ASSURE 2023

8th International Workshop on Assurance Cases for Software-intensive Systems

Call for Papers

Software plays a key role in high-risk systems, e.g., safety and security-critical systems. Assurance cases have been recommended or mandated for software-intensive systems in a number of domains, and are a promising way forward for assurance of autonomous systems. The goals of the 2023 Workshop on Assurance Cases for Software-intensive Systems (ASSURE 2023) are to:

- explore techniques for creating and assessing assurance cases for software-intensive systems, especially those enabling autonomy, including structured argumentation, graphical notations, narrative forms, etc.
- examine the role of assurance cases in the engineering lifecycle of critical systems;
- identify the dimensions of effective practice in the development and evaluation of assurance cases;
- investigate the relationship between dependability techniques and assurance cases; and,
- identify critical research directions, define a roadmap for future development, and formulate challenge problems.

The workshop will be hybrid, and run on Central European Time (CET).

We solicit high-quality contributions (research, practice, tools, and position papers) on the application of assurance case principles and techniques to assure that the dependability properties of critical software-intensive systems have been met. ASSURE 2023 additionally solicits papers that contain new, forward-looking, ideas with emerging results and concrete plans for comprehensive empirical validation, works-in-progress, as well as reflections that examine current research under a new lens, calling for future research directions. Papers should attempt to address the workshop goals in general.

Topics of interest include, but are not limited to:

- **Assurance issues in emerging paradigms**, e.g., autonomous and AI-based systems, including self-driving cars, unmanned aircraft systems, complex health care and decision making systems, etc.
- **Standards:** Industry guidelines and standards are increasingly requiring the development of assurance cases, e.g., the automotive standard ISO 26262, the FDA guidance on the total product life cycle for infusion pumps and the OMG standard on argumentation (Structured Assurance Case Metamodel, SACM).
- **Certification and Regulations:** The role and usage of assurance cases in the certification of critical systems, as well as to show compliance to regulations.
- **Empiricism** Empirical assessment of the applicability of assurance cases in different domains and certification regimes.
- **Dependable architectures**: How do fault-tolerant architectures and design measures such as diversity and partitioning relate to assurance cases?
- **Dependability analysis:** What are the relationships between dependability analysis techniques and the assurance case paradigm?
- **Safety and security co-engineering:** What are the impacts of security on safety, particularly safety cases and how can safety and security cases (e.g., as proposed in ISO 26262 and J3062 respectively) be reconciled?
- **Tools:** Using the output from software engineering tools (testing, formal verification, code generators) as evidence in assurance cases / using tools for the modeling, analysis and management of assurance cases. More generally, the role of formal verification in the wider context of assurance.
- **Application of formal techniques** for the creation, analysis, reuse, and modularization of arguments. Exploration of relevant techniques for assurance cases for real-time, concurrent, and distributed systems.

- **Assurance of software quality attributes**, e.g., safety, security and maintainability as well as dependability in general, including tradeoffs, and exploring notions of the quality of assurance cases themselves.
- **Domain-specific assurance issues**, in domains such as aerospace, automotive, healthcare, defense and power.
- **Reuse and Modularization:** Contracts and patterns for improving the reuse of assurance case structures.
- **Relations between different formalisms** and paradigms of assurance and argumentation, such as Goal Structuring Notation, STAMP, IBIS, and goal-oriented formalisms such as KAOS.

Submission Guidelines

Papers will be peer-reviewed by at least 3 program committee members, and accepted papers will be published in the SAFECOMP 2023 Workshop proceedings, to be published by Springer in the Lecture Notes in Computer Science (LNCS) series.

- All papers must be original work not published, or in submission, elsewhere. Submission will be via EasyChair: https://easychair.org/conferences/?conf=assure2023
- Papers should be submitted in PDF only. Please verify that papers can be reliably printed and viewed on screen before submission.
- Papers should conform to the LNCS paper formatting guidelines: http://www.springer.com/computer/lncs?SGWID=0-164-6-793341-0
    - Regular (research, or practice), Tools, and Experience papers can be up to 10 pages, including figures, references, and any appendices. Note that authors of accepted tools papers will be expected to give a demonstration of the tool(s) at the workshop. Papers describing the experience of an organization in developing assurance cases are particularly welcome.
    - Position papers, and papers presenting new ideas, works-in-progress, and emerging results can be 6 pages, including figures, references, and any appendices.

Important Dates	Paper submission	2 May 2023
	Author notification	25 May 2023
	Camera-ready papers	5 June 2023
	Workshop	19 September 2023

Organizers	Ewen Denney	KBR / NASA Ames, USA
	Ibrahim Habli	University of York, UK
	Ganesh Pai	KBR / NASA Ames, USA