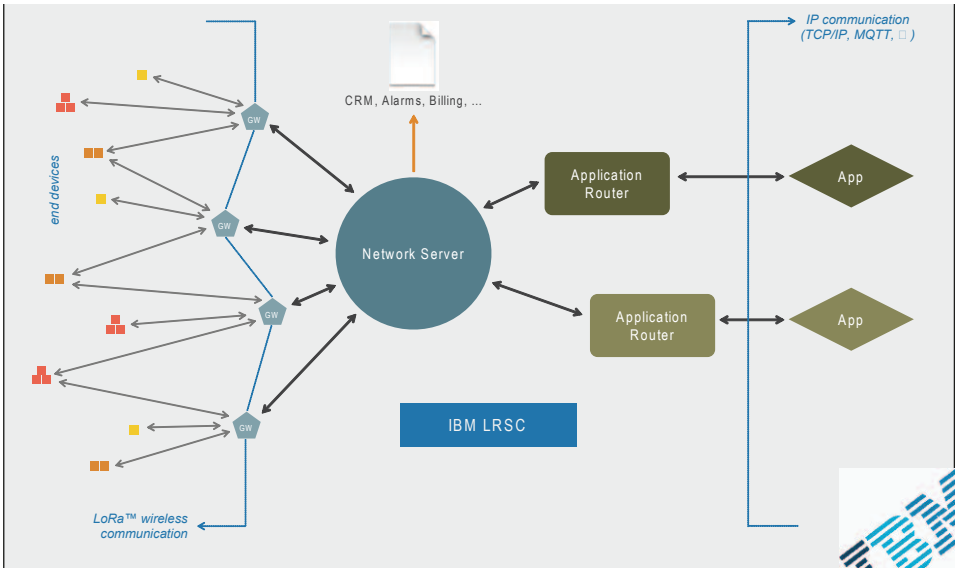


Figure 1: A typical Long-Range Signaling and Control (LRSC) installation comprises a central network server linking hundreds or thousands of radio gateways (GWs) to dozens of application routers. In this way, hundreds of thousands of end devices can establish a secure bidirectional, low-data-rate connection with corresponding Apps, thus enabling millions of small, IoT-type transactions per day per system installation.

Gateways

The primary role of the gateways is to relay traffic between end devices and the network server bi-directionally: concretely, to add timestamps and metadata to the messages received from the end devices, send messages to the end devices following a schedule set by the network server, regularly broadcast beacons for end devices of Class B, and provide operational meta-information to the network server for network optimization. LoRa gateways managed by IBM LRSC communicate with the network server using TLS (Transport Layer Security) certificate-based authentication, and limit the impact on the network server potentially caused by traffic from malicious end devices. Furthermore, gateways are time-synchronized, provide management commands for the network operator, and allow for automatic updates.

Network Server

The network server functions as the central control center and communication hub, managing the complete infrastructure and scheduling all up- and downlink traffic for potentially millions of end devices while maximizing the use of the available bandwidth. It further keeps the network in an optimal state (e.g., by global data-rate optimization for every single end device), collects usage data for network operation, optimization, and billing, and provides a broad range of management and maintenance interfaces. Billions of events are generated by all entities in the system, e.g., gateways, devices, application routers, conveying not only data-flow related information but also system health and security critical aspects. All these events are persistently logged, and can be queried and analyzed to enable network operators full insight and control over the infrastructure. To ensure fault tolerance, a warm stand-by network server on a remote secondary node can take over using regularly mirrored data.

Application Router

The application routers serve as the interface to the backend application servers with typically one application router per application. As part of this, application routers relay traffic between network server and application servers, authorize LoRaWAN JOIN requests issued by end devices, and serve as the application-level encryption endpoint for the end-to-end user data payload encryption. To ensure fault tolerance, application routers are typically run in a warm stand-by configuration.

The overall system separates the network operator from the application owners, providing privacy, fault tolerance, and security. After large-scale simulation with hundred thousands of end devices, a physical test bed has been built in the laboratory to study and improve the system subject to real-world problems like RF-interference.

Links:

http://www.research.ibm.com/labs/zurich/ics/lrsc/
http://lora-alliance.org/
http://www.zdnet.com/article/25-billion-connected-devices-by-2020-to-build-the-internet-of-things/

Please contact:
Michael Baentsch, IBM Research Zurich, Switzerland
E-mail: mib@zurich.ibm.com

Resilient Collaboration for Mobile Cloud Computing

by Nadir Guetmi, Moulay Driss Mechaoui and Abdessamad Imine

Designing reliable and resilient collaborative applications has become a hot topic in mobile cloud computing, raising challenging issues such as data management and failure recovery.

The powerful evolution of hardware, software and data connectivity of mobile devices (such as smartphones and tablets) stimulates people to publish and share their personal data independently of spatial and temporal constraints. Indeed, by the end of 2014, the number of mobile-broadband subscriptions reached 2.3 billion globally [1]. Taking advantage of the increasing availability of built-in communication networks, mobile devices enable users to manipulate collaborative applications, such as communicating by email and short messages, playing games, sharing information, organizing videoconferences, and coordinating business events.

Although mobile device hardware and network modules are continually evolving and improving, these devices will always be resource-poor and with unstable connectivity and constrained energy [2]. For instance, to manage natural catastrophe recovery in disaster-stricken zones, collaboratively writing a shared report in real-time through ad-hoc peer-to-peer mobile networks is often very expensive because it requires enormous energy consumption to (i) manage the rescue team scalability (join and leave events), and most importantly, (ii) synchronize multiple copies of the shared report to maintain a consistent and global view of the disaster situation. Moreover, it is not possible to ensure a continuous collaboration due to frequent disconnections.

To overcome the mobile device resource limitations, one straightforward solution is to leverage cloud computing, which is an emerged model based on virtualization for efficient and flexible use of hardware assets and software services over a network without requiring user intervention. Virtualization extends the mobile device resources by offloading execution from the mobile to the cloud where a clone (or virtual machine) of the mobile is running. Cloud computing allows users to build virtual networks 'à la peer-to-peer' where a mobile device may be continuously connected to other mobiles to achieve a common task. Current cloud systems provide only the creation of infrastructures as only the process for provisioning the system. However, other steps such as installation, deployment, configuration, monitoring and management of failure recovery are needed to fully provide reliable and resilient collaboration for mobile users in the cloud. For example, users must be able to easily recover all shared documents in the event of a technical hitch (e.g. crash, theft or loss of mobile device) and be able to seamlessly continue the collaboration.

In [3], we have designed a new cloud-based platform to ensure an efficient and scalable real-time collaboration service

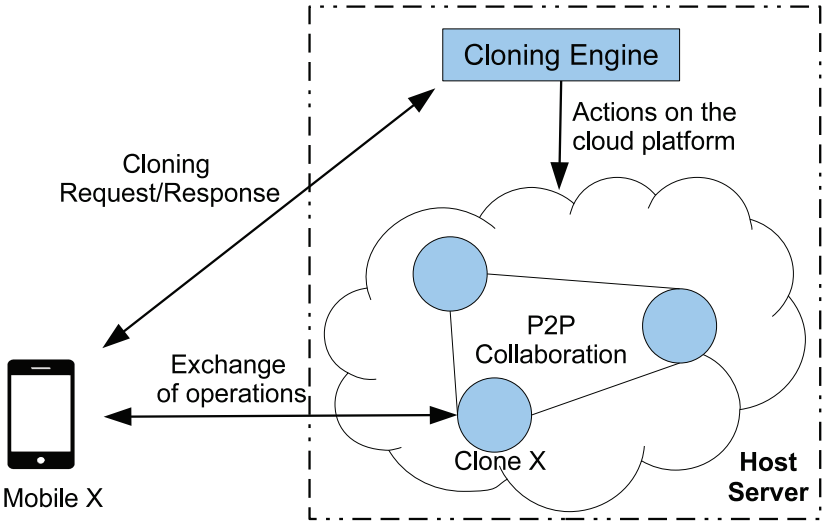


Figure 1: Architecture of our cloud-based collaboration service.

for mobile devices. Thus, each user owns two copies of the shared document (such as XML or RDF documents) with the first copy stored in the mobile device and the second on its clone (at the cloud level). The user modifies the mobile copy and then sends local modifications to the clone in order to update the second copy and propagate these modifications to other clones (i.e. other mobile devices).

As illustrated in Figure 1, our service consists of two levels. The first level (Cloning Engine) provides self-protocol to manage the complete life cycle of clones. This protocol (i) instantiates clones for mobile devices, (ii) builds virtual peer-to-peer networks across collaborative groups, (iii) seamlessly manages the join and leave of clones inside the groups, and (iv) creates a new instance of a clone when a failure appears. Our cloning deployment protocol also deals with many failure situations and it allows any failed clone to restore its consistent state and re-join its collaborative group. This cloning-based solution enables us to achieve data availability and fault tolerance. Indeed, the shared data and the collaborative service are continuously available. Even if a user's mobile device is lost, the user can recover the current shared data from the clone copy. Moreover, the user can work during disconnection by means of the mobile device's copy.

Clone-to-clone and mobile-to-clone interactions may cause concurrent updates to lead to data inconsistency. Thus, the second level (Collaboration Engine) furnishes group collaboration mechanisms in real-time and procedures for maintaining consistency of shared documents. All concurrent updates are synchronized in decentralized fashion in order to avoid a single point of failure, where each clone communicates and synchronizes itself with all other clones. Thus, it offers (i) better performance as the bottlenecks will be eliminated, and (ii) better fault tolerance, since if one clone fails, the rest of the system can still function. This data synchronization is mainly performed at the cloud level, minimizing the amount of energy used by the mobile device during collaboration.

References:
[1] Brahima Sanou: "The World in 2014: ICT Facts and Figures", http://www.itu.int/en/ITUD/Statistics/Documents/facts/ICTFactsFigures2014-e.pdf, 2014
[2] M. Satyanarayanan, et al.: "The case for vm-based cloudlets in mobile computing", Pervasive Computing, IEEE, 8(4), 14-23, 2009.
[3] N. Guetmi, et al.: "Mobile Collaboration: a Collaborative Editing Service in the Cloud", to appear in ACM SAC, 2015.

Please contact:
Nadir Guetmi
LIAS/ISAE-ENSMA, Poitiers University, Chasseneuil, France
E-mail: Nadir.Guetmi@ensma.fr

Virtual Prediction Markets in Medicine

by Pavel A. Mozolyako and Nikolai N. Osipov

Probability estimates for different prognoses in the medical field may be achieved by means of a global system of weighted expert assessments. The system, based on the concept of a virtual prediction market, will allow aggregation of the intuitive opinions of various experts about outcomes of a medical case.

Imagine a process with several possible outcomes that are mutually exclusive: for example, an illness that may result in either recovery or death. A pool of experts is available to offer their intuitive opinions about the likely outcome. The following question naturally arises: how do we aggregate these opinions to obtain probability estimates for outcomes? The answer: by using a virtual prediction market.

Commercial prediction markets are systems where people bet with each other on possible outcomes of an event, choosing various odds (prices) and amounts of money to risk. Equilibrium prices in such a market are known to give good probability estimates for outcomes [1]. However, if such a market is commercial, this activity is close in spirit to bookmaking and cannot be considered ethical (especially when applied to medicine). We can, however, organize a virtual analogue of such a market, using virtual points ('votes') instead of money, to create an excellent system of weighted voting. An 'expert' is anyone with an opinion about the process and its outcomes; unskilled 'experts' have little impact on the process since their collective weight in the vote pool is small. In this sense, prediction markets are very stable systems.

At least one such system is already successfully applied in medicine. This is the CrowdMed project, which is designed to provide sophisticated diagnoses by means of weighted voting of a large number of experts. For example, it allows diagnosis of nontrivial genetic abnormalities. This system also allows a solution to be selected, but without a detailed analysis of its possible effects.

The system we are designing will be mainly intended to assist with choice of treatment for already diagnosed patients. For each case, the system will analyse in detail all possible effects for each solution that is proposed either by the patient's attending physician, by the patient, or by another expert participating in the voting. So while CrowdMed is mainly dedicated to making sophisticated diagnosis, our system is intended for cases where we have nontrivial solutions with effects that are difficult to forecast.

A patient with a confirmed diagnosis may have several variants of treatment to choose from (for example, 'no treatment', 'surgical treatment', 'drug treatment 1', and 'drug treatment 2'). For each variant, the attending doctor may describe one or more possible effects, and will open voting (implemented as a virtual prediction market) for each of them. For example, the doctor could add 'the patient will survive for five years' effect for the 'no treatment' variant; 'the patient will survive the operation' and 'the patient will survive for five years' effects for the 'surgical treatment' variant, and so on. After the voting, we will obtain some estimates for the corresponding conditional probabilities (for example, the conditional probability of the event 'the patient will survive for five years' given the event 'surgical treatment'), and the doctor will be able to choose the most appropriate treatment.

How should the above estimates be calculated? As we have said before, some probability estimates are given by equilibrium prices of the corresponding virtual markets. But such estimates are too rough, and a lot of time is needed to achieve the equilibrium state. We are developing a method that will allow effective utilization of prediction market data and extraction of an aggregated opinion of experts. Our approach is based on one of the latest concepts of decision theory (lottery dependent utility) [2], analysis of censored samples, and some equilibrium equations. We also aim to compare the methods of classical medical statistics with our approach. Namely, we are going to show that our system gives probability estimates that are at least as accurate as those obtained by the classical method of regressions on medical data [3].

Picture source: http://consiliummanagement.com/investment-management/

How to transform the intuition of many experts into one probability estimate?

This project has been running since 2014. It is a joint project between Alexandra Yu. Kalinichenko (SPb. Inform. and Analyt. Center), Dina Yu. Kalinichenko (SPbSU), Pavel A. Mozolyako (NTNU), Alexey V. Osipov (OLMA invest. comp.), Nikolai N. Osipov (NTNU and PDMI), and Dmitry V. Ponomarev (Inria).

Link:

CrowdMed project: http://www.crowdmed.com/

References:

[1] Lionel Page and Robert T. Clemen, Do prediction markets produce well-calibrated probability forecasts?, The Econom. J., Vol. 123, No. 568, 491–513, 2013

[2] Michèle Cohen, Security level, potential level, expected utility: a three-criteria decision model under risk, Theory and Decision, Vol. 33, No. 2, 101–134, 1992

[3] James K. Lindsey, Applying Generalized Linear Models, Springer Texts in Statistics, 2000

Please contact:

Nikolai N. Osipov
ERCIM research fellow, NTNU, Norway
E-mail: nicknick@pdmi.ras.ru

CyberROAD: Developing a Roadmap for Research in Cybercrime and Cyberterrorism

by Peter Kieseberg, Olga E. Segou and Fabio Roli

The CyberROAD project – a collaboration between several major European research institutions, companies and stakeholders - develops a European research roadmap for researching and fighting cybercrime and cyberterrorism.

Cybercrime and cyberterrorism represent a fundamental challenge for future societies, especially given the increasing pervasiveness of interconnected devices, such as home automation systems, connection of industrial systems to the Internet, the Internet of Things and simple commodity items in the area of wearable computing and the storage of private data in the cloud (see Figure 1). Public awareness of cybercrime has increased of late, owing to more frequent reports of online criminal and terrorist activity, as well as the increasing level of damage that can result from successful attacks. The damage caused by such activities in recent years is estimated to be large [1], although the actual figures are a subject of debate - which often becomes political. Current R&D activities in information and communication security do not address the problem at a global level, either in terms of the geographical coverage, or in terms of the involvement of all relevant stakeholders. CyberROAD bridges this gap by drawing together a wide network of expertise and experience, to address cybercrime and cyberterrorism from a broad perspective.

CyberROAD aims to identify the research gaps needed to enhance the security of individuals and society as a whole against forms of crime and terrorism conducted via and within cyberspace. This research addresses current technologies to some extent, but its main challenge is to anticipate tomorrow's world of interconnected living, in particular the dangers and challenges arising from the further incorporation of the digital world into our offline life, building atop initiatives such as [2].

We focus on the following fundamental questions:

- When does crime become cybercrime? When does terrorism become cyberterrorism? This separation is critical in order to identify the research questions that are specific to the cyber-environment, as opposed to the questions still unsolved in common (offline) crime and terrorism.
- How can we subdivide cybercrime and cyberterrorism into meaningful categories? This helps identify subclasses based on common attributes in order to rank the identified research gaps.
- What are the real economic and societal costs of cybercrime and cyberterrorism? As indicated in [2], the costs are often dramatically increased in political discussions. Objective and accurate figures are needed in order to accurately assess the importance of the identified research gaps.
- What are the major research gaps and what are the challenges that must be addressed?
- Once key research gaps have been identified, how do we pinpoint appropriate questions that need to be tackled by research projects? Appropriate approaches to research must be clearly defined.
- How can we test and evaluate security solutions, and to what extent can we test real solutions? Testing is critical in this area, but many challenges exist, especially when it comes to developing test beds for criminal environments and case studies in real life (criminal and terrorist) ecosystems.
- What economic, social, political and technological factors will foster cybercrime and cyber-terrorism? This question focusses largely on the influences of society and the availability of technologies on cyberspace, but also on the influence of cybercrime and cyberterrorism on the development, and especially suppression, of new technologies, which in turn lead to changes in society (see Figure 2) [3, pp. 15].

The main outcome of CyberROAD will be a research roadmap regarding the analysis and mitigation of cybercrime and cyberterrorism. This roadmap will be developed based on a gap analysis regarding future scenarios extrapolated

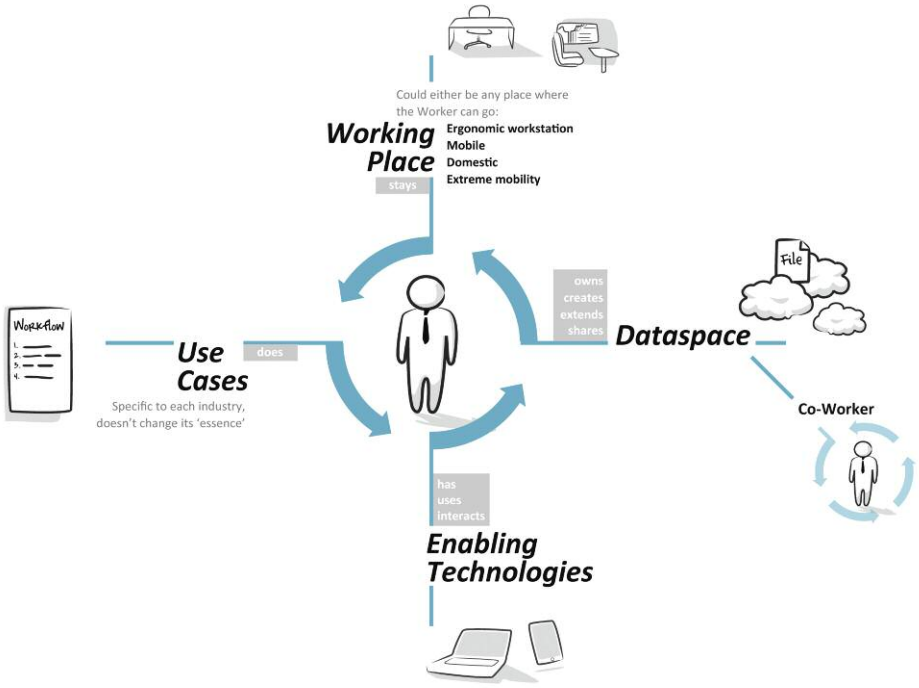


Figure 1: The integration of ICT into everyday life (by courtesy of Enrico Frumento, CEFRIEL • ICT Institute Politecnico di Milano).

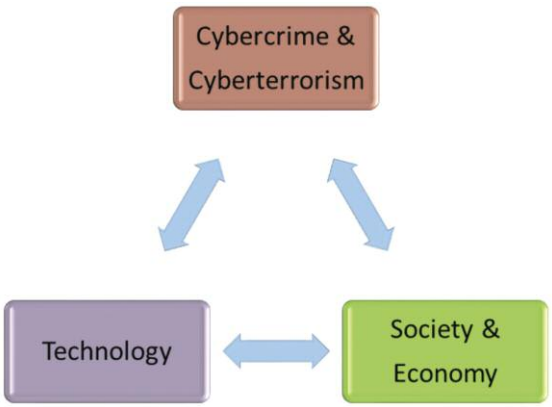


Figure 2: Technology, Society and Cybercrime/Cyberterrorism.

from the current state of technology and society, compared to the means of defence (legally) available to system owners and society as a whole. This includes conducting risk assessments for future and emerging technologies with respect to their impact in order to rank the importance of the identified research roadmap topics. While the main driver for the roadmap is the continuing penetration of society by new technology, the topics of ethics, privacy, law, society and fundamental rights are inextricably linked to this area and, as such, research questions relating to these issues are tightly incorporated into the project.

The identified roadmap items will serve as starting points for the development and setup of new projects, largely on a European level. CyberROAD will also serve as an incubator for enhancing the state of research regarding cybercrime, cyberterrorism and the underlying technological and societal variables.

The CyberROAD project has been running since June 2014 and is funded by the European Commission through the seventh framework programme. The project is led by the University of Cagliari and carried out by a team of 20 partners across Europe, ranging from (governmental) stakeholders to universities and private industrial partners.

Links:
http://www.cyberroad-project.eu/
The survey homepage: http://cyberroad.eu/

References
[1] R. Anderson, et al.: "Measuring the cost of cybercrime", The economics of information security and privacy", pp. 265-300, Springer, 2013.
[1] C. Wilson: "Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for congress", Library of Congress Washington DC congressional Research Service, 2008.
[2] J. Larosa, et. al. (2014). ERCIM White paper on Cybersecurity and privacy research, http://www.ercim.eu/images/stories/pub/white-paper-STM.pdf
[3] M. Yar, "Cybercrime and society", Sage, 2013.

Please contact:
Peter Kieseberg, SBA Research, Austria
E-mail: pkieseberg@sba-research.org

Exciting News from IFIP TC6: Open Publication is here!

by Harry Rudin

The IFIP (International Federation for Information Processing) Technical Committee 6 (TC6) held its spring 2015 meeting in Toulouse just before its 2015 Networking conference. At the meeting, the TC6 Chairman, Aiko Pras, announced continued progress with the TC6 open digital library: http://dl.ifip.org/. It is now truly operational.

TC6 deals with Communication Systems and organizes a number of conferences each year, one of them being "Networking". What is exciting is that the papers from the conference are freely available online: Have a look at http://dl.ifip.org/db/conf/networking/networking2015/index.html

Freely available means that no fee is charged for access: One needs neither to be a subscriber nor to pay a per paper access fee. It is also worth pointing out that the authors did not have to pay to have their papers published either.

At many TC6 conferences a best paper award is given. For the 2015 conference, out of the over 200 papers submitted, 48 papers were selected for presentation. The winner of the best paper award is "Information Resilience through User-Assisted Caching in Disruptive Content-Centric Networks" by Vasilis Sourlas, Leandros Tassiulas, Ioannis Psaras, and George Pavlou. Interested? Then just have a look at http://dl.ifip.org/db/conf/networking/networking2015/1570063627.pdf

The plans are to make open publishing available for all IFIP TC6 conferences. In the meantime, enjoy the papers already available!

Link:
http://dl.ifip.org/

Please contact:
Harry Rudin
Swiss Representative to IFIP TC6
E-mail: hrudin@sunrise.ch

Android Security Symposium

Vienna, 9-11 September 2015

This symposium brings together people from different backgrounds (academic, industry, rooting/exploiting community) who are interested in and actively working on Android device security. The event will feature exiting expert talks on topics around the Android security architecture, trusted computing concepts, usable security for everyone, malware analysis, and countermeasures. In addition there will be a PhD school where doctoral candidates get an opportunity to present their current research ideas. The symposium is an ideal platform to discuss current and upcoming security developments in Android and provides various networking opportunities.

Speakers include: N. Asokan (Aalto University, Finland), Andrew Hoog (NowSecure, USA), Joanna Rutkowska (Invisible Thing Lab, Poland), Nikolay Elenkov (Android Security Blogger, Japan), Federico Maggi (Politecnico di Milano, Italy) and Collin Mulliner (Northeastern University, USA).

The Android Security Symposium is funded by the Christian Doppler Forschungsgesellschaft (CDG) and organized by the Josef Ressel Center u'smile at the University of Applied Sciences Upper Austria in cooperation with SBA Research and the Institute of Networks and Security (INS) at Johannes Kepler University Linz. Attendance is free of charge.

More information:
https://usmile.at/symposium

Call for Participation

ICEC 2015 – International Conference on Entertainment Computing

Trondheim, Norway, 30 Septembe – 2 October, 2015

The IFIP International Conference on Entertainment Computing is the primary forum for disseminating and showcasing research results relating to the creation, development and use of digital entertainment. The conference brings together practitioners, academics, artists and researchers interested in design, practice, implementation, application and theoretical foundations of digital entertainment.

Topics

Papers, posters, demos, tutorials and workshop will cover all topics related to original research in digital entertainment, including but not limited to:

- Digital Games and Interactive Entertainment
- Design and Analysis
- Interactive Art, Performance and Novel Interactions
- Entertainment Devices, Platforms & Systems
- Theoretical Foundations and Ethical Issues
- Entertainment for Purpose & Persuasion
- Computational Methodologies for Entertainment

More information
http://icec2015.idi.ntnu.no/

Call for Participation

SAFECOMP 2015 and the ERCIM/ EWICS/ARTEMIS Workshop DECSoS

Delft, The Netherlands, 22-25 September 2015

Since it was established in 1979 by the European Workshop on Industrial Computer Systems, Technical Committee 7 on Reliability, Safety and Security (EWICS TC7), SAFECOMP has contributed to the progress of the state-of-the-art in dependable application of computers in safety-related and safety-critical systems. SAFECOMP is an annual event covering the experience and new trends in the areas of safety, security and reliability of critical computer applications. It provides ample opportunity to exchange insights and experience on emerging methods, approaches and practical solutions.

The 34th edition of SAFECOMP focuses on the challenges arising from networked multi-actor systems for delivery of mission-critical services. A particular area is that of medical technology which is meant to help patients and to support health care providers to deliver care and treatment while doing the patient no unintentional harm.

The already well-established ERCIM/ EWICSARTEMIS Workshop on Dependable Embedded Cyber-physical Systems and Systems-of-Systems" (DECSoS) of the ERCIM DES-Working Group, co-hosted by the ARTEMIS/ECSEL projects EMC², ARROWHEAD and CRYSTAL, takes place as a one-day workshop on 22 September 2015.

Links:
http://safecomp2015.tudelft.nl/
http://safecomp2015.tudelft.nl/decsos15

Please contact:
Erwin Schoitsch, Austrian Institute of Technology, Austria, and
Amund Skavhaug, NTNU
Co-chairs of the ERCIM DES Working Group and the 2015 DECSoS Workshop
E-mail: erwin.schoitsch@ait.ac.at, amund.skavhaug@ikt.ntnu.no

Call for Participation

Special Session "Teaching, Education and Training for Dependable Embedded Cyber-Physical Systems" at SEAA 2015

Funchal, Madeira, Portugal, 27 August 2015

A special session on "Teaching, Education and Training for Dependable Embedded Cyber-Physical Systems" (TET-DEC) will be held on 27 August as part of the Euromicro SEAA (Software Engineering and Avanced Applications) conference in Funchal, Madeira, Portugal, August 26 – 28, 2015. The Euromicro Conference series on Software Engineering and Advanced Applications (SEAA) is a long-standing international forum to present and discuss the latest innovations, trends, experiences, and concerns in the field of software engineering and advanced applications in information technology for software-intensive systems.

This workshop is co-organized by the ERCIM Working Group Dependable Embedded Systems and will provide some insight in education and training activities and outputs of European research projects and their partners, utilizing and exploiting research results for education & training in the area of dependable critical systems engineering.

Links:
http://paginas.fe.up.pt/~dsd-seaa-2015/seaa2015/
http://paginas.fe.up.pt/~dsd-seaa-2015/seaa2015/call-for-papers-seaa-2015/tet-dec-special-session/

Please contact:
Erwin Schoitsch, Austrian Institute of Technology, Austria, and
Amund Skavhaug, NTNU
Co-chairs of the ERCIM DES Working Group and the TET-DEC Special Session at SEAA 2015
E-mail: erwin.schoitsch@ait.ac.at, amund.skavhaug@ikt.ntnu.no

Call for Participation

ESORICS 2015 – 20th European Symposium on Research in Computer Security

Vienna, 21-25 September 2015

Computer security is concerned with the protection of information in environments where there is a possibility of intrusion or malicious action. The aim of ESORICS is to further the progress of research in computer security by establishing a European forum for bringing together researchers in this area, by promoting the exchange of ideas with system developers and by encouraging links with researchers in related areas.

Since its inception in 1990, ESORICS has been hosted in a series of European countries and has established itself as the premiere European research event in computer security.

This year the Symposium will be held at the Vienna University of Technology, on September 23-25, 2015. The following workshops will be held in conjunction with ESORICS 2015 on September 21-22, 2015:

- STM 2015, the 11th International Workshop on Security and Trust Management, organised by the ERCIM Working Group "Security and Trust Management".
- 10th DPM International Workshop on Data Privacy Management
- 4th International Workshop on 'Quantitative Aspects of Security Assurance' (QASA 2015)
- 2nd International Workshop on Security in highly connected IT Systems (SHCIS'15)
- International Workshop on Secure Internet of Things 2015 (SIoT 2015)
- 1st Workshop on the Security of Cyber-Physical Systems (WOS-CPS 2015)
- 1st Conference on Cybersecurity of Industrial Control Systems (CyberICS).

More information:
http://esorics2015.sba-research.org/

11th EUROPEAN COMPUTER SCIENCE SUMMIT

http://www.informatics-europe.org/ecss/ecss-2015.html

ECSS 2015

VIENNA, AUSTRIA | **12 > 14** OCTOBER

Source: www.pachd.com

Join leading decision makers in Informatics Research and Education to discuss the trends and issues that will shape the future of the discipline.

INFORMATICS IN THE FUTURE - IN THE YEAR 2025

KEYNOTE SPEAKERS

Jean-Pierre Bourguignon - ERC
Dirk Brockmann - Humboldt University
Stefano Ceri - Politecnico di Milano
Jeroen van den Hoven - Delft University of Technology
Maarja Kruusmaa - Tallinn University of Technology
Bertrand Meyer - ETH Zurich
Dunia Mladenić - Jozef Stefan Institute
Reinhard Posch - TU Graz
Britta Schinzel - University of Freiburg
Matti Tedre - Stockholm University
Moshe Vardi - Rice University

PRE-SUMMIT WORKSHOPS | 12 OCTOBER

- For Deans, Department Chairs and Research Directors
- Experiences and Practices in MOOCs

Conference Chairs	Program Chairs
Carlo Ghezzi - Politecnico di Milano	**Hannes Werthner** - TU Wien
Gerald Steinhardt - TU Wien	**Frank van Harmelen** - VU Amsterdam

ERCIM "Alain Bensoussan" Fellowship Programme

ERCIM offers fellowships for PhD holders from all over the world.

Topics cover most disciplines in Computer Science, Information Technology, and Applied Mathematics. Fellowships are of 12-month duration, spent in one ERCIM member institute. Fellowships are proposed according to the needs of the member institutes and the available funding.

Conditions

Applicants must:

- have obtained a PhD degree during the last 8 years (prior to the application deadline) or be in the last year of the thesis work with an outstanding academic record
- be fluent in English
- be discharged or get deferment from military service
- have completed the PhD before starting the grant.

In order to encourage mobility:

- a member institute will not be eligible to host a candidate of the same nationality.
- a candidate cannot be hosted by a member institute, if by the start of the fellowship, he or she has already been working for this institute (including phd or postdoc studies) for a total of 6 months or more, during the last 3 years.

The fellows are appointed for 12 months either by a stipend (an agreement for a research training programme) or a working contract. The type of contract and the monthly allowance (for stipends) or salary (for working contracts) depend on the hosting institute.

Application deadlines: 30 April and 30 September.

More information:
http://fellowship.ercim.eu/

Start of Lightning Explained: Hail and Cosmic Particles

For the first time researchers could explain how lightning starts: by a combination of hail and high energy particles from space, originating from exploding stars. This mechanism is modelled by researchers from the Multiscale Dynamics research group at CWI, together with colleagues from the University of Groningen and the Vrije Universiteit Brussel. The research was partly funded by the Technology Foundation STW and the Foundation for Fundamental Research on Matter (FOM) . The article "Prediction of lightning inception by large ice particles and extensive air showers" is published on 30 June in Physical Review Letters.

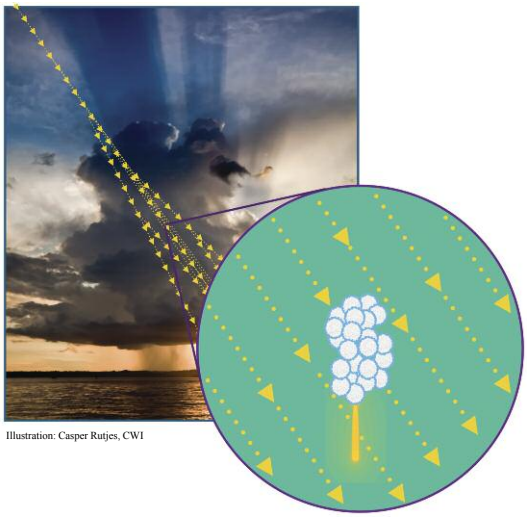


Illustration: Casper Rutjes, CWI

The start of lightning: a cosmic particle produces a particle shower, which generates free electrons. As soon as these electrons are available, a streamer discharge starts growing from a large hailstone, or an aggregate of graupel, where the electric field is amplified.

Ute Ebert (CWI and TU/e) says: "The start of lightning is highly complex because there are many processes unfolding at very different scales in space, time and energy. PhD students from my group, Anna Dubinova and Casper Rutjes, now calculated for the first time in detail how it works." The main challenges were that the electric field in a thundercloud is too low to start lightning, and that there are not enough free electrons available to start a discharge. In the new model, there are hail stones that are large and sharp enough to form high electric fields around their points. In addition, a particle shower in the atmosphere, caused by one energetic cosmic particle, makes sure there are plenty of free electrons available for the formation of lightning. If the particle shower enters the high electric field of the hail point, a streamer discharge begins to grow and lightning starts.

More information:
http://homepages.cwi.nl/~ebert

In Memoriam

Christos Nikolaou (1954-2015)

Prof. Christos Nikolaou passed away on April 30, 2015. Christos was a renowned researcher in the area of distributed systems and an enthusiastic teacher for more than three decades. He obtained a Ph.D. from Harvard University in 1982 and worked as a researcher and group leader at IBM T.J. Watson Research Center. He joined the faculty of the Department of Computer Science of the University of Crete in 1992 and served as Rector of the University from 1999 to 2004. During his term as Rector he implemented many innovative practices and reforms in the academic, administrative and student services domains. He undertook many initiatives that resulted in the ranking of the University of Crete in the top 100 young universities worldwide. Christos was also the head of the Pleiades Distributed Systems Group in the Institute of Computer Science of FORTH.

Christos was very active within the ERCIM Community. He served as the Chair of ERCIM's Executive Committee from 1995 to 1998. He led and participated in ERCIM projects in the area of Digital Libraries and established collaboration with several ERCIM institutes. He will be remembered as a visionary researcher, inspired teacher and tireless worker. He will be greatly missed by his friends and colleagues. The ERCIM Community expresses its sincere condolences to his family.

Building a Community around Linguistic Linked Data: The LIDER Project

In the last 18 months, the LIDER project has organized several roadmapping events to gather a broad community around the topic of linguistic linked data. In July this year, LIDER will engage with two selected communities. On 6 July, the 5th LIDER roadmapping workshop will be held in Rome at Sapienza University of Rome. The topic will be cross-media linked data and the event will provide several high level speakers from the multimedia area. On 13 July LIDER will organize the 6th roadmappping workshop in Munich. The event will be hosted by Siemens and will focus on content analytics and linked data in healthcare and medicine.

LIDER will finish end of October 2015, but the community will continue to be active in W3C, as the latter serves as the umbrella organization with an anchor in the Internationalization Activity and several related groups like Linked Data for Language Technologies (LD4LT), OntoLex or BPMLOD.

Links:
LIDER project: http://lider-project.eu/
W3C Internationalization Activity:
https://www.w3.org/International/

ERCIM
European Research Consortium for Informatics and Mathematics

ERCIM - the European Research Consortium for Informatics and Mathematics is an organisation dedicated to the advancement of European research and development, in information technology and applied mathematics. Its member institutions aim to foster collaborative work within the European research community and to increase co-operation with European industry.

ERCIM is the European Host of the World Wide Web Consortium.

Consiglio Nazionale delle Ricerche
Area della Ricerca CNR di Pisa
Via G. Moruzzi 1, 56124 Pisa, Italy
http://www.iit.cnr.it/

Norwegian University of Science and Technology
Faculty of Information Technology, Mathematics and Electrical Engineering, N 7491 Trondheim, Norway
http://www.ntnu.no/

Czech Research Consortium
for Informatics and Mathematics
FI MU, Botanicka 68a, CZ-602 00 Brno, Czech Republic
http://www.utia.cas.cz/CRCIM/home.html

SBA Research gGmbH
Favoritenstraße 16, 1040 Wien
http://www.sba-research.org

Centrum Wiskunde & Informatica
Science Park 123,
NL-1098 XG Amsterdam, The Netherlands
http://www.cwi.nl/

SICS Swedish ICT
Box 1263,
SE-164 29 Kista, Sweden
http://www.sics.se/

Spanish Research Consortium for Informatics and Mathematics
D3301, Facultad de Informática, Universidad Politécnica de Madrid
28660 Boadilla del Monte, Madrid, Spain,
http://www.sparcim.es/

Fonds National de la Recherche
6, rue Antoine de Saint-Exupéry, B.P. 1777
L-1017 Luxembourg-Kirchberg
http://www.fnr.lu/

Science and Technology Facilities Council
Rutherford Appleton Laboratory
Chilton, Didcot, Oxfordshire OX11 0QX, United Kingdom
http://www.scitech.ac.uk/

FWO
Egmontstraat 5
B-1000 Brussels, Belgium
http://www.fwo.be/

F.R.S.-FNRS
rue d'Egmont 5
B-1000 Brussels, Belgium
http://www.fnrs.be/

Magyar Tudományos Akadémia
Számítástechnikai és Automatizálási Kutató Intézet
P.O. Box 63, H-1518 Budapest, Hungary
http://www.sztaki.hu/

Foundation for Research and Technology - Hellas
Institute of Computer Science
P.O. Box 1385, GR-71110 Heraklion, Crete, Greece
http://www.ics.forth.gr/

University of Cyprus
P.O. Box 20537
1678 Nicosia, Cyprus
http://www.cs.ucy.ac.cy/

University of Geneva
Centre Universitaire d'Informatique
Battelle Bat. A, 7 rte de Drize, CH-1227 Carouge
http://cui.unige.ch

Fraunhofer ICT Group
Anna-Louisa-Karsch-Str. 2
10178 Berlin, Germany
http://www.iuk.fraunhofer.de/

University of Southampton
University Road
Southampton SO17 1BJ, United Kingdom
http://www.southampton.ac.uk/

INESC
c/o INESC Porto, Campus da FEUP,
Rua Dr. Roberto Frias, nº 378,
4200-465 Porto, Portugal

Universty of Warsaw
Faculty of Mathematics, Informatics and Mechanics
Banacha 2, 02-097 Warsaw, Poland
http://www.mimuw.edu.pl/

Institut National de Recherche en Informatique
et en Automatique
B.P. 105, F-78153 Le Chesnay, France
http://www.inria.fr/

Universty of Wroclaw
Institute of Computer Science
Joliot-Curie 15, 50–383 Wroclaw, Poland
http://www.ii.uni.wroc.pl/

I.S.I. - Industrial Systems Institute
Patras Science Park building
Platani, Patras, Greece, GR-26504
http://www.isi.gr/

VTT Technical Research Centre of Finland Ltd
PO Box 1000
FIN-02044 VTT, Finland
http://www.vttresearch.com