Research Directions: Cyber-Physical Systems

www.cambridge.org/cbp

Can we develop holistic approaches to delivering cyber-physical systems security?

John Fitzgerald and Charles Morisset

School of Computing, Newcastle University, Newcastle upon Tyne, UK

Question

Cite this article: Fitzgerald J and Morisset C (2024). Can we develop holistic approaches to delivering cyber-physical systems security? *Research Directions: Cyber-Physical Systems*. **2**, e2, 1–2. https://doi.org/10.1017/cbp.2024.1

Received: 2 April 2024
Accepted: 9 April 2024

Corresponding author:
John Fitzgerald;
Email: john.fitzgerald@newcastle.ac.uk

Context: Holistic CPS security

Cyber-Physical Systems (CPSs) combine cyber, physical and human activities through computing and network technologies, creating opportunities for benign and malign actions that affect organisations in both the physical and computational spheres. The US National Cyber Security Strategy (US White House, 2023) warns that this exposes crucial systems to disruption over a wide CPS attack surface. The UK National Cyber Security Centre Annual Review (UK National Cyber Security Centre, 2023) acknowledges that, although some organisations are evolving 'a more holistic view of critical systems rather than purely physical assets', this is not reflected in governance structures that still tend to treat cyber and physical security separately.

This RQ focuses on developing and evaluating *holistic approaches* to CPS security. Such approaches have both technical and non-technical elements. They are *cross-domain* in that they span computational and physical processes and their interactions, supporting the examination of overall system-level effects. They are also *explainable* in that they support decision-making at multiple levels 'from the circuit board to the executive board'.

For example, chemical process operators may wish to address the risk of plant damage resulting from digital attacks on sensors and control units. A holistic solution might model and verify physical failsafe mechanisms, software-based authorisation for potentially dangerous actions and governance changes restricting remote access software. It would help explain risks and trade-offs of cost and business implications through techniques such as modelling, simulation, dashboards and visualisation that engage the full range of stakeholders.

There are technical and non-technical challenges in delivering holistic CPS security.

- From a technical perspective, surveys (e.g., those by Wu et al. (2016), Giraldo et al. (2017), Humayed et al. (2017), Alguliyev et al. (2018) or Kayan et al. (2022)) identify needs for systems engineering methods and tools that work across computational and physical domains. There is a need for these to support the maintenance and adaptation of security properties as both cyber and physical system elements change, as well as CPS response, resilience and survivability when facing attacks (e.g., the cross-domain attacks identified by Yampolskiy et al. (2013)). Testbeds and synthetic datasets are needed to form a basis for benchmarking, simulation and proof-of-concept studies.
- From a non-technical perspective, the 2023 UK Cyber Security Breaches Survey (UK Dept. for Science, 2023) shows that some businesses may not protect cybersecurity spending when it is seen as part of the IT budget, creating challenges for people in cyber roles making cases for security investment when governance boards can lack expertise and time to engage with cybersecurity issues. This is crucial in the CPS context, where, as Rosado et al. suggest, there is no adequate risk assessment (Rosado et al., 2022), and, as Savtschenko et al. (2017) indicate, new IT governance structures are required. Viganò and Magazzeni have pointed out that, in this environment, research should help stakeholders explain cybersecurity risks, options and decisions (Viganò et al., 2018). One approach is integrating results with toolkits such as the NCSC Cyber Security Toolkit for Boards (UK National Cyber Security Centre, 2023).

Scope

We welcome contributions that advance holistic approaches to CPS security. These should help to address the challenges of cross-domain and explainable security outlined above, identifying which stakeholders (e.g., designers, users and governance) generate and use results within systems engineering activities (e.g., requirements elicitation, design, implementation, and defence). Topics in scope include but are not limited to:

- Foundations for holistic CPS security.
- Well-founded methods and tools for engineering cross-domain CPS security, including effectively integrating existing methods and tools.

© The Author(s), 2024. Published by Cambridge University Press. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

- Authentication and evidence supporting trust in CPSs.
- Architectures, methods and tools for analysing and ensuring CPS security and privacy.
- Methods for assessing and increasing CPS resilience and survivability, including redundancy and improved incident response.
- Temporal performance as critical to CPS resilience.
- Maintenance of security-related properties under change in computational and physical processes.
- Domain-relevant tensions, for example, security/usability in medical devices.
- Adaptability and context awareness: maintenance of up-to-date security mechanisms.
- Testbeds and synthetic datasets development of realistic datasets and testbeds that are open and accessible for benchmarking, simulation and proof-of-concept studies.
- Contributions to stakeholder decision-making processes.

How to contribute to this Question

If you believe you can contribute to answering this Question with your research outputs, find out how to submit them in the Instructions for authors (https://www.cambridge.org/core/journals/research-directions-cyber-physical-systems/information/author-instructions/preparing-your-materials). This journal publishes Results, Analyses, Impact papers and additional content such as preprints and 'grey literature'. Questions will be closed when the editors agree that enough has been published to answer the Question so before submitting, check if this is still an active Question. If it is closed, another relevant Question may be currently open, so do review all the open Questions in your field. For any further queries, check the information pages (https://www.cambridge.org/core/journals/research-directions-cyber-physical-systems/information/about-this-journal) or contact this email (cps@cambridge.org).

Competing interests. None.

References

Alguliyev R, Imamverdiyev Y, Sukhostat L (2018) Cyber-physical systems and their security issues. *Computers in Industry* **100**, 212–223. https://doi.org/10.1016/j.compind.2018.04.017

Giraldo J, Sarkar E, Cardenas AA, Maniatakos M and Kantarcioglu M (2017) Security and privacy in cyber-physical systems: a survey of surveys. *IEEE Design & Test* **34**, 7–17. https://doi.org/10.1109/MDAT.2017.2709310

Humayed A, Lin J, Li F and Luo B (2017) Cyber-physical systems security—a survey. *IEEE Internet of Things Journal* **4**, 1802–1831. https:doi.org/10.1109/JIOT.2017.2703172.

Kayan H, Nunes M, Rana O, Burnap P, and Perera C (2022) Cybersecurity of industrial cyber-physical systems: a review. *ACM Computing Surveys* **54**, 35 pp. https://doi.org/10.1145/3510410

Rosado DG, Santos-Olmo A, Sánchez LE, Serrano MA, Blanco C, Mouratidis H and Fernández-Medina E (2022) Managing cybersecurity risks of cyber-physical systems: The MARISMA-CPS pattern. *Computers in Industry* **142**, 103715.

Savtschenko M, Schulte F and Voß S (2017) IT governance for cyber-physical systems: The case of Industry 4.0. In *Design, User Experience, and Usability: Theory, Methodology, and Management: 6th International Conference, DUXU 2017, Held as Part of HCI International 2017, Vancouver, BC, Canada, July 9-14, 2017, Proceedings, Part I 6*. Springer International Publishing, pp. 667–676.

UK Dept. for Science (2023) Innovation and Technology, Cyber Security Breaches Survey. Available at https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023.

UK National Cyber Security Centre (2023) Annual Review 2023. Available at NCSC Annual Review 2023 - NCSC.GOV.UK.

UK National Cyber Security Centre (2023) Cyber Security Toolkit for Boards. Available at Cyber Security Toolkit for Boards - NCSC.GOV.UK.

US White House (2023) National Cybersecurity Strategy. Available at National-Cybersecurity-Strategy-2023.pdf (whitehouse.gov).

Viganò L and Magazzeni D (2018) Explainable Security, IJCAI/ECAI 2018 Workshop on Explainable Artificial Intelligence (XAI). Available at https://arxiv.org/abs/1807.04178 arXiv e-prints.

Wu G, Sun J and Chen J (2016) A survey on the security of cyber-physical systems. *Control Theory and Technology* **14**, 2–10. https://doi.org/10.1007/s11768-016-5123-9

Yampolskiy M, Horvath P, Koutsoukos XD, Xue Y and Sztipanovits J (2013) Taxonomy for description of cross-domain attacks on CPS. In *Proceedings of the 2nd ACM international conference on High confidence networked systems*, pp. 135–142.