Springer

Call for Papers

Editors

Jingsha He
jsh.bjut@gmail.com
Beijing University of Technology, China

Tao Yue
yuetao@buaa.edu.cn
Beihang University
China

Iulian Ober
iulian.ober@isae.fr
ISAE-Supaero
France

Geylani Kardas
geylani.kardas@ege.edu.tr
Ege University
Turkey

Important Dates

Intent to submit	01-Oct-2026
Paper submission	01-May-2027
Notification	01-Oct-2027

Theme Section:
Model-Driven Engineering for Security and Adaptability in Intelligent Systems

Intelligent systems—such as autonomous vehicles, industrial robots, and AI-driven decision-support systems—are increasingly deployed in open, dynamic, and sometimes adversarial environments. Their increasing autonomy, connectivity, and operational complexity create new engineering challenges. These systems face security threats such as unauthorized access, data tampering, sensor spoofing, and service disruption, which can compromise the confidentiality, integrity, or availability of system assets and operations. Meanwhile, adaptability is required to accommodate component changes, varying operating conditions, evolving requirements, and uncertain environments, but is often constrained by fixed system configurations. Many existing engineering approaches treat security as a late-stage concern and adaptability as an add-on capability. This separation can make it difficult to analyze trade-offs, maintain assurance, and ensure that adaptation decisions do not introduce new vulnerabilities. Engineering intelligent systems that can respond to changing conditions and emerging threats without extensive redesign therefore remains a significant challenge.

Model-Driven Engineering (MDE) provides a systematic foundation for addressing this challenge. MDE raises the level of abstraction beyond implementation-level code and configuration artifacts by using models of system architecture, behavior, requirements, and deployment environments as central engineering artifacts. Models can make security properties, adaptation goals, contextual assumptions, and configuration constraints explicit and analyzable. Model-based analysis and verification techniques can support the early identification of inconsistencies, undesirable interactions, and potential vulnerabilities. Model transformations and generative techniques can facilitate the systematic derivation of security mechanisms, adaptation logic, tests, and implementation artifacts from higher-level specifications. Runtime models and feedback loops can further support online monitoring, adaptation planning, and dynamic reconfiguration as the system or its environment evolves. Models also provide shared and traceable representations of security requirements and adaptation decisions throughout the system lifecycle.

This theme section focuses on modeling languages, model-based analysis methods, model transformations, runtime models, and tool-supported engineering processes for integrating security and adaptability in intelligent systems. It invites original research, rigorous empirical studies, tool-supported approaches, and industrial experience reports that advance the specification, design, analysis, implementation, and runtime evolution of secure and adaptive intelligent systems.

The *Journal of Software and Systems Modeling* (SoSyM) invites original, high-quality submissions for its theme section on "Model-Driven Engineering for Security and Adaptability in Intelligent Systems" focusing on topics including:

- **Modeling foundations and requirements:** formal foundations, domain-specific modeling languages, and metamodels for security and adaptability; model-based elicitation and specification of security, adaptation, and assurance requirements.
- **Model-based analysis and assurance:** threat and vulnerability modeling; verification and validation of secure and self-adaptive systems; analysis of trade-offs, uncertainty, consistency, and interactions between security constraints and adaptation decisions.
- **Design, transformation, and artifact generation:** model-driven design of secure and adaptive mechanisms; model composition, refinement, and transformation; generation of security mechanisms, adaptation logic, tests, and code artifacts from models.
- **Runtime models and adaptive coordination:** runtime models and feedback loops for monitoring, adaptation planning, and dynamic reconfiguration; model-based coordination and trust management in distributed and multi-agent intelligent systems; traceability and co-evolution of design-time and runtime models.
- **Scalable methods, tools, and empirical evidence:** lightweight and scalable modeling techniques for resource-constrained and large-scale systems; modeling and analysis tool environments; benchmarks, industrial case studies, rigorous empirical evaluations, and experience reports involving autonomous, robotic, cyber-physical, IoT, and AI-enabled software systems.

General Author Information

- Papers must be written in a scientifically rigorous manner with adequate references to related work.
- Submitted papers must not be simultaneously submitted in an extended form or in a shortened form to other journals or conferences. It is however possible to submit extended versions of previously published work if less than 75% of the content already appeared in a non-journal publication, or less than 40% in a journal publication. Please see the SoSyM Policy Statement on Plagiarism for further conditions.
- Submitted papers do not need to adhere to a particular format or page limit. Please consult the SoSyM author information for submitting papers for more details.
- Each paper will be reviewed by at least three reviewers.

Making a submission

- Communicate your intent to submit a paper by emailing the theme section editors the following information before the Intent to Submit deadline: Title, Authors, and an Abstract.
- Possible submission formats are:
  - Word (.doc, without macros)
  - Rich Text Format (.rtf)
  - PostScript (.ps, special fonts must be embedded)
  - PDF (saved as readable in version 5.0 or earlier)
- Submit your work using the online submission system manuscript central:
  - In step 1, select "Theme Section Paper" as the manuscript type.
  - In step 5, make sure field "Cover Letter" includes the line: "Submission for Theme Section on Model-Driven Engineering for Security and Adaptability in Intelligent Systems".

Further information

If you have any questions or require additional information about this theme section, please contact the editors.