Datum: 19.03.2026

bulletin.ch

Bulletin.ch / electrosuisse
8320 Fehraltorf
https://www.bulletin.ch/de/

Genre de média: Imprimé
Type de média: Médias professionnels
Tirage: 6'811
Parution: mensuel

Page: 32,33,34,35,36
Surface: 51'045 mm²

Hes·so

Ordre: 1073023
N° de thème: 375009
Référence: 6c7bf24e-f82b-4e73-b805-d18815c86a7c
Coupure Page: 1/5

Sécurisation des systèmes de transport intelligents coopératifs en Suisse

Feuille de route pour la mise en place d'un centre national des opérations de sécurité

Kilian Marty et al.

L'essor rapide des systèmes de transport intelligents coopératifs (Cooperative Intelligent Transport Systems, C-ITS) révolutionne la mobilité routière en Suisse. Ces systèmes permettent l'échange d'informations en temps réel entre véhicules, infrastructures et usagers, promettant une circulation plus sûre, efficace et durable. Cette interconnexion croissante, moteur d'innovation et d'optimisation du trafic, s'accompagne toutefois de nouveaux risques tels que la multiplication des interfaces numériques, qui élargit la surface d'attaque et rend les infrastructures critiques plus vulnérables aux cybermenaces.

Face à cette réalité, la cybersécurité devient un pilier incontournable de la mobilité moderne. Les incidents récents, comme le piratage de feux de signalisation aux Pays-Bas [1], illustrent les conséquences potentielles d'une faille de sécurité sur la fluidité du trafic et la sécurité publique. En réponse à ces défis, l'Office fédéral des routes (OFROU) a lancé un projet de recherche, réalisé par CertX et le centre de compétence Rosas (Robust and Safe Systems) de la Haute école d'ingénierie et d'architecture de Fribourg (HEIA-FR), dont l'objectif consistait à définir une feuille de route pour la mise en place d'un centre national des opérations de sécurité (Security Operations Center, SOC) dédié aux C-ITS. Ce SOC vise à assurer une surveillance continue, une détection rapide des menaces ainsi qu'une réponse coordonnée aux tentatives de cyberattaques et aux cyberincidents, tout en garantissant la conformité aux exigences réglementaires nationales et européennes.

Cet article détaille la démarche, les choix organisationnels et technologiques, ainsi que la feuille de route proposée pour la création d'un SOC national. Il met en lumière les défis spécifiques à l'intégration des systèmes IT et OT, la gestion complexe d'actifs de différents types ainsi que la nécessité d'une coordination étroite entre acteurs publics et privés. Enfin, il propose des perspectives de recherche et d'innovation pour renforcer la résilience et la confiance dans la mobilité connectée suisse.

Enjeux des CIT-S et contexte réglementaire

Les systèmes de transport intelligents coopératifs couvrent un large éventail d'applications concrètes qui transforment la mobilité et la gestion des infrastructures routières. En facilitant l'échange d'informations en temps réel entre véhicules, infrastructures et usagers, ces systèmes permettent l'émergence de nouveaux services axés sur la sécurité, l'efficacité et la fluidité du trafic. Leur déploiement s'appuie sur une diversité de cas d'usage déjà expérimentés ou en service aussi bien en Suisse qu'à l'international.

Parmi les applications, on retrouve la **gestion intelligente des feux de circulation :** certains feux adaptent leur cycle selon le trafic détecté ou accordent la priorité aux véhicules d'urgence grâce à la réception de signaux spécifiques. Une faille a été exploitée aux Pays-Bas par un hacker éthique qui a pu manipuler à distance des feux de signalisation, mettant en évidence la nécessité d'une cybersécurité renforcée dans ce domaine. Une autre application : la **gestion centralisée du trafic.** Les centres collectent et analysent les informations de capteurs, caméras et véhicules connectés pour optimiser la circulation, détecter les incidents et informer les usagers via des panneaux dynamiques et des applications mobiles. Les **unités**

Datum: 19.03.2026

bulletin.ch

Bulletin.ch / electrosuisse
8320 Fehraltorf
https://www.bulletin.ch/de/

Genre de média: Imprimé
Type de média: Médias professionnels
Tirage: 6'811
Parution: mensuel

Page: 32,33,34,35,36
Surface: 51'045 mm²

Hes·so

Ordre: 1073023
N° de thème: 375009
Référence: 6c7bf24e-f82b-4e73-b805-d18815c86a7c
Coupure Page: 2/5

routières connectées (Roadside Units, RSU), installées sur l'infrastructure routière – par exemple au niveau des tunnels, carrefours ou autoroutes –, mesurent le flux de véhicules, détectent des incidents et transmettent des alertes ou recommandations directement aux véhicules à proximité [2]. Sur les derniers modèles de véhicules, les **applications embarquées** permettent de recevoir des informations sur le temps restant jusqu'à ce qu'un feu passe au vert ou sur la vitesse recommandée pour fluidifier le trafic et réduire la consommation [3]. La **surveillance et la gestion des tunnels** reposent, pour leur part, sur des capteurs et la vidéosurveillance pour détecter les incidents et gérer la ventilation ou le contrôle de l'éclairage, ce qui assure une réaction rapide en cas d'événement. Enfin, les C-ITS transmettent en temps réel des **alertes de sécurité et notifications contextuelles** sur des dangers tels que les chantiers, les accidents ou les conditions météo défavorables, et ce, directement au conducteur via le tableau de bord ou son smartphone.

Les C-ITS s'intègrent dans une architecture technique complète qui relie plusieurs niveaux de gestion, de contrôle et de surveillance des infrastructures routières. La figure 1 met en évidence la structure des réseaux informatiques (IT) et opérationnels (OT) qui permettent d'orchestrer, de sécuriser et de superviser les différents composants du C-ITS.

Les C-ITS s'inscrivent ainsi dans le champ des infrastructures critiques, soumises à des exigences réglementaires strictes. En Suisse, le cadre légal (loi sur la sécurité de l'information LSI [4], loi sur la protection des données LPD [5]) s'aligne sur les directives européennes (RGPD [6], NIS2 [7], directive ITS révisée [8]) imposant la gestion des risques, la notification des incidents et la protection des données. Depuis avril 2025, la déclaration des cyberattaques sur les infrastructures critiques est devenue obliga-

Figure: Illustration générée par IA

RÉSUMÉ

Datum: 19.03.2026

bulletin.ch

Bulletin.ch / electrosuisse
8320 Fehraltorf
https://www.bulletin.ch/de/

Genre de média: Imprimé
Type de média: Médias professionnels
Tirage: 6'811
Parution: mensuel

Page: 32,33,34,35,36
Surface: 51'045 mm²

Hes·so

Ordre: 1073023
N° de thème: 375009
Référence: 6c7bf24e-f82b-4e73-b805-d18815c86a7c
Coupure Page: 3/5

toire auprès de l'Office fédéral de la cybersécurité (OFCS), renforçant l'importance d'une surveillance centralisée, tant proactive que réactive.

Pourquoi mettre en place un centre national des opérations de sécurité pour les C-ITS ?

La transformation numérique des infrastructures routières suisses, y compris des tunnels, carrefours intelligents, panneaux dynamiques et feux de circulation connectés, s'accompagne d'une interconnexion croissante entre équipements, véhicules et centres de gestion. Cette évolution expose toutefois le réseau routier à de nouveaux cyberrisques, tant sur le plan technique qu'opérationnel.

Les infrastructures routières incorporent désormais une multitude de systèmes connectés, tels que des capteurs routiers, des feux de circulation intelligents, des panneaux à messages variables, ainsi que des systèmes centralisés de gestion du trafic comme les TMS (Traffic Management Systems) et TMC (Traffic Management Centers), sans oublier les tunnels équipés de dispositifs de surveillance et de commande à distance. Cette diversité technologique, conjuguée à la convergence des technologies IT et OT, étend et complique considérablement la surface d'attaque à gérer, car une vulnérabilité au sein d'un seul composant peut provoquer des répercussions en cascade sur l'ensemble du réseau.

La mise en place d'un SOC national dédié aux C-ITS, centré sur les infrastructures routières, permettrait d'assurer une **surveillance continue et centralisée des équipements critiques** tels que les feux, tunnels, panneaux et RSU sur l'ensemble du territoire, avec la capacité de détecter en temps réel les anomalies et tentatives d'intrusion. De plus, un SOC national faciliterait la **coordination de la réponse aux incidents** entre tous les acteurs concernés, y compris les opérateurs routiers, les autorités cantonales et fédérales ainsi que les fournisseurs de technologies, ce qui est crucial pour limiter l'impact éventuel d'une attaque et rétablir rapidement le service.

Une **centralisation de la gestion des alertes** et de la notification réglementaire auprès de l'OFCS garantirait la conformité aux obligations légales et une réactivité optimale. Par ailleurs, la **mutualisation des compétences et des outils** au sein d'un SOC national permettrait d'optimiser l'utilisation des ressources humaines et technologiques, de faciliter l'accès à des expertises spécialisées et de bénéficier d'une cybersurveillance centralisée couvrant l'ensemble du réseau routier suisse. Enfin, **renforcer la confiance des usagers et la résilience des infrastructures** constitue un enjeu majeur pour la sécurité et la mobilité durable en Suisse.

Fonctions et organisation d'un SOC C-ITS

L'interconnexion des équipements, la diversité des technologies (IT/OT) et la multiplicité des acteurs rendent indispensable une approche structurée et centralisée pour surveiller, détecter et traiter les incidents de sécurité. Dans ce contexte, le SOC joue un rôle de tour de contrôle: il assure la protection continue des actifs critiques, anticipe les menaces émergentes et garantit la conformité aux exigences réglementaires nationales et européennes.

Le SOC s'articule autour des cinq fonctions clés du cadre NIST Cybersecurity Framework [9]:

- Gouverner: définir la stratégie, les politiques et la gestion des risques.
- Identifier: inventorier les actifs et évaluer les vulnérabilités.
- Détecter: surveiller les systèmes et réseaux pour repérer les anomalies.
- Répondre: coordonner les mesures de confinement et de remédiation.
- Protéger et restaurer: assurer la continuité des services essentiels.

Trois piliers soutiennent ces fonctions: des processus documentés; des technologies adaptées – SIEM (Security Information and Event Management), IDS/IPS (Intrusion Detection System/Intrusion Prevention System), SOAR (Security Orchestration, Automation and Response), outils d'inventaire; et des ressources humaines qualifiées.

Modèles organisationnels et stratégie de déploiement

Trois modèles de SOC ont été évalués. Le **modèle de SOC interne** offre un contrôle maximal, mais demande des investissements humains et tech-

Datum: 19.03.2026

bulletin.ch

Bulletin.ch / electrosuisse
8320 Fehraltorf
https://www.bulletin.ch/de/

Genre de média: Imprimé
Type de média: Médias professionnels
Tirage: 6'811
Parution: mensuel

Page: 32,33,34,35,36
Surface: 51'045 mm²

Hes·so

Ordre: 1073023
N° de thème: 375009
Référence: 6c7bf24e-f82b-4e73-b805-d18815c86a7c
Coupure Page: 4/5

niques importants. Le **modèle de SOC externalisé,** assuré par un fournisseur de services de sécurité gérés (Managed Security Service Provider, MSSP), permet d'optimiser l'expertise et les coûts, mais entraîne une perte de souveraineté. Enfin, le **modèle hybride** constitue un compromis, alliant le contrôle interne des incidents critiques à l'externalisation des tâches moins sensibles, bien que cette approche nécessite un effort plus important. Une analyse prenant en compte plusieurs critères (coûts, compétences, évolutivité, capacité d'intégration, gouvernance, contrôle, conformité, etc.) a révélé que le modèle hybride constitue la solution la plus équilibrée et la plus adaptée au contexte suisse, combinant efficacité opérationnelle, conformité réglementaire et flexibilité.

Parallèlement, différentes approches de déploiement du SOC ont été considérées. Le déploiement

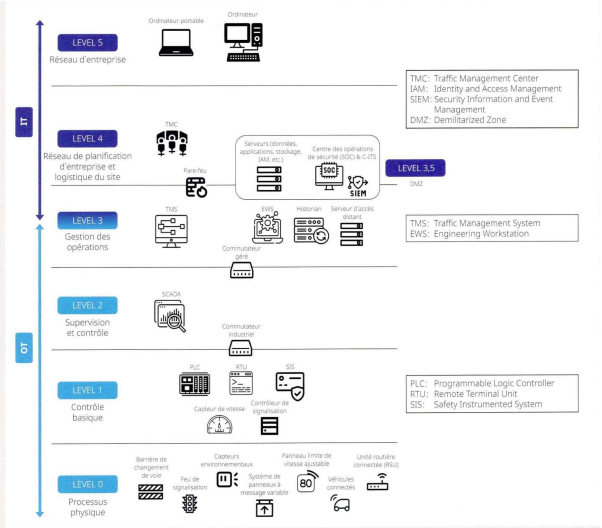

Figure 1 Le modèle Purdue appliqué au contexte du C-ITS.
Figure: CertX

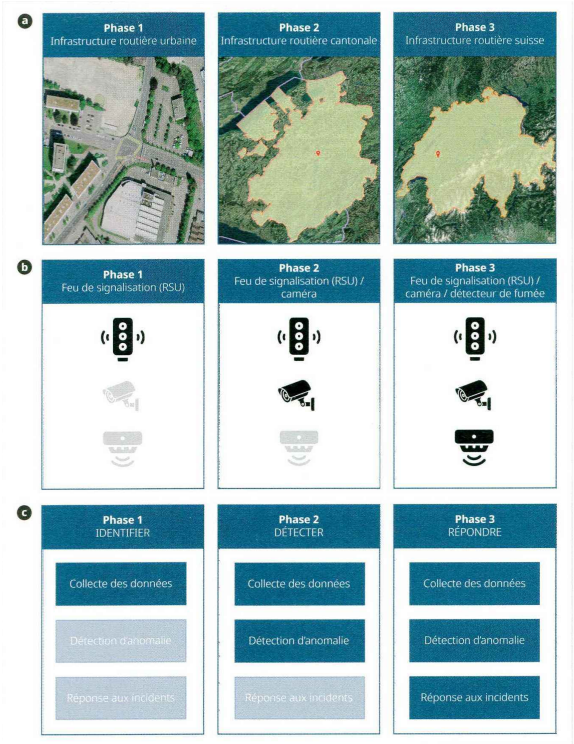

Figure 2 Approches de déploiements considérées : **a)** déploiement géographique, **b)** déploiement technologique, et **c)** déploiement par capacité fonctionnelle.
Figure: CertX

Datum: 19.03.2026

bulletin.ch

Bulletin.ch / electrosuisse
8320 Fehraltorf
https://www.bulletin.ch/de/

Genre de média: Imprimé
Type de média: Médias professionnels
Tirage: 6'811
Parution: mensuel

Page: 32,33,34,35,36
Surface: 51'045 mm²

Hes·so

Ordre: 1073023
N° de thème: 375009
Référence:
6c7bf24e-f82b-4e73-b805-d18815c86a7c
Coupure Page: 5/5

géographique (figure 2a) consiste en une extension progressive de la couverture de surveillance, débutant par une zone urbaine pilote, puis s'étendant aux niveaux cantonaux avant de couvrir l'ensemble du territoire national. Le déploiement technologique (figure 2b) prévoit l'intégration progressive des diverses technologies et capteurs tels que les RSU, les caméras et les panneaux à messages dynamiques. Enfin, le déploiement par capacité fonctionnelle (figure 2c) implique une montée en puissance graduelle des fonctionnalités du SOC, de la collecte de données à la gestion complète des incidents. Les capacités essentielles (identifier, détecter, répondre) sont couvertes dès le départ.

La stratégie retenue combine les approches technologique et géographique, tout en veillant à ce que les capacités essentielles (identifier, détecter, répondre) soient opérationnelles dès le début. L'implémentation initiale ciblera une technologie spécifique (par exemple, les unités routières de feux de circulation) dans une zone urbaine pilote. Au fur et à mesure de la montée en maturité, le SOC étendra sa couverture à d'autres technologies et zones géographiques, garantissant ainsi une valeur ajoutée rapide et une évolutivité optimale.

Feuille de route pour la mise en œuvre d'un SOC

La mise en place d'un SOC dédié aux C-ITS nécessiterait une démarche structurée et progressive. La feuille de route recommandée s'articulerait autour des cinq phases illustrées dans la figure 3, chacune répondant à des objectifs précis pour garantir l'efficacité et la pérennité du dispositif.

- Fondation: définition du mandat, gouvernance, analyse des besoins, allocation des ressources.
- Construction: mise en place de l'infrastructure, intégration des outils, formation des équipes.