# Can We Develop Holistic Approaches to Delivering Cyber-Physical Systems Security?

John Fitzgerald[1] and Charles Morisset[1]

[1]Newcastle University, UK

## Context: Holistic CPS Security

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 [1] warns that this exposes crucial systems to disruption over a wide CPS attack surface. The UK National Cyber Security Centre Annual Review [2] 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’.

10.1017/cbp.2024.1

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. [3], Giraldo et al. [4], Humayed et al. [5], Alguliyev et al. [6], or Kayan et al. [7]) 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. [8]). 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 [9] 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 [10], and, as Savtschenko et al. indicate [11], new IT governance structures are required. Viganò & Magazzeni have pointed out that, in this environment, research should help stakeholders explain cybersecurity risks, options, and decisions [12]. One approach is integrating results with toolkits such as the NCSC Cyber Security Toolkit for Boards [13].

## 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, governance) generate and use results within systems engineering activities (e.g., requirements elicitation, design, implementation, defence). Topics in scope include, but are not limited to:

https://doi.org/10.1017/cbp.2024.1 Published online by Cambridge University Press

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

https://doi.org/10.1017/cbp.2024.1 Published online by Cambridge University Press

**References:**

[1] US White House. National Cybersecurity Strategy. National-Cybersecurity-Strategy-2023.pdf (whitehouse.gov), March 2023

[2] UK National Cyber Security Centre. Annual review 2023. NCSC Annual Review 2023 - NCSC.GOV.UK November 2023.

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

[4] J. Giraldo, E. Sarkar, A. A. Cardenas, M. Maniatakos and M. Kantarcioglu, *Security and Privacy in Cyber-Physical Systems: A Survey of Surveys*, in *IEEE Design & Test*, vol. 34, no. 4, pp. 7-17, Aug. 2017, doi: 10.1109/MDAT.2017.2709310

[5] A. Humayed, J. Lin, F. Li and B. Luo, *Cyber-Physical Systems Security—A Survey*, in *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1802-1831, Dec. 2017, doi: 10.1109/JIOT.2017.2703172.

[6] Rasim Alguliyev, Yadigar Imamverdiyev, Lyudmila Sukhostat, *Cyber-physical systems and their security issues*, Computers in Industry 100, 2018 pp. 212-223 https://doi.org/10.1016/j.compind.2018.04.017

[7] Hakan Kayan, Matthew Nunes, Omer Rana, Pete Burnap, and Charith Perera. 2022. Cybersecurity of Industrial Cyber-Physical Systems: A Review. ACM Comput. Surv. 54, 11s, Article 229 (January 2022), 35 pages. https://doi.org/10.1145/3510410

[8] Yampolskiy, M., Horvath, P., Koutsoukos, X. D., Xue, Y., & Sztipanovits, J. (2013, April). 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).

[9] UK Dept. for Science, Innovation and Technology, Cyber Security Breaches Survey, April 2023. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023

[10] Rosado, D. G., Santos-Olmo, A., Sánchez, L. E., Serrano, M. A., Blanco, C., Mouratidis, H., & Fernández-Medina, E. (2022). Managing cybersecurity risks of cyber-physical systems: The MARISMA-CPS pattern. *Computers in Industry*, *142*, 103715.

https://doi.org/10.1017/cbp.2024.1 Published online by Cambridge University Press

[11] Savtschenko, M., Schulte, F., & 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* (pp. 667-676). Springer International Publishing.

[12] Luca Viganò and Daniele Magazzeni, Explainable Security, IJCAI/ECAI 2018 Workshop on Explainable Artificial Intelligence (XAI), https://arxiv.org/abs/1807.04178 arXiv e-prints, July 2018.

[13] UK National Cyber Security Centre. Cyber Security Toolkit for Boards. Cyber Security Toolkit for Boards - NCSC.GOV.UK, March 2023.

https://doi.org/10.1017/cbp.2024.1 Published online by Cambridge University Press