IEEE Control Systems Letters (L-CSS)

Call for submissions to the L-CSS Special Section "Enhancing Trustworthiness of Cyber-Physical Systems"

The L-CSS invites submissions for a Special Section entitled **"Enhancing Trustworthiness of Cyber-Physical Systems"** (to be included, tentatively, in the 2026 volume of L-CSS). Authors are invited to submit **six-page** manuscripts for review on this topic. Submission for this Special Section will be possible starting on **May 4, 2026** until **June 5, 2026**.
Submission instructions can be found on the L-CSS website at the following webpage: https://ieee-cssletters.uniroma2.it/Page_authors.php?p=1 .

Guest Editors

- Daniela Selvi (Leading Proposer) – Politecnico di Milano
- Antoine Girard (L-CSS Senior Editor) – CNRS, CentraleSupélec, Université Paris-Saclay
- Mahdieh S. Sadabadi – The University of Manchester
- Cédric Escudero – INSA Lyon
- Sadegh Soudjani – University of Birmingham & MPI-SWS
- Walter Lucia – Concordia University

The growing interconnection and complexity of engineered systems, driven by advances in autonomy, intelligent control, and machine learning, have transformed modern life. Cyber-Physical Systems (CPS) have undoubtedly played a key role within this transformation, enabling applications such as autonomous vehicles, intelligent transportation networks, smart medical devices, smart grids, and industrial automation. While this tight integration of computation, communication, and control has increased efficiency and functionality, it has also expanded CPS' exposure to faults, safety hazards, specification violations, and cyberattacks. In safety-critical CPS, minor design errors, software bugs, or unexpected environmental interactions can lead to catastrophic failures. Additionally, the widespread data exchange across distributed components heightens the risk of unauthorized access, data manipulation, and system disruption by malicious actors. Finally, as CPS increasingly rely on neural networks and learning-based components, they become susceptible to new classes of threats that target these data-driven modules.

These challenges call for advanced control solutions and rigorous methods to ensure safety, security, and reliability throughout the system lifecycle while keeping pace with increasingly scaled and autonomous systems. Understanding system failures, attack

strategies, unintended behaviors, and propagation of uncertainties is critical not only for timely detection but also for developing preventive and mitigation strategies. As perfect protection against faults or attacks is unattainable in practice, resilience must be explicitly incorporated into the control design requirements, for example by including formal verification and validation techniques, fault-tolerant strategies, and secure-by-design architectures that can guarantee an adaptive and correct operation even under adversarial conditions or partial system degradation.

The aim of this Special Section is to present recent advances and emerging research directions within the Control Systems community for enhancing the trustworthiness of CPS. Particular focus is on solutions in the areas of control, estimation, information fusion, and machine learning for improving safety, resilience, and privacy of highly-interconnected systems, and further bridging the gap between theory and real-world deployment.

Topics of interest include, but are not limited to:

- Secure and resilient control, estimation, and sensor fusion
- Network and control reconfiguration under failures or adversarial conditions
- Safety analysis, verification, validation, and formal methods for trustworthy learning-enabled CPS
- Fault/attack detection, prevention, and mitigation strategies
- Privacy-preserving control, estimation, and communication over networked systems
- Resilience and performance metrics under uncertainty and adversarial action in networked and distributed control systems
- Adversarial attacks and defenses for neural network controllers
- Applications to autonomous systems, transportation, robotics, power & energy systems, manufacturing, and healthcare

Manuscripts submitted to the Special Section must strictly follow the author guidelines of the IEEE L-CSS and will be reviewed according to the journal's policy. In particular, according to this policy, all submitted articles will be pre-screened to evaluate the manuscript's adequacy for the journal and the Special Section. Please note that substandard or out-of-scope manuscripts will not be reviewed. Manuscripts having passed the pre-screening phase will be peer-reviewed by international experts, and the final decision will be communicated to the authors within two rounds of review. In addition, all manuscripts must be written in the L-CSS **six-pages two-column** journal format; please refer to the “Guidelines for Authors” on the above-mentioned web link for details regarding the submission procedure.

Only for Special Sections Authors are allowed to provide a brief document as supplementary material (e.g., videos, additional examples and simulations, brief appendices showing non-essential parts of a mathematical derivation), but according to the journal policy only the contents of the main six-page manuscript will be evaluated and considered in the publication decision. That is, supplementary material is to be considered only as support, but the 6 page manuscript must be self-contained relative to the main contribution. Note that the need for compactness complies with the limited time allocated to reviewers.