Datum: 19.03.2026

bulletin.ch

Hes·so

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: 36,37,38
Surface: 22'950 mm²

Ordre: 1073023
N° de thème: 375009
Référence:
6c298ec7-2c8a-41b3-a5f9-290a06ea94af
Coupure Page: 1/3

Sicherheit kooperativer intelligenter Verkehrssysteme in der Schweiz

Fahrplan für die Einrichtung eines nationalen Sicherheitsoperationszentrums

Der rasante Aufstieg kooperativer intelligenter Verkehrssysteme (Cooperative Intelligent Transport Systems, C-ITS) revolutioniert den Strassenverkehr. Diese Systeme ermöglichen den Austausch von Informationen in Echtzeit zwischen Fahrzeugen, Infrastrukturen und Nutzern und versprechen einen sichereren, effizienteren und nachhaltigeren Verkehr. Diese Vernetzung birgt jedoch auch neue Risiken: Die Vervielfachung digitaler Schnittstellen vergrössert beispielsweise die Angriffsfläche und macht kritische Infrastrukturen anfälliger für Cyberbedrohungen.

Als Antwort auf diese Herausforderungen hat das Astra ein Forschungsprojekt initiiert, das von CertX und dem Kompetenzzentrum Rosas der Hochschule für Technik und Architektur Freiburg (HEIA-FR) durchgeführt wurde: Ziel war es, einen Fahrplan für die Einrichtung eines nationalen Sicherheitsoperationszentrums (Security Operations Center, SOC) für C-ITS zu definieren. Dieses SOC soll eine kontinuierliche Überwachung, eine schnelle Erkennung von Bedrohungen sowie eine koordinierte Reaktion auf Cyberangriffe und Cybervorfälle gewährleisten und gleichzeitig die Einhaltung der nationalen und europäischen Vorschriften sicherstellen.

Laut den Studienautoren würde die Einrichtung eines C-ITS-SOC in der Schweiz mehrere Herausforderungen mit sich bringen: Neben der technologischen Komplexität (IT/OT-Integration, Verwaltung von Altsystemen, Erfassung heterogener Logs sowie Management und Aktualisierung diverser Tools) würde das Projekt mit einem Fachkräftemangel konfrontiert sein. Die Koordination zwischen öffentlichen, privaten und akademischen Akteuren wäre auch eine grosse Herausforderung, besonders im Hinblick auf die Zusammenarbeit und den Austausch von Informationen und Bedrohungsindikatoren. Die Autoren empfehlen daher die Schaffung eines nationalen SOC auf der Grundlage eines hybriden Modells, d. h. einer Kombination aus interner Kontrolle kritischer Vorfälle und Auslagerung weniger sensibler Aufgaben, sowie auf der Basis eines schrittweisen Fahrplans: Die Einführung würde einen gezielten technologischen Start, beispielsweise die Überwachung der RSU von Ampeln, mit einer schrittweisen geografischen Ausweitung verbinden, beginnend mit einem städtischen Pilotgebiet bis hin zu einer nationalen Abdeckung. Die Abdeckung der Schlüsselfunktionen des SOC (wie Identifizierung, Erkennung und Reaktion auf Vorfälle) würde bereits in der ersten Phase der Einführung gewährleistet sein.

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: 36,37,38
Surface: 22'950 mm²

Hes·so

Ordre: 1073023
N° de thème: 375009
Référence: 6c298ec7-2c8a-41b3-a5f9-290a06ea94af
Coupure Page: 2/3

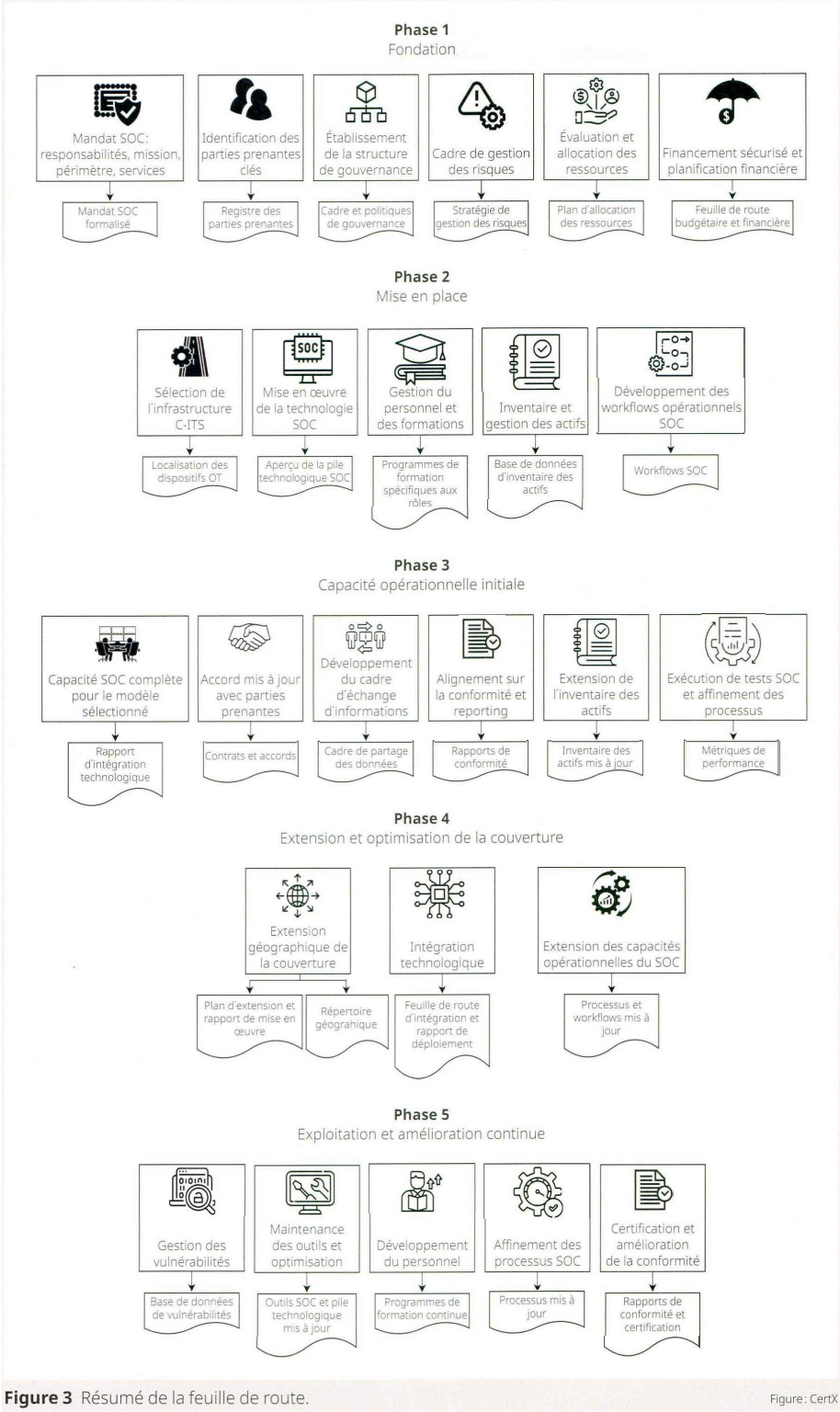

Figure 3 Résumé de la feuille de route. Figure: CertX

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: 36,37,38
Surface: 22'950 mm²

Hes·so

Ordre: 1073023
N° de thème: 375009
Référence: 6c298ec7-2c8a-41b3-a5f9-290a06ea94af
Coupure Page: 3/3

- Capacité opérationnelle initiale: exploitation sur un périmètre restreint, mise en conformité, tests de processus.
- Extension et optimisation: élargissement à de nouveaux territoires et technologies, optimisation des workflows et de l'automatisation.
- Exploitation et amélioration continue: maintien, adaptation et certification du SOC, formation continue, revue annuelle des performances.

La mise en œuvre de la feuille de route SOC risque d'être complexe en raison de la nécessité de gérer plusieurs activités et phases en parallèle. Une séquence d'étapes logique est certes définie, mais en pratique, plusieurs volets, tels que la mise en place technique, l'inventaire des actifs et la coordination des parties prenantes, devront probablement être menés simultanément. Une priorisation et un ordonnancement appropriés de ces activités sont essentiels pour garantir la cohérence et maintenir la dynamique tout au long du projet.

Défis et perspectives

La mise en place d'un SOC C-ITS en Suisse soulèverait plusieurs défis, notamment la complexité technologique liée à l'intégration IT/OT, à la gestion des systèmes hérités, à la collecte de logs hétérogènes, ainsi qu'à la gestion et à la mise à jour d'un large éventail d'outils. Sur le plan des ressources humaines, le projet serait confronté à une pénurie de spécialistes, d'où la nécessité d'une formation continue et d'efforts pour rendre les postes attractifs. La coordination entre les acteurs publics, privés et académiques représente également un défi important, en particulier pour la collaboration et le partage d'informations et d'indicateurs de menace. Enfin, il faudrait adapter le SOC aux évolutions réglementaires nationales et européennes pour assurer la conformité.

Des opportunités de recherche existent, notamment dans le développement d'outils d'inventaire automatisé, la simulation d'incidents et l'expérimentation pilote en milieu urbain.

Conclusion

La cybersécurisation des C-ITS constitue un enjeu stratégique pour la mobilité suisse. La création d'un SOC national, fondé sur un modèle hybride et une feuille de route progressive, constitue la réponse la mieux adaptée pour garantir la résilience, la conformité et la confiance dans les infrastructures de transport connectées. L'implication de tous les acteurs, la mutualisation des compétences et l'adaptabilité aux nouveaux risques constitueront les clés du succès de cette transformation numérique.

Références

[1] NL Times, «Tens of thousands of Dutch traffic lights vulnerable to hackers: report», 7 octobre 2024.
[2] Audi Newsroom, «Audi, Applied Information and Temple launch C-V2X school safety development program in Georgia», 27 octobre 2020.
[3] Volkswagen Newsroom, «Technical milestone in road safety: experts praise Volkswagen's Car2X technology», 19 mars 2020.
[4] Loi fédérale sur la sécurité de l'information au sein de la Confédération (Loi sur la sécurité de l'information, LSI) du 18 décembre 2020, situation au 1er octobre 2025.
[5] Loi fédérale sur la protection des données (LPD) du 25 septembre 2020, situation au 7 juillet 2025.
[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[7] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive).
[8] Directive (EU) 2023/2661 of the European Parliament and of the Council of 22 November 2023 amending Directive 2010/40/EU on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport.
[9] A. Nelson, S. Rekhi, M. Souppaya, K. Scarfone, «Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile», NIST Special Publication 800-61r3, National Institute of Standards and Technology, avril 2025.

Liens

> Rapport du projet «Roadmap for Swiss C-ITS Security Operation Center»: www.aramis.admin.ch/Texte/?ProjectID=53691
> Rapport du projet précédent «Cyber Threat Intelligence Framework and Recommendations for C-ITS»: www.aramis.admin.ch/Texte/?ProjectID=49812

Auteurs

Kilian Marty est consultant en cybersécurité et CEO de CertX Solutions.
> CertX Solutions, 1700 Fribourg
> kilian.marty@certx.com

Prof. Michael Mäder est professeur en informatique et systèmes de communication à la Haute école d'ingénierie et d'architecture de Fribourg.
> HEIA-FR, 1700 Fribourg
> michael.maeder@hefr.ch

Gabriel Python est chef de projet et chercheur en cybersécurité chez CertX SA.
> CertX SA, 1700 Fribourg
> gabriel.python@certx.com

Alexia Schmid est consultante en cybersécurité chez CertX Solutions.
> alexia.schmid@certx.com

Loan Bétend est responsable du domaine cybersécurité chez CertX SA.
> loan.betend@certx.com