# Call for Papers: Theme Issue on Formal Methods at Scale

## IEEE S&P seeks submissions for this upcoming issue.

Formal methods (FM) have a rich history spanning a half-century. Mathematical proof of properties of programs have been sought since the early days of computing. Despite these aspirations, FM has not taken hold due to barriers of scale, usability, engineering realism, and mission incentives. Indeed, for decades, FM tools and ecosystems could only operate on problems and systems of modest scale. There has nonetheless been strong impetus to continue the advance of FM driven by emerging uses of computing hardware and software in critical systems such as space and aircraft flight control, communication security, and cryptography. Recently, however, FM has advanced to the point that techniques are breaking through the barriers and being adopted in a broader range of engineering organizations where reliability and assurance are highly critical, particularly in cloud infrastructure, operating system kernels, and other applications. This is timely, because assurance needs are ramping up due to the growing sophistication of modern cyber threats, as well as the increase in complexity and interconnection of systems. Indeed, many of the modern applications of FM address scale and interconnection challenges through emphasis on composition, integration with modern tooling, and better accessibility for mainstream software developers, including invisible FM, where FM-originated techniques are built in to languages and tools in ways that yield the benefits while nonetheless “hiding the math” from developers.

This special issue of IEEE Security & Privacy aims at understanding how the FM community, working in partnership with sponsors and users, is achieving broader use of this critical technology and at increasing levels of scale. Still further, this special issue seeks to present this discussion in a form accessible to a general audience of researchers and practitioners thereby increasing the understanding of the community around FM. In the long history of FM, we have experienced both major steps forward and also some crises of expectations. Some have suggested that we might be at a new inflection point–and so it is important to consider the landscape. Topics include, but are not limited to:

- Dimensions of scale, to include
    - The range of properties and qualities that are modeled and reasoned about, such as relating to security, safety, performance, fault tolerance, and real-time;
    - Complexity and the size of systems and their supply chains, including issues related to composability;
    - Efficiency of FM-related modeling, tooling, and engineering practices, including integration into mainstream tooling and practices;
    - Ability to rapidly co-evolve systems and associated evidence; and

    - Ease of use for non-expert developers and evaluators.
- Dimensions of experience, to include
    - Experiences that can help ground our conversation and help us understand cross-cutting considerations such as commonalities in technical foundations and challenges relating to adoption into practice and tooling;
    - Applications to specific major systems in government and industry;
    - Tour-de-force results, such as proofs of significant mathematical results or reasoning about modern processors;
    - Advancement of FM ecosystems surrounding the various provers and stacks; and
    - Integration of more limited capabilities into broader communities of practice, such as has been happening in major tech firms.

## Important Dates

**Submissions due**: 30 November 2021
Publication: May/June 2022

## Submission Guidelines

For author information and guidelines on submission criteria, please visit the Author Information page. Please submit papers through the ScholarOne system, and be sure to select the special-issue name. Manuscripts should not be published or currently submitted for publication elsewhere. Please submit only full papers intended for review, not abstracts, to the ScholarOne portal.

## Guest Editors

Contact the guest editors at sp3-22@computer.org.

- Patrick Lincoln, SRI, Director CSL
- William “Brad” Martin, DARPA, I2O PM
- William Scherlis, DARPA, I2O Director

---

Articles should run between 4,900 to 7,200 words, including all main body, abstract, keyword, bibliography, biography, and table text. The word count should include 250 words for each table and figure. There should be no more than 15 references. The abstract word limit is 50 words.

Submissions will be subject to the peer-review methodology for refereed papers. Articles should be understandable to a broad audience of people interested in security and privacy. The writing should be down to earth, practical, and original. Authors should

not assume that the audience will have specialized experience in a particular subfield. All accepted articles will be edited. As this is not a research journal, please **do not submit** research papers.

**Before submitting, please read our author guidelines.** When you are ready to submit, please go to https://mc.manuscriptcentral.com/sp-cs.