Paper Submission: May 22, 2018 • Author Notification: June 4, 2018 • Camera-ready Papers: June 18, 2018

Call for Papers

Software plays a key role in high-risk systems, e.g., safety and security-critical systems. A number of certification standards/guidelines now recommend and/or mandate the development of assurance cases for software-intensive systems, e.g., defense (UK MoD DS-0056), aviation (CAP 670, FAA's operational approval guidance for unmanned aircraft systems), automotive (ISO 26262), and healthcare (FDA infusion pumps total product lifecycle guidance). As such, there is a need to develop models, techniques and tools that target the development of assurance arguments for software.

The goals of the 2018 Workshop on Assurance Cases for Software-intensive Systems (ASSURE 2018) are to:

- explore techniques for creating/assessing assurance cases for software-intensive systems;
- 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.

We solicit high-quality contributions (research, practice, tools, and position papers) on applying assurance case principles and techniques to assure that the dependability properties of critical software-intensive systems have been met.

Topics

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., adaptive and autonomous 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 and the FDA guidance on the total product lifecycle for infusion pumps.
- **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.
- **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.

Paper Submission: May 22, 2018 • Author Notification: June 4, 2018 • Camera-ready Papers: June 18, 2018

Submission Guidelines

Papers will be peer-reviewed by at least 3 program committee members, and accepted papers will be published in the SAFECOMP 2018 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.
- 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.
  - Regular (research, or practice) papers as well as Tools papers can be up to 8 pages long, 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.
  - Position papers (relating to ongoing work or proposed aspects of challenge problems) can be between 4 and 6 pages long, including figures, references, and any appendices.

Submit your paper electronically by May 22, 2018, through the workshop website:
http://ti.arc.nasa.gov/event/assure2018/

Workshop Organizers

Ewen Denney, SGT / NASA Ames Research Center, USA
Ibrahim Habli, University of York, UK
Richard Hawkins, University of York, UK
Ganesh Pai, SGT / NASA Ames Research Center, USA