SASSUR 2023

10th International Workshop on Next Generation of System Assurance Approaches for Critical Systems

19 September 2023, Toulouse, France

Held in conjunction with SAFECOMP 2023 - 42nd International Conference on Computer Safety, Reliability and Security

For further details: see https://sites.google.com/view/sassur2023/

System assurance and certification are amongst the most expensive and time-consuming tasks in the development of critical systems, e.g., safety-critical, security-critical, privacy-critical, explainability-critical, mission-critical, and business-critical ones. Assurance can be defined as the set of planned and systematic actions necessary to provide adequate confidence and evidence that a system satisfies given requirements, e.g., for system safety or for compliance with some standards. Certification can be defined as the legal recognition that a system complies with standards and regulations designed to ensure that the system can be depended upon to deliver its intended service.

Assurance and certification of critical systems require the execution of complex and labour-intensive activities, e.g., the management of compliance with hundreds or thousands of criteria defined in standards, the management of a large volume of evidence artefacts throughout a system's lifecycle to demonstrate compliance, or the provision of convincing and valid justifications that a system is dependable. Therefore, the companies developing critical systems or components, as well as the companies assessing the systems and components, need approaches that facilitate these activities and ideally increase their efficiency. In addition, re-certification is usually required for any evolution of the system. The challenges arising from system assurance and certification are further growing as a result of the technological advancements of critical systems. For example, embedded systems have significantly increased in number, technical complexity, and sophistication towards open, interconnected, networked, intelligent systems such as "the connected car". This has brought a "cyber-physical" and an autonomy dimension with it, exacerbating the problem of ensuring safety, as well as other dependability concerns such as security, availability, robustness, and reliability, in the presence of human, environmental, and technological risks. Privacy is also a major concern for systems managing personal or sensitive data. The rise of notions such as cyber-physical and autonomous systems and their complexity are leading to the need for new approaches for system assurance and certification. In general, practitioners expect improvements in the available methods and tool support for assurance and certification.

The SASSUR workshop is intended to explore new ideas on assurance and certification of critical systems. In particular, SASSUR will provide a forum for thematic presentations and in-depth discussions about specification, analysis, reuse, composition, and combination of assurance arguments, of assurance evidence, and of contextual information about critical products, in a way that makes assurance and certification more cost-effective, precise, and scalable.

SASSUR aims at bringing together experts, researchers, and practitioners from diverse communities, such as safety, privacy, and security engineering the recently coined explainability engineering, certification processes, model-based engineering, software and hardware design, critical systems, and application communities (transport, healthcare, industrial automation, robotics, nuclear, defence, etc.).

SASSUR 2023 is co-located with the SAFECOMP 2023 conference.

Authors are invited to submit short papers (6 pages) or full paper (max. 12 pages) in PDF format using Easychair: https://easychair.org/conferences/?conf=sassur2023

Submissions must conform to the Springer LNCS formatting guidelines (https://www.springer.com/gp/computer-science/lncs/editor-guidelines-for-springer-proceedings). Papers will be peer-reviewed through a regular refereeing procedure, with a minimum of three reviewers per paper. If accepted for presentation, the papers will be published in the SAFECOMP 2023 Workshops proceedings (LNCS series in the last years).

At least one author of each accepted paper must register to the workshop so that the paper is included in the proceedings.

The **important dates** are:

- Paper submission: 2 May 2023
- Notification of acceptance: 25 May 2023
- Camera-ready submission: 5 June 2023
- Workshop: 19 September 2023

The workshop is supported by the iRel40, REBECCA, and VALU3S EU projects, the ETHEREAL Spanish national project, and the 4DASafeOps and ET4CQPPAJ Swedish projects (Software Center)