

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

Flavio Oquendo, Axel Legay, Khalil Drira

► **To cite this version:**

Flavio Oquendo, Axel Legay, Khalil Drira. GT SoS: Research Network on Trustworthy Software-intensive Systems-of-Systems. ERCIM News, ERCIM, 2015. <hal-01242651>

**HAL Id: hal-01242651**

**<https://hal.inria.fr/hal-01242651>**

Submitted on 4 Feb 2016

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

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

Flavio Oquendo, Axel Legay and Khalil Drira

July 2015

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 con-

stituent 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 unpredictable 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.

**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 (tude prospective sur les technologies cls 2015-2025, Direction Gnrale de la Comptitivit, de lIndustrie et des Services du Ministre de lEconomie). 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



Figure 1: Systems-of-Systems - A digital agenda for Europe (source: <https://ec.europa.eu/digital-agenda/en/system-systems/>).

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 Rhne-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 Scurit, 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] Mohammad Jamshidi (Ed). *System of Systems Engineering: Innovations for the Twenty-First Century*. Wiley, 2008.
- [2] Flavio Oquendo et. al. (Eds). *Software Engineering for Systems-of-Systems*. ACM, 2013.