Security Analysis of Cyber-Physical Systems: from Formal Methodologies to ICS Honeypots

Massimo Merro

Department of Computer Science
University of Verona - Italy

Verona, 29 May 2025

Research conducted in the last 10 years (1/2)

Foundations of IoT systems and Cyber-Physical Systems (CPSs)

- Formal languages reason on IoT systems and CPSs [1, 2, 3, 4]
- Reachability analysis of CPSs: decidable classes of linear CPSs [5]

Foundations of IoT and CPS Security

- Security and safety issue in IoT Platforms [6, 7]
- Formal threat models for physics-based attacks [8, 9]
- (Statistical) model checking of security properties of CPSs [10, 11, 12]
- Runtime enforcement od Industrial Controllers (PLCs) [13, 14, 15, 16]
- Impact metrics for Cyber-Physical Attacks [17, 18]
- Formal Robustness and Tolerance of CPSs [19, 20, 21, 22]
- Obfuscation techniques to protect PLCs from reverse eng. [23, 24]

Research conducted in the last 10 years (2/2)

Advanced Honeypots for Industrial Control Systems

- HoneyICS: A High-interaction physics-aware honeynet for Industrial Control Systems [25, 26]
- Latitudinal studies of IT and ICS interactions on ICS honeypots [27, 28]
- A framework to rank the fidelity of ICS noicy simulations [29]

The research mentioned above is mainly supported by the project "Novel Methodologies and Tools for Next Generation Cyber Ranges" (NoMeN), in partnership with the "Centro Alti Studi della Difesa Italiana" (CASD), and within the PNRR project ARTIC from University of Genoa.
PI: Prof. Massimo Merro. Total fundings: 789K Euros.

References 1/6


[1] Lanotte and Merro
A Semantic Theory of the Internet of Things (Extended Abstract)
In 18th IFIP Int. Conf. COORDINATION Models and Languages, 2016


[2] Lanotte and Merro
A Semantic Theory of the Internet of Things
Information & Computation, 259(1):72-101, 2018


[3] Lanotte and Merro
A Calculus of Cyber-Physical Systems
In 11th Language and Automata Theory and Applications (LATA) 2017


[4] Lanotte, Merro and Tini
A Probabilistic Calculus of Cyber-Physical Systems
Information & Computation, vol. 279 art. 104618, pages 1-30, 2021


[5] Lanotte, Merro and Mogavero
On the decidability of linear bounded periodic cyber-physical system
In 22nd ACM Hybrid Systems: Computation and Control (HSCC), 2019

References 2/6

[6] Balliu, Merro and Pasqua
Securing Cross-App Interactions in IoT Platforms
In 32nd IEEE Computer Security Foundations Symposium (CSF), 2019.

[7] Balliu, Merro, Pasqua and Shcherbakov
Frindly Fire: Cross-app Interactions in IoT Platforms
ACM Trans. Privacy and Security, vol. 24(3) pp. 16:1-16:40, 2021.

[8] Lanotte, Merro, Muradore and Viganò
A Formal Approach to Cyber-Physical Attacks.
In 30th IEEE Computer Security Foundations Symposium (CSF), 2017

[9] Lanotte, Merro, Munteanu and Viganò.
A Formal Approach to Physics-Based Attacks in Cyber-physical Systems.
ACM Trans. Privacy and Security, vol. 23(1) pp. 3:1-3:41, 2020.

[10] Lanotte, Merro and Munteanu
A Modest Security Analysis of Cyber-Physical Systems: A Case Study
In 38th Formal Techn. for Distr. Objects, Comp. and Systems (FORTE) 2018

References 3/6


[11] Munteanu, Pasqua and Merro
Impact Analysis of Cyber-Physical Attacks on a Water Tank System via Statistical Model Checking
In 8th IEEE/ACM Formal Methods in Sw Engineering (FormaliSE) 2020


[12] Lanotte, Merro and Zannone
Impact Analysis of Coordinated Cyber-Physical Attacks via Statistical Model Checking: A Case Study
In 43rd Formal Techn. for Distr. Objects, Comp. and Sys. (FORTE) 2023


[13] Lanotte, Merro and Munteanu
Runtime Enforcement for Control System Security
In 33rd IEEE Computer Security Foundations Symposium (CSF) 2020


[14] Lanotte, Merro and Munteanu
A Process Calculus Approach to Correctness Enforcement of PLCs
In 21th Italian Conference on Theoretical Computer Science (ICTCS) 2020

References 4/6

[15] Lanotte, Merro and Munteanu
A process calculus approach to detection and mitigation of PLC malware
Theoretical Computer Science, 890:125-146, 2021

[16] Lanotte, Merro and Munteanu
Industrial Control Systems Security via Runtime Enforcement
ACM Trans. Privacy and Security, vol. 26(1) pp. 4:1-4:41, 2023

[17] Lanotte, Merro and Tini
Towards a formal notion of impact metric for cyber-physical attacks
In 14th Integrated Formal Methods (IFM), 2018

[18] Lanotte, Merro, Munteanu and Tini
Formal Impact Metrics for Cyber-physical Attacks
In 34th IEEE Computer Security Foundations Symposium (CSF), 2021

[19] Chong, Lanotte, Merro, Tini and Xiang
Quantitative Robustness Analysis of Sensor Attacks on CPSs
In 26th ACM Hybrid Systems: Control and Computation (HSCC) 2023

References 5/6

[20] Xiang, Lanotte, Tini, Chong and Merro
Measuring Robustness in Cyber-Physical Systems under Sensor Attacks
Nonlinear Analysis: Hybrid Systems, vol. 56 art. 101559, pages 1-25, 2025

[21] Xiang, Tini, Lanotte and Merro
Formal Robustness for Cyber-Physical Systems under Timed Attacks
In 38th IEEE Computer Security Foundations Symposium (CSF), 2025

[22] Xiang, Tini, Lanotte and Merro
Formal Quantitative Tolerance of CPSs under Periodic Attacks
submitted for publication

[23] Cozza, Dalla Preda, Lucchese, Merro and Zannone
Towards Obfuscaton of Programmable Logic Controllers
In 18th Int. Conf. on Availability, Reliability and Security (ARES) 2023

[24] Cozza, Dalla Preda, Lanotte, Lucchese, Merro and Zannone
Obfuscation strategies for Industrial Control Systems
Int. Journal of Critical Infrastructure Protection, vol. 47, art. 100717, 2024

References 6/6

[25] Lucchese, Merro, Paci and Zannone
Towards A High-interaction Physics-aware Honeynet for ICSs
In 38th ACM/SIGAPP Symposium On Applied Computing (SAC) 2023

[26] Lucchese, Lupia, Merro, Paci, Zannone and Furfaro
HoneyICS: A High-interaction Physics-aware Honeynet for ICSs
In 18th Int. Conf. on Availability, Reliability and Security (ARES) 2023

[27] Lupia, Lucchese, Merro and Zannone
ICS Honeypot Interactions: A Latitudinal Study
2023 IEEE International Conference on Big Data (IEEE BigData)

[28] Ondrinov, Donadel, Lupia, Merro, dos Santos, Zambon and Zannone
A Comparative Study of ICS Honeypot Deployments
Submitted for publication

[29] Donadel, Crestanello, Morandini, Antonioli, Conti and Merro
SimProcess: High Fidelity Simulation of Noisy ICS Physical Processes
In 11th ACM Cyber-Physical System Security Workshop, at AsiaCCS, 2025