APPEL À PROJETS #3

Ouverture 19.06.2025 | Clôture 15.11.2025

Les entreprises industrielles se digitalisent et s'exposent ainsi à de nouvelles menaces, telles que la compromission du fonctionnement des machines et la perturbation des lignes de production, ou encore l'espionnage industriel et l'exfiltration de données.

Cet appel à projets vise à stimuler l'innovation collaborative pour proposer des solutions répondant aux défis actuels de sécurité numérique des environnements industriels. Il est mené en collaboration avec le Groupement suisse de l'Industrie des Machines (GIM).

Nous invitons les chercheurs des Hautes Ecoles, les acteurs du secteur industriel et technologique et les experts en digitalisation et en cybersécurité à œuvrer ensemble pour renforcer la capacité d'innovation et de résilience de l'industrie face aux nouvelles cybermenaces, contribuant ainsi à préserver sa survie, sa pérennité et sa compétitivité.

CONTEXTE ET ENJEUX

L'essor de l'industrie 4.0 rime avec la numérisation des processus de production, la multiplication des capteurs et des actionneurs, la connexion d'objets intelligents et la communication *machine-to-machine,* le partage de données avec les constructeurs et les sous-traitants, ou encore intégration d'intelligences artificielles. Les systèmes industriels, autrefois isolés, sont ainsi de plus en plus connectés et intégrés aux technologies de l'information, augmentant donc fortement leur exposition aux cybermenaces.

La convergence des technologies de l'information (*IT – Information Technology*) et des technologies opérationnelles (*OT – Operational Technology*) a ainsi ouvert la voie à de nouvelles opportunités, mais aussi à des vulnérabilités accrues.

De nombreuses entreprises industrielles peinent encore à mettre en place des stratégies et des solutions de cybersécurité efficaces pour protéger leurs infrastructures et leurs données, assurer la continuité de leurs opérations et préserver leurs secrets de fabrication. Les environnements industriels présentent en effet des particularités (maintien en production de systèmes obsolètes, hétérogénéité des systèmes, multitudes de composants, protocoles propriétaires spécifiques, etc.) qui requièrent des exigences pointues et des nouvelles approches en matière de cybersécurité et de tests. Cela explique pourquoi la mise en œuvre de mesures de sécurité efficaces dans les réseaux OT est encore aujourd'hui largement insuffisante.

Les risques auxquelles s'exposent ces entreprises sont majeurs et les conséquences peuvent être dramatiques, notamment au niveau de la sécurité physique (perturbation de services vitaux, mise en danger des employés, etc.) et de la fuite de secrets industriels ; ce qui porte attention aux *hackers* qui y voient une nouvelle opportunité financière. Les cyberattaques ciblant les infrastructures industrielles ont ainsi connu une augmentation significative ces dernières années, avec des incidents notables impliquant des *ransomwares* (cryptolockage contre demande de rançon), des attaques sur les chaînes d'approvisionnement et des infiltrations dans les systèmes de supervision et d'acquisition de données.

Face à ce fléau, les réglementations imposant aux acteurs industriels de renforcer leur cybersécurité se multiplient. Il devient donc urgent d'intégrer la cybersécurité comme un pilier fondamental de la transformation numérique des entreprises industrielles afin que celles-ci puissent se moderniser dans un cadre de confiance (sûr, sécurité et robuste).

OBJECTIFS

Cet appel à projets vise à **explorer de nouvelles idées, étudier et élaborer des concepts disruptifs et développer des solutions techniques innovantes pour renforcer la cybersécurité et résilience des systèmes industriels**, et ainsi contribuer à la pérennité de l'industrie suisse et la protection de nos infrastructures critiques.

Plus spécifiquement, les objectifs sont les suivants (non-exhaustif) :

- **Renforcer la sécurisation des technologies opérationnelles (OT)** par l'adoption d'une approche holistique pour gérer les cybermenaces spécifiques aux environnements industriels et protéger les infrastructures critiques (systèmes de surveillance en temps réel, *hardening* des équipements industriels, contrôle des flux d'information, solutions de segmentation réseau, sécurité des protocoles industriels, mécanismes d'authentification avancés, protection contre les attaques par injection et compromission de *firmware*)
- **Favoriser une approche *Zero Trust* dans les environnements industriels et OT** par le développement d'architectures spécifiques aux infrastructures industrielles, tenant compte des contraintes de disponibilité et de performance (pare-feu industriels, segmentation des réseaux IT/OT et DMZ, sécurisation des communications *machine-to-machine*, accès distants sécurisés, mécanismes de chiffrement adaptés aux contraintes)
- **Développer des technologies et solutions de protection des systèmes de contrôle industriel (ICS)** capables de détecter des anomalies et de prévenir les intrusions sans perturber les opérations, notamment par l'utilisation de l'intelligence artificielle et de l'apprentissage automatique
- **Améliorer la gestion des risques et la conformité** en offrant une meilleure visibilité des risques et des menaces permettant une prise de décision efficace (outils pour l'évaluation dynamique des risques et la mise en conformité avec les réglementations)

DOMAINES

Les projets s'inscrivent notamment dans les domaines suivants (non-exhaustif) :

- **Sécurité des systèmes de contrôle industriel (ICS)** : conception d'architectures sécurisées des systèmes OT, sécurisation des protocoles industriels, gestion de la segmentation IT/OT, *hardening* des équipements industriels, solutions de détection d'anomalies adaptées aux environnements ICS
- **Sécurisation des réseaux industriels** : conception d'architectures réseau sécurisées pour l'OT (*firewalls* industriels, VLAN, micro-segmentation), IDS/IPS pour OT, gestion des accès distants sécurisés (fournisseurs, maintenance, sous-traitants, …), surveillance du trafic industriel (analyse des communications M2M), solutions de protection contre les attaques spécifiques sur l'OT (*replay attacks*, MITM, injection de commandes)
- **Sécurité des terminaux** : durcissement et protection des codes source des *firmwares* et *softwares*, protection des systèmes embarqués (automates, capteurs, passerelles IoT), gestion des vulnérabilités des équipements industriels, détection et prévention des malwares OT
- **Détection et réponse aux incidents OT** : *threat hunting* en environnement OT, identification des attaques avancées (APT), analyse forensique des systèmes ICS après incident, SOC et SIEM dédiés aux infrastructures industrielles, analyse comportementale des équipements industriels pour détecter les anomalies
- **Cryptographie et sécurisation des données en environnement contraint** : chiffrement des communications industrielles, protection des identités et authentification forte (MFA, PKI industrielle), sécurisation des API industrielles exposées, prévention des attaques par injection sur les interfaces homme-machine, protection des données industrielles contre l'exfiltration et la manipulation
- **Automatisation & IA pour la sécurité OT** : détection des comportements anormaux via *Machine Learning*, automatisation du monitoring des vulnérabilités ICS, modélisation des menaces industrielles (*cyber kill chain* appliquée aux infrastructures critiques)

CALENDRIER

19.06.2025
Ouverture de l'appel à projets dans le cadre de l'événement Digital Industry

30.08.2025
Soumission des pré-projets
(1 pager + vidéo pitch 3-5mn)

15.09.2025
Attribution des *Setup Boosters*

15.11.2025
Soumission des projets finaux

05.12.2025
Sélection des projets et attribution des soutiens financiers par le Comité **[seal]**

01.03.2026
Date limite pour débuter les projets

28.02.2027
Date limite de clôture des projets

05-06.2027 (TBD)
Evénement de valorisation des projets

CONTACT

Pour toute demande de renseignement ou besoin d'accompagnement pour initier un projet, veuillez prendre contact avec :

Sandy Wetzel
Responsable du Programme **[seal]**
+41 78 761 23 36
contact@seal-innovation.ch