[seal]
EPFL . HEIG-VD . UNIL

CALL FOR PROJECTS #3

Opening 19.06.2025 | Closing 15.11.2025

As industrial companies become more digitized, they become vulnerable to new threats. These include compromising machine operation, disrupting production lines, industrial espionage, and data exfiltration.

This call for projects aims to stimulate collaborative innovation to propose solutions that address today's digital security challenges in industrial environments. It is conducted in collaboration with the Groupement suisse de l'Industrie des Machines (GIM) (*Swiss Machinery Industry Group*).

University researchers, industry and technology players, and experts in digitalization and cybersecurity are invited to collaborate to strengthen industry's capacity for innovation and resilience in the face of new cyber threats, thereby helping to safeguard its survival, sustainability, and competitiveness.

CONTEXT AND CHALLENGES

The rise of Industry 4.0 is marked by the digitization of production processes, an abundance of sensors and actuators, connected intelligent objects, machine-to-machine communication, data sharing with manufacturers and subcontractors, and the integration of artificial intelligence. Once isolated, industrial systems are now increasingly connected and integrated with information technologies, greatly increasing their exposure to cyber threats.

The convergence of IT (information technology) and OT (operational technology) has created new opportunities but also increased vulnerabilities.

Many industrial companies still struggle to implement effective cybersecurity strategies and solutions to protect their infrastructure and data, ensure operational continuity, and safeguard their manufacturing secrets. Industrial environments have particularities that call for sophisticated requirements and new approaches to cybersecurity and testing, such as obsolete systems kept in production, system heterogeneity, a large number of components, and specific proprietary protocols. This explains why effective security measures are still largely insufficient in OT environments.

These companies face major risks, and the consequences can be dramatic. This is particularly true with regard to physical security, as it can lead to the disruption of vital services and endangerment of employees. Additionally, the leakage of industrial secrets attracts hackers who see this as a new financial opportunity. Incidents involving ransomware (where data is locked against a ransom demand), attacks on supply chains, and infiltration of supervision and data acquisition systems have thus increased significantly in recent years.

In the face of this scourge, regulations requiring industrial players to strengthen their cybersecurity are multiplying. Therefore, it is urgent that industrial companies integrate cybersecurity as a fundamental pillar of their digital transformation, so they can modernize within a framework of trust (safe, secure, and robust).

OBJECTIVES

This call for projects aims to **explore new ideas and study and develop disruptive concepts and innovative technical solutions that enhance the cybersecurity and resilience of industrial systems**. These solutions will contribute to the sustainability of Swiss industry and the protection of our critical infrastructures.

More specifically, the objectives are as follows (non-exhaustive):

- **Enhance the security of operational technologies (OT)** by adopting a holistic approach to managing cyber threats specific to industrial environments and protecting critical infrastructures. This includes real-time monitoring systems, hardening industrial equipment, controlling information flows, implementing network segmentation solutions, securing industrial protocols, using advanced authentication mechanisms, and protecting against firmware injection and compromise attacks.
- **Promote a Zero Trust approach in industrial and OT environments** by developing specific architectures for industrial infrastructures, taking into account availability and performance constraints (industrial firewalls, IT/OT and DMZ network segmentation, secure machine-to-machine communications, secure remote access, encryption mechanisms adapted to constraints).
- **Develop protection technologies and solutions for industrial control systems (ICS)** that can detect anomalies and prevent intrusions without disrupting operations, including particularly the use artificial intelligence and machine learning for this purpose.
- **Improve risk management and compliance** by providing better visibility of risks and threats. This enables effective decision-making with tools for dynamic risk assessment and regulatory compliance.

FIELDS OF APPLICATION

Projects include (but are not limited to) the following areas:

- **Industrial Control System (ICS) Security**: design of secure OT system architectures, securing industrial protocols, IT/OT segmentation management, hardening of industrial equipment, anomaly detection solutions adapted to ICS environments
- **Industrial Network Security**: design of secure OT network architectures (industrial firewalls, VLANs, micro-segmentation), IDS/IPS for OT, secure remote access management (suppliers, maintenance, subcontractors, etc.), industrial traffic monitoring (analysis of M2M communications), protection solutions against specific OT attacks (replay attacks, MITM, command injection)
- **Endpoint Security:** hardening and protection of firmware and software source code, protection of embedded systems (PLCs, sensors, IoT gateways), management of industrial equipment vulnerabilities, detection and prevention of OT malware
- **Incident Detection and Response in OT Environments**: threat hunting, identification of advanced attacks (APT), post-incident forensic analysis of ICS systems, SOC and SIEM dedicated to industrial infrastructures, behavioral analysis of industrial equipment to detect anomalies
- **Cryptography and Data Security in Constrained Environments**: encryption of industrial communications, identity protection and strong authentication (MFA, industrial PKI), securing exposed industrial APIs, preventing injection attacks on man-machine interfaces, protecting industrial data against exfiltration and manipulation
- **Automation & AI for OT Security**: detection of abnormal behavior via Machine Learning, automation of ICS vulnerability monitoring, industrial threat modeling (cyber kill chain applied to critical infrastructures)

TIMETABLE

19.06.2025
Opening of the call for projects during the event Digital Industry

30.08.2025
Submission of pre-projects
(1 pager + 3-5mn video pitch)

15.09.2025
Allocation of *Setup Boosters*

15.11.2025
Submission of full proposals

05.12.2025
Selection of projects and allocation of financial support by **[seal]** Committee

01.03.2026
Deadline for starting projects

28.02.2027
Closing date for projects

05-06.2027 (TBD)
Projects promotion event

CONTACT

If you have any questions or would like assistance in initiating a project, please contact:

Sandy Wetzel
[seal] Program Manager
+41 78 761 23 36
contact@seal-innovation.ch