

Stefano Longari

Curriculum Vitae

Last updated: April 7, 2025

I received my Ph.D. degree in Information Technology from Politecnico di Milano in June 2021 with a thesis on the security of automotive systems. I am currently an assistant professor (RTDa) at Politecnico di Milano, working in the system security group at NECST Laboratory inside the Dipartimento di Elettronica, Informazione e Bioingegneria. The focus of my research revolves around threat modeling and developing offensive and defensive techniques for the security of cyber-physical systems and transportation systems, e.g., automotive, space, industry 4.0, and critical infrastructure. I teach mainly courses and lectures on (cyber-physical) systems security and social engineering.

Contents

○ Overview	1	○ Academic Roles	4
○ Research Interests	2	○ Speaker Engagements	5
○ Experience	2	○ Advisor Activities	6
○ Education	2	○ Teaching Activities	7
○ Publications	2	○ Other Activities	8
○ Fundings	4		

Overview

Current Role: Junior Researcher (RTDa) at Politecnico di Milano since May 2023

Scientific Productivity: Author of 6 Q1 journal papers and 17 peer-reviewed conference papers. Author of 2 patents.

Based on Google Scholar: h-index 8 citations 295

Based on Scopus: h-index 7 citations 189

Fundings: Task leader for the *AHEAD* european project, participant of the *SARIL* and *KEEPER* european projects. Local PI for the *SOCRATE* project funded by ASI, and participant to the *MICS* PNRR project. PI for an industrial contract on satellite cybersecurity.

Academic Roles: Chair and member for the master *thesis examination boards* of Politecnico di Milano and Bocconi. Coordinator of the *Security Specialist specialization degree* (equivalent to an academic master) for CEFRIEL and Politecnico di Milano. Organizer of OWASP Italy Day 2023.

Worked as PC of 9 cybersecurity-related conferences, amongst which ACSAC and DIMVA.

Reviewer for 13 Q1 journals and transactions.

Invited Talks: Various presentations at industrial events, HackInBo, and Hardwear.io.

Advisor Activities:

Currently advisor of 3 Ph.D. students in Computer Science and Engineering.

Advisor or Co-advisor of over 50 Master Theses for the Computer Science and Engineering Master.

Advisor of ~5 Master Theses for the Cyber Risk Strategy and Governance Master.

Teaching Activities: Currently course instructor for 1 Ph.D. course, 2 Master courses, and various industrial courses.

Ph.D.: Advanced Research Topics in Cybersecurity.

Master: Human and Physical Aspects of Security course for Politecnico di Milano.

Master: Emerging Topics in Cybersecurity Course for Bocconi.

Research Interests

My research spans approximately seven years, beginning with my Ph.D. studies, which initially focused on automotive cybersecurity. I concentrated on securing vehicle on-board systems, specifically targeting vulnerabilities and intrusion detection mechanisms within the Controller Area Network (CAN) protocol. This early work involved creating real-world datasets, publishing *machine learning-based IDS frameworks*, and identifying *novel threats* and attack surfaces. Building upon this foundation in automotive security, I have broadened my expertise into the wider domain of Cyber-Physical Systems (CPS). My current research encompasses diverse fields, still including the automotive one, but expanding to industrial robots, railway infrastructure, e-vehicle charging solutions, satellite systems, and critical infrastructure resilience. Across these domains, my main interests are *attack detection and threat modeling*, exploring threats emerging from integrating novel technological solutions into existing systems. Additionally, I am participating in various projects addressing emerging cybersecurity challenges involving AI-driven social engineering, covert communication channels utilizing Large Language Models (LLMs), and vulnerabilities within federated learning systems.

Experience

Junior Researcher (RTDa)

Politecnico di Milano (Milan, Italy)

May 2023 — Current

Research topic: Threat modeling, offensive, and defensive measures for novel cyber-physical systems.

Research group: NECSTLab, System security research group.

Postdoctoral Researcher

Politecnico di Milano (Milan, Italy)

Jun 2021 — Apr 2023

Research topic: Offensive and defensive security techniques for cyber-physical systems.

Research group: NECSTLab, System security research group.

Research Internship

ESCRYPT GmbH (Stuttgart, Germany)

Oct 2019 — Apr 2020

Research topic: Development of new security techniques for automotive on-board CAN-connected devices.

Education

Ph.D. in Information Technology, Politecnico di Milano

Jun 2021

Dissertation title: *On the security of connected automotive systems*

M.Sc. in Computer Science and Engineering, Politecnico di Milano

Apr 2018

Dissertation title: *On the security of connected vehicles*

Bachelor in Computer Science and Engineering, Politecnico di Milano

Sep 2015

Publications

Productivity and Impact Metrics

Scientific Productivity: Author/Co-author of 7 scientific publications on journal papers, including 6 top-ranked Q1 journal papers based on SCIMAGO, and 17 peer-reviewed conferences, including 1 top-ranked security conference where the work received an award for its value. 14 publication entries on Scopus (+8 yet to be published but accepted in Scopus-indexed venues). 23 publication entries on Google Scholar.

Based on Google Scholar: h-index 8 citations 295

Based on Scopus: h-index 7 citations 189

Peer-reviewed Journals

- Barelli, R., D'Onghia, M., & Longari, S. (2025). *Towards Secure Electronic Voting: a Survey on E-Voting Systems and Attacks*. (To be published) IEEE Access.
- Longari, S., Jannone, J., Carminati, M., Tanelli, M., & Zanero, S. (2024). *Janus: A Trusted Execution Environment Approach for Attack Detection in Industrial Robot Controllers*. IEEE Transactions on Emerging Topics in Computing.

- **Longari, S.**, Pozzone, A., Leoni, J., Polino, M., Carminati, M., Tanelli, M., & Zanero, S. (2023). *CyFence: Securing Cyber-physical Controllers Via Trusted Execution Environment*. IEEE Transactions on Emerging Topics in Computing.
- Nichelini, A., Pozzoli, C. A., **Longari, S.**, Carminati, M., & Zanero, S. (2023). *Canova: a hybrid intrusion detection framework based on automatic signal classification for CAN*. Computers & Security, 128, 103166.
- Maffiola, D., **Longari, S.**, Carminati, M., Tanelli, M., & Zanero, S. (2021). *GOLIATH: A Decentralized Framework for Data Collection in Intelligent Transportation Systems*. IEEE Transactions on Intelligent Transportation Systems.
- **Longari, S.**, Valcarcel, D. H. N., Zago, M., Carminati, M., & Zanero, S. (2020). *CANnolo: An anomaly detection system based on LSTM autoencoders for controller area network*. IEEE Transactions on Network and Service Management, 18(2), 1913-1924.
- Zago, M., **Longari, S.**, Tricarico, A., Carminati, M., Pérez, M. G., Pérez, G. M., & Zanero, S. (2020). *ReCAN-Dataset for reverse engineering of Controller Area Networks*. Data in brief, 29, 105149.

Peer Reviewed Conference Proceedings

- Mammone, D. and Bossi, L., Carminati, M., Zanero, S., & **Longari, S.** (2025). *Linux hurt itself in its confusion! Exploiting Out-of-Memory Killer for Confusion Attacks via Heuristic Manipulation*. (To be published) SIG SIDAR Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA 2025)
- Panebianco F., and Isgrò, A., **Longari, S.**, Zanero, S., & Carminati, M. (2025). *Guessing As A Service: Large Language Models Are Not Yet Ready For Vulnerability Detection*. (To be published) Joint National Conference on Cybersecurity (ITASEC & SERICS 2025)
- Balossini, M., Carminati, M., Zanero, S., & **Longari, S.** (2025). *Micro-Mobility Security: A Holistic Approach via Mobile App Analysis*. (To be published) Joint National Conference on Cybersecurity (ITASEC & SERICS 2025)
- Abbasi, S.M., & **Longari, S.** (2025). *CANPak: An Intrusion Detection System against Error Frame Attacks for Controller Area Network*. (To be published) Joint National Conference on Cybersecurity (ITASEC & SERICS 2025)
- Giannubilo, D., Giorgeschi, T., Carminati, M., Zanero, S., & **Longari, S.** (2025). *A Deep Learning Approach for False Data Injection Attacks Detection in Smart Water Infrastructure*. (To be published) Joint National Conference on Cybersecurity (ITASEC & SERICS 2025)
- **Longari, S.**, Galletti, G., Holle, J., & Zanero, S. (2025). *CANter: data-link layer detection of drop-and-spoof attacks on CAN and CAN FD*. (To be published) Joint National Conference on Cybersecurity (ITASEC & SERICS 2025)
- Amico, A., Apicella, V., Bianchini, D., Butera, A., Cesana, M., Digregorio, G., Garda, M., Gatteschi, V., Innamorati, C., Leotta, F., **Longari, S.**, Pizzo, M.R., (2025). *BOTQUAS: Blockchain-based Solutions for Trustworthy Data Sharing in Sustainable and Circular Economy*. Proceedings of the Euromicro Conference on Software Engineering and Advanced Applications (EUROMICRO-SEAA 2024).
- Cestari, R., **Longari, S.**, Zanero, S., & Formentin, S. (2025). *Model Predictive Control with adaptive resilience for Denial-of-Service Attacks mitigation on a Regulated Dam*. (To be published) 2024 Conference on Decision and Control (CDC 2024).
- Digregorio, G., Cainazzo, E., **Longari, S.**, Carminati, M., & Zanero, S. (2024, June) *Evaluating the Impact of Privacy-Preserving Federated Learning on CAN Intrusion Detection*. In proceedings of the IEEE Vehicular Technology Conference Spring (VTC Spring 2024).
- Cerracchio, P., **Longari, S.**, Carminati, M., & Zanero, S. (2024, February) *Investigating the Impact of Evasion Attacks Against Automotive Intrusion Detection Systems*. In Proceedings of the 2024 Symposium on Vehicle Security and Privacy (VehicleSec 2024).
- Marazzi, M., **Longari, S.**, Carminati, M., & Zanero, S. (2024, February) *Securing LiDAR Communication through Watermark-based Tampering Detection*. In Proceedings of the 2024 Symposium on Vehicle Security and Privacy (VehicleSec 2024).
- **Longari, S.**, Pozzoli, C. A., Nichelini, A., Carminati, M., & Zanero, S. (2023, June). *Candito: improving payload-based detection of attacks on controller area networks*. In International Symposium on Cyber Security, Cryptology, and Machine Learning (pp. 135-150). Cham: Springer Nature Switzerland.
- **Longari, S.**, Nosedà, F., Carminati, M., & Zanero, S. (2023, June). *Evaluating the Robustness of Automotive Intrusion Detection Systems Against Evasion Attacks*. In International Symposium on Cyber Security, Cryptology, and Machine Learning (pp. 337-352). Cham: Springer Nature Switzerland.
- Avanzi, D., **Longari, S.**, Polino, M., Carminati, M., Zanchettin, Tanelli, M., & Zanero, S. (2023). *Task Aware Intrusion Detection for Industrial Robots*. In Proceedings of the Italian Conference on Cyber Security (ITASEC 2023) (pp. 1-16). CEUR.
- de Faveri Tron, A., **Longari, S.**, Carminati, M., Polino, M., & Zanero, S. (2022, November). *CANflict: Exploiting Peripheral Conflicts for Data-Link Layer Attacks on Automotive Networks*. In Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (pp. 711-723).

- **Longari, S.**, Penco, M., Carminati, M., & Zanero, S. (2019, November). *Copycan: An error-handling protocol based intrusion detection system for controller area network*. In Proceedings of the ACM Workshop on Cyber-Physical Systems Security & Privacy (pp. 39-50).
- **Longari, S.**, Cannizzo, A., Carminati, M., & Zanero, S. (2019, December). *A secure-by-design framework for automotive on-board network risk analysis*. In 2019 IEEE Vehicular Networking Conference (VNC) (pp. 1-8). IEEE.

Awards

- Best Paper Runner Up, Securing LiDAR Communication through Watermark-based Tampering Detection. 2024 Symposium on Vehicle Security and Privacy (VehicleSec 2024).
- Best Paper Honorable Mention, CANflict: Exploiting Peripheral Conflicts for Data-Link Layer Attacks on Automotive Networks. 2022 ACM SIGSAC Conference on Computer and Communications Security.

Patents

- Sistema di controllo in tempo-reale implementato mediante computer per il controllo di un sistema o dispositivo fisico (Computer-implemented real-time control system for controlling a physical system or device), International application ref: WO2023002321A1. Numero di pubblicazione italiano: IT202100018998A1. **S. Longari**, A. Pozzone, M. Tanelli, S. Zanero. Published 2023. 01. 26.
- Submitted: Verfahren zum Erkennen eines Angriffs auf einen zu sichernden Busteilnehmer, Überwachungseinheit und Bussystem (Method for detecting an attack on a to be protected bus node, monitoring system and the bus). Registration number: DE 102022207911.6. **S. Longari**, J. Holle. Registered on 01.08.2022.

Fundings

European Projects:

- | | |
|--|-------------|
| AHEAD: <i>AI-informed Holistic EVs integration Approaches for Distribution grids</i> | 2024 — 2028 |
| Role: Task Leader. | |
| SARIL: <i>Sustainability And Resilience for Infrastructure and Logistics networks</i> | 2023 — 2026 |
| Role: Participant. | |
| KEEPER: <i>Key Code based on Nanomaterials to Protect Services and Products</i> | 2024 — 2027 |
| Role: Participant. | |

Other open calls:

- | | |
|--|-------------|
| SOCRATE: <i>Satellite Operations Cyber Range Evaluation</i> | 2023 — 2025 |
| Founding source: Agenzia Spaziale Italiana | |
| Role: Local PI. | |
| MICS: <i>Made in Italy Circolare e Sostenibile</i> | 2023 — 2025 |
| Founding source: PNRR | |
| Role: Participant. | |

Industrial contracts:

- | | |
|--|-------------|
| Satellite Cybersecurity: <i>development of Intrusion Detection Solutions for intra-satellite networks</i> | 2024 — 2025 |
| Founding source: D-Orbit | |
| Role: PI. | |

Academic Roles

Specialization Degree Coordinator:

- | | |
|---|----------------|
| Security Specialist <i>specialization degree ("Master universitario di primo livello")</i> | 2022 — Present |
| Organizers: CEFRIEL and Politecnico di Milano | |
| Number of students: ~20 | |
| Length: 2yrs. | |

Events and Conferences Organization:

Organizers: OWASP Italy and Politecnico di Milano

Program Committee:

- Annual Computer Security Applications Conference, **ACSAC** 2025
- Italian conference on Cybersecurity, **ITASEC** 2024 — 2025
- IEEE Security and Privacy Symposium, **IEEE S&P** (Subreviewer) 2023 — 2025
- Conference on Detection of Intrusions and Malware & Vulnerability Assessment, **DIMVA** 2024
- Workshop on Re-design Industrial Control Systems with Security, **RICSS** (in conjunction with Euro S&P) 2023
- Cyber-Physical System Security Workshop, **CPSS** (in conjunction with ASIACCS) 2023
- Workshop on Automotive Cybersecurity, **ACSW** (in conjunction with EURO S&P) 2022 — 2025
- Joint Workshop on CPS & IoT Security and Privacy, **CPSIoTSec** (in conjunction with ACM CCS) 2022
- International Conference on Security for Information Technology and Communications, **SecITC2022** 2022

Reviewer:

- ACM Transactions on Cyber-Physical Systems, **ACM TCPS** 2025
- IEEE Internet of Things Journal, **IEEE IoT** 2022 — 2025
- Elsevier Computer and Security, **COSE** 2019 — 2025
- ACM Computing Surveys, **ACM CSUR** 2024
- IEEE Transactions on Automation Science and Engineering, **IEEE T-ASE** 2024
- ACM Computers and Communication Security, **ACM CCS** (Subreviewer) 2023 — 2024
- Elsevier Journal of Parallel and Distributed Computing, **JPDC** 2024
- IEEE Transactions on Intelligent Transportation Systems, **IEEE T-ITS** 2023
- IEEE Transactions on Aerospace and Electronic Systems, **IEEE TAES** 2022 — 2023
- IEEE Transactions on Dependable and Secure Computing, **IEEE TDSC** 2022
- IEEE Transactions on Industrial Informatics, **IEEE TII** 2021 — 2022
- IEEE Transactions on Information Forensics and Security, **IEEE T-IFS** 2021
- IEEE Transactions on Emerging Topics in Computing, **IEEE TETC** 2018

Other Academic Roles:

Examination Board Chair 2024 — Current

Course: Computer Science and Engineering Master, Politecnico di Milano

Examination Board Member 2022 — Current

Course: Computer Science and Engineering Master, Politecnico di Milano

Examination Board Member 2023 — Current

Course: Cyber Risk Strategy and Governance Master, Bocconi and Politecnico di Milano

Academic Advisor for Politecnico's Career Service 2025 — Current

Handle industrial stages proposed to the students of the Cyber Risk Strategy and Governance master.

Academic Cybersecurity Area Referent for MADE Competence Center 2023 — Current

Organize the future directions of the cybersecurity area in cooperation with the industrial partners.

Speaker Engagements

Invited Talks

- REDDER Level Up 2024
Title: *L'anello debole: l'IA punta sugli esseri umani*
- Bosch Next Event 2024
Title: *Challenges in Industrial Cybersecurity*
- Hromatka Group 2023
Title: *Risk and Industrial Security*
- HackInBo 2022
Title: *The CAN Link-Layer, or how we implemented a broken protocol, and can we fix it?*

- Automotive Security Research Group 2021
Title: *CAN Error Handling Attacks and Countermeasures*
- Hardwear.io 2019
Title: *It's easier to break than to patch: a stealthy DoS attack against CAN*
- Infosek conference 2018
Title: *Automotive Security*

Paper Presentations

- Italian Conference on Cybersecurity (ITASEC) 2025
Paper - *CANPak: An Intrusion Detection System against Error Frame Attacks for Controller Area Network*
Paper - *A Deep Learning Approach for False Data Injection Attacks Detection in Smart Water Infrastructure*
- Italian Conference on Cybersecurity (ITASEC) 2024
Paper - *CANter: data-link layer detection of drop-and-spoof attacks on CAN and CAN FD*
- Symposium on Vehicle Security and Privacy (VehicleSec) 2024
Paper - *Investigating the Impact of Evasion Attacks Against Automotive Intrusion Detection Systems.*
Paper - *Securing LiDAR Communication through Watermark-based Tampering Detection.*
- International Symposium on Cyber Security, Cryptology, and Machine Learning (CSCML) 2023
Paper - *Candito: improving payload-based detection of attacks on controller area networks*
Paper - *Evaluating the robustness of automotive intrusion detection systems against evasion attacks*
- IEEE Vehicular Networking Conference (IEEE VNC) 2019
Paper - *A secure-by-design framework for automotive on-board network risk analysis*
- ACM Workshop on Cyber-Physical Systems Security & Privacy (ACM CPS-SPC) 2019
Paper - *Copycan: An error-handling protocol based intrusion detection system for controller area network*

Advisor Activities

Ph.D. Thesis Advisor Activities:

- | | |
|--|----------------|
| (temporary title) On the security of e-vehicle charging infrastructure. <i>Balossini Marco</i> | 2024 — Current |
| Security of Cyber-Physical Systems. <i>Mammone Daniele</i> | 2023 — Current |
| Offensive and Defensive Cybersecurity for Critical Infrastructures. <i>Digregorio Gabriele</i> | 2023 — Current |

Master Thesis Advisor Activities:

- | | |
|---|------|
| A DL Approach for FDI Attacks Detection in SWI <i>Giannubilo Davide & Giorgeschi Tommaso</i> | 2025 |
| Exploiting Out-of-Memory Killer for Confusion Attacks via Heuristic Manipulation. <i>Bossi Lorenzo</i> | 2025 |
| Evaluating FL Algorithms for Intrusion Detection in the Automotive Domain. <i>Cardani Federico</i> | 2025 |
| Enhancing Security in Blockchain-based Decentralized FL. <i>Caroli Federico & Bleggi Francesco</i> | 2025 |
| Threat Modeling of Autonomous Vehicle Security: a Case Study on the AIDA Prototype. <i>Boccia Giuseppe</i> | 2024 |
| CANdemonium: An Evaluation Test Bed for Objective CAN IDSs Benchmarking. <i>Azzarà Daniele</i> | 2024 |
| Implementation of a DNS Filtering System for User-Friendly Online Security. <i>Zuelli Arianna Luisa</i> | 2024 |
| Bypassing ARM TrustZone Security: A JTAG-based Approach. <i>Martelli Vincenzo</i> | 2024 |
| Towards Effective CAN IDS Validation: Dataset Limitations and Requirements Definition. <i>Porta Alessia</i> | 2024 |
| Performance Evaluation of CANdito . <i>Marelli Giacomo</i> | 2024 |
| Sandboxing in Space: A Feasibility Study on Application Sandboxing for Small Satellites. <i>Marra Gabriele</i> | 2024 |
| Race Conditions Detection in Web Applications: An Analysis Tool. <i>Paratici Ilaria</i> | 2024 |
| Novel attack strategies targeting PROFibus and PROFIsafe Exploiting Error Management. <i>Alfonsi Alessio</i> | 2024 |
| CANPak: An IDS against Stealthier Attacks for CAN. <i>Mehmood Abbasi Sikandar</i> | 2024 |
| Meeting Proof Protocol: a Protocol for Physical Anchor Systems. <i>Sironi Mattia</i> | 2024 |
| Empirical Security Evaluation of Digital Therapeutic Applications. <i>Gervasio Dario Alex</i> | 2024 |
| Micro-Mobility Security: A Systematic Approach via Mobile App Analysis. <i>Balossini Marco</i> | 2024 |
| CANtera: A novel real-world dataset on advanced CAN attacks for IDSs. <i>Valencic Jas</i> | 2024 |
| Evaluation of Graph-based IDS Based on Outlier Detection Methods for CAN-bus. <i>Balalipour Pedram</i> | 2024 |
| On the feasibility of Adversarial Attacks against IDSs in Automotive CAN. <i>Montalbano Ivan</i> | 2024 |
| Location inference through social media and social relationships. <i>Rizzi Matteo</i> | 2023 |
| Panettone: evaluating federated learning implementations of CAN IDSs. <i>Cainazzo Elisabetta</i> | 2023 |
| A Blockchain-based framework to enhance air traffic control security using ADS-B protocol. <i>Saputelli Edoardo</i> | 2023 |

A Comprehensive Study of Cyber Threats and Countermeasures in Micromobility. <i>Rosati Nicholas</i>	2023
Exploring gradient-based evasion techniques against automotive intrusion detection systems. <i>Cerracchio Paolo</i>	2023
Towards Secure Electronic Voting : a Literature Review on E-Voting Systems and Attacks. <i>Barelli Riccardo</i>	2023
Securing Lidar communication through watermark-based tampering detection. <i>Marazzi Michele</i>	2023

Co-Advisor of over 20 Master Theses over the years 2018-2025

Teaching Activities

Course Instructor - Ph.D.s:

- *Advanced Research Topics In Cyber Security* 2024 — 2025
Politecnico & Bocconi, Computer Science and Engineering & Cyber Risk Strategy and Governance Milan, Italy
Number of students: ~10.
Hours: 30/year.

Course Instructor - Masters:

- *Human and Physical aspects of Security* 2024 — Current
Politecnico & Bocconi, Computer Science and Engineering & Cyber Risk Strategy and Governance Milan, Italy
Number of students: ~60.
Hours: 50/year.
- *Emerging Topics in Cybersecurity* 2024 — Current
Bocconi, Cyber Risk Strategy and Governance Master Milan, Italy
Number of students: ~30.
Hours: 16/year.
- *Social Engineering* 2022 — 2024
Bocconi, Cyber Risk Strategy and Governance Master Milan, Italy
Number of students: ~30.
Hours: 16/year.

Teaching Assistant - Masters & Bachelors:

- *Cybersecurity Technologies, Procedures and Policies* 2023 — Present
Politecnico & Bocconi, Cyber Risk Strategy and Governance Milan, Italy
Number of students: ~30.
Hours: 17/year.
- *Informatica B* 2023 — 2024
Politecnico di Milano, Ingegneria Energetica e Matematica Milan, Italy
Number of students: ~250.
Hours: 25/year.
- *Computer Security* 2019 — 2023
Politecnico di Milano, Computer Science and Engineering Milan, Italy
Number of students: ~200.
Hours: 10/year.

Non-University Courses:

- *Cybersecurity* 2022 — Current
CEFRIEL & Politecnico di Milano, "security specialist" specialization degree. Milan, Italy
Number of students: ~25.
Hours: 110/year.
- *Introduction to Industrial Cybersecurity* 2023 — Present
MADE Competence Center per l'Industria 4.0 Milan, Italy
Various single-day instances between 2 and 8 hours.
- *Cybersecurity* 2019 — 2022
POLI.DESIGN, Fundamentals of the air transport system Milan, Italy
Number of students: ~20.
Hours: ~10/year.

Recorded Courses:

- *Introduction to Industrial Cybersecurity*
MADE Competence Center per l'Industria 4.0
12 ~30 minutes lectures on the basics of security in industrial scenarios.

2024
Milan, Italy

Other Activities

- Interviews on deepfake social engineering for RAI*
- Consulting work for RAI Radiotelevisione Italiana*

2024
2024