



APPEL À PROJETS #4

Ouverture 24.09.2026 | Clôture 15.01.2027



L'écosystème aérospatial se digitalise à un rythme accéléré, connectant satellites, drones, systèmes de gestion de vol et infrastructures au sol. Cette interconnexion accrue expose le secteur à de nouvelles vulnérabilités stratégiques : brouillage et leurrage des communications, prises de contrôle à distance, exfiltration de données spatiales sensibles ou sabotage de systèmes embarqués.

Cet appel à projets vise à stimuler l'innovation collaborative pour développer des solutions de sécurité numérique robustes et adaptées aux contraintes extrêmes des environnements aérospatiaux. Il est mené en [collaboration avec swiss aeropole](#), le parc technologique vaudois spécialisé dans l'aérospatial et les technologies à forte valeur ajoutée, basé à Payerne.

Nous invitons les chercheurs des Hautes Écoles, les acteurs industriels du secteur aérospatial et de la défense, ainsi que les experts en cybersécurité à œuvrer ensemble pour renforcer la résilience des infrastructures critiques et préserver la souveraineté technologique vaudoise et suisse.

CONTEXTE ET ENJEUX

L'avènement du New Space, la multiplication des constellations de nanosatellites, l'automatisation de la gestion du trafic aérien (UTM/ATM) et l'intégration de composantes logicielles complexes dans les systèmes embarqués redéfinissent le secteur aérospatial. Longtemps protégés par leur isolement ou l'utilisation de technologies propriétaires spécifiques, les systèmes spatiaux et aéronautiques s'appuient désormais largement sur des « Commercial off-the-shelf » (COTS) et des réseaux IP connectés.

Cette dynamique s'accélère en Suisse occidentale avec des initiatives majeures telles que la Swiss Space Factory développée conjointement avec l'EPFL Innovation Park. Parallèlement, le cadre réglementaire se durcit avec l'entrée en application du règlement Part-IS (Information Security in civil aviation), imposant une maîtrise rigoureuse des risques cyber pesant sur les organisations aériennes, les exploitants d'aérodromes et les prestataires de navigation.

La convergence entre segment spatial, segment sol et terminaux utilisateurs ouvre la voie à de nouvelles opportunités d'innovation, mais crée également une surface d'attaque inédite.

Les contraintes propres au secteur (ressources matérielles et énergétiques très limitées à bord, latence des communications, impossibilité d'effectuer des interventions physiques de maintenance, longs cycles de vie des équipements) rendent l'application des mesures de cybersécurité traditionnelles particulièrement complexe. Les conséquences d'une cyberattaque dans ce domaine peuvent être critiques, allant de la perte de satellites stratégiques à la fuite de données de géolocalisation ou au piratage de systèmes de navigation.

Il devient donc indispensable d'intégrer la cybersécurité dès la conception (Security by Design) des systèmes aérospatiaux afin de garantir la confiance et la continuité des opérations dans ce secteur clé pour le canton de Vaud.

OBJECTIFS

Cet appel à projets vise à **explorer de nouvelles idées, élaborer des concepts novateurs et développer des solutions techniques de pointe pour sécuriser les systèmes embarqués et les infrastructures de communication aérospatiales.**

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

[Sécuriser les communications spatiales et aéronautiques] : Garantir l'intégrité, la confidentialité et la disponibilité des liaisons descendantes/montantes (uplink/downlink) et inter-satellites contre le brouillage (jamming), le leurrage (spoofing) et l'interception.

[Renforcer la sécurité des systèmes embarqués et du hardware] : Développer des architectures matérielles et logicielles résilientes adaptées aux contraintes d'énergie et de calcul à bord des satellites, sondes et vecteurs aériens.

[Protéger le segment sol, les centres de mission et les systèmes aéroportuaires] : Sécuriser les stations terriennes, les centres de contrôle de mission spatiale, ainsi que les systèmes opérationnels des aérodromes (gestion des mouvements au sol, autorisations PPR - Prior Permission Required, interfaces de télémessure et échanges de données avec les prestataires de navigation aérienne) face aux risques d'intrusion ou d'indisponibilité.

[Assurer la résilience des systèmes de navigation et de positionnement (GNSS)] : Développer des mécanismes de détection et de mitigation d'attaques ciblant la géolocalisation critique.

DOMAINES

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

[Cybersécurité du segment spatial & satellites] : Hardening des calculateurs bord, sécurisation des OS temps réel (RTOS), protection des mises à jour logicielles à distance (Over-The-Air), authentification des télécommandes (TC) et chiffrement des télémessures (TM).

[Chiffrement et cryptographie adaptée aux contraintes] : Cryptographie légère (Lightweight Cryptography), mise en œuvre de systèmes de distribution de clés (y compris Quantum Key Distribution - QKD) adaptées aux liaisons satellites.

[Sécurité des drones, des essais en vol et de la gestion du trafic aérien (UTM/ATM)] : Authentification des aéronefs non habités, sécurisation des protocoles de communication C2 (Command & Control), intégrité des liaisons lors d'essais en vol et prévention du piratage ou détournement de flottes autonomes.

[Résilience des stations sol, infrastructures critiques et opérations aéroportuaires : Détection d'intrusions (IDS/IPS) dédiée aux réseaux spatiaux et aéroportuaires, sécurisation des flux de données scientifiques et commerciales, et mise en conformité des systèmes d'information opérationnels avec **les standards Part-IS**.

[IA et autonomie sécurisée à bord : Algorithmes d'apprentissage embarqués pour la détection en temps réel d'anomalies ou de comportements malveillants sur les satellites sans dépendre du segment sol.

FINANCEMENT ET MODALITÉS

[Projet Standard : Soutien jusqu'à CHF 100'000.- (taux max. 90 %).

[Maxi-projet : Jusqu'à 1 projet d'envergure financé jusqu'à CHF 200'000.-.

[Setup Boosters : Forfaits de **CHF 5'000.-** (max. 4 boosters) pour la phase de montage des pré-projets retenus.

Consulter le Règlement des appels à projets pour le détail des critères d'éligibilité budgétaire.

CALENDRIER

24.09.2026

Annonce de thématique lors des Trust Valley Days

31.10.2026

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

15.11.2026

Attribution des *Setup Boosters*

(budget max. 4 – comité Resp. de programme)

15.01.2027

Clôture du dépôt des projets

29.01.2027

Évaluation et pré-sélection des projets par le Comité
de sélection (COSEC) **[seal]**

20.02.2027

Décision d'attribution finale des soutiens financiers
par le Comité de pilotage (COPIL) **[seal]**

01.06.2027

Date limite de démarrage des projets

31.05.2028

Clôture des projets (durée : 12 mois)

CONTACT

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

Yohan Martini

Responsable du Programme **[seal]**

+41 76 615 25 13

contact@seal-innovation.ch