1st International Workshop on Multi-concern Assurance Practices in Software Design (MAPSOD 2021)

1st International Workshop on Multi-concern Assurance Practices in Software Design (MAPSOD 2021)

Jason Jaskolka[1], Brahim Hamid[2], and Sahar Kokaly[3]

[1] Systems and Computer Engineering, Carleton University, Ottawa, ON, Canada
jason.jaskolka@carleton.ca
[2] IRIT, University of Toulouse, Toulouse, France
brahim.hamid@irit.fr
[3] General Motors, Markham, ON, Canada
sahar.kokaly@gm.com

1 Introduction

Complex software systems have become increasingly entwined in a wide variety of systems such as critical infrastructure, industrial control systems, medical devices, automobiles, airplanes, and spacecraft. Assuring the security and safety, as well as other dependability aspects such as availability, robustness, and reliability, of these software-intensive systems remains among the top priorities for governments and providers of critical systems and services. Manufacturers, owners, and operators of the components and devices that make up these software systems strive to ensure that they have adequately addressed emerging concerns related to safety hazards, security threats, and performance challenges, among others. For this reason, there is a need to address these various concerns within the architecture and design of these systems in the context of the subjective and often contradicting, competing, and conflicting needs and beliefs of stakeholders, and to do so with a level of confidence that is commensurate with the tolerable loss consequences associated with each of these objectives.

2 This Year's Workshop

This is the first edition of the MAPSOD workshop co-located at SAFECOMP 2021. MAPSOD 2021 is centred on rethinking the concept of assurance and certification, taking into account the nature and the full range of design concerns of software-intensive systems. The topics provide coverage of architecture and design trends supporting multi-concern assurance of software-intensive systems of high relevance to software practitioners. Special emphasis has been devoted to promoting discussion and interaction between researchers and practitioners focused on addressing concerns related to safety, security, reliability, availability, and robustness within the architecture and design of software-intensive systems.

The workshop comprised three presentations:

1. An Accountability Approach to Resolve Multi-stakeholder Conflicts, by Yukiko Yanagisawa and Yasuhiko Yokote.
   This paper presents an approach to resolve conflicts among multiple stakeholders based on the notion of an accountability map. The approach involves identifying events requiring accountability and the risks that come from conflicting stakeholder viewpoints and claims to incorporate the recommendations from IEC 62853. It also involves describing the resolution procedures to support various risk responses.
2. Architecture-Supported Audit Processor: Interactive, Query-Driven Assurance, by Sam Procter and Jerome Hugues.
   This paper presents an interactive tool called the Architecture-Supported Audit Processor (ASAP). ASAP focusses on system safety and extracts safety-specific viewpoints from system architecture models expressed using AADL. The viewpoints are dynamically generated as diagrams and tables. Using these viewpoints, the paper discusses integrations with Systematic Analysis of Faults and Errors (SAFE) and System Theoretic Process Analysis (STPA).
3. Towards Assurance-Driven Architectural Decomposition of Software Systems, by Ramy Shahin.
   The paper discusses the limits of using abstraction techniques to handle the complexity of computer systems from design and analysis perspectives. The proposed approach combines three architectural views (computation, coordination, stateful) and a meta-programming envelope to decompose software systems. The resulting 4-dimension meta-architecture allows the capture of assurance expectations, early on in the design stage. The proposed decomposition method contributes to the reconciliation between the two different visions, cultures, and the produced artifacts related to SDLC and assurance activities.

The program was completed with a keynote talk given by Barbara Gallina (Mälardalen University) on “Multi-concern Assurance: Current Practices, Challenges, and Ways Forward”. Moreover, the workshop closed with a discussion session about the future of the workshop.

3 Acknowledgements

As chairpersons of the workshop, we want to thank all authors and contributors who submitted their work, Friedemann Bitsch, the SAFECOMP publication chair, Simos Gerasimou and Erwin Schoitsch, the SAFECOMP workshop co-chairs, and the members of the International Program Committee who provided a fair and thorough evaluation through reviews of the submitted papers. We extend our thanks to the SAFECOMP organizers, and their chairperson John McDermid, who provided us the opportunity to organize the workshop at SAFECOMP 2021 as an online event.

It is our sincerest hope that all participants will enjoy and benefit from the workshop and will join it again in the future!

International Program Committee

Morayo Adedjouma	CEA LIST, France
Marsha Chechik	University of Toronto, Canada
Eduardo B. Fernandez	Florida Atlantic University, USA
Barbara Gallina	Mälardalen University, Sweden
Mallory Graydon	National Aeronautics and Space Administration, USA
Ibrahim Habli	University of York, UK
Brahim Hamid	IRIT – University of Toulouse, France
Jason Jaskolka	Carleton University, Canada
Sahar Kokaly	General Motors, Canada
Thierry Lecomte	ClearSy, France
Shiva Nejati	University of Ottawa, Canada
Richard Paige	McMaster University, Canada
Sam Procter	SEI – Carnegie Mellon University, USA
Ramesh S.	General Motors R&D, USA
Genaina Rodrigues	University of Brasilia, Brazil
Mehrdad Sabetzadeh	University of Ottawa, Canada
Irfan Sljivo	KBR/NASA Ames Research Center, USA