Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK
Département fédéral de l'environnement, des transports, de l'énergie et de la communication DETEC
Dipartimento federale dell'ambiente, dei trasporti, dell'energia e delle comunicazioni DATEC

Bundesamt für Strassen
Office fédéral des routes
Ufficio federale delle Strade

Roadmap for Swiss C-ITS Security Operation Center

Feuille de route pour centre opérationnel de cyber sécurité suisse des C-ITS

Roadmap für Schweizer C-ITS Security Operation Center

CertX SA
Kilian Marty
Loan Bétend
Alexia Schmid
Gabriel Python

ROSAS
Michael Mäder
Denis Rosset
Urban Willi
Tony Licata

Forschungsprojekt MB4_20_02G_01 auf Antrag der Arbeitsgruppe Mobilität 4.0 (MB4)

October 2025 **1805**

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK
Département fédéral de l'environnement, des transports, de l'énergie et de la communication DETEC
Dipartimento federale dell'ambiente, dei trasporti, dell'energia e delle comunicazioni DATEC

Bundesamt für Strassen
Office fédéral des routes
Ufficio federale delle Strade

Roadmap for Swiss C-ITS Security Operation Center

Feuille de route pour centre opérationnel de cyber sécurité suisse des C-ITS

Roadmap für Schweizer C-ITS Security Operation Center

CertX SA
Kilian Marty
Loan Bétend
Alexia Schmid
Gabriel Python

ROSAS
Michael Mäder
Denis Rosset
Urban Willi
Tony Licata

Forschungsprojekt MB4_20_02G_01 auf Antrag der Arbeitsgruppe Mobilität 4.0 (MB4)

October 2025 **1805**

Impressum

Research center and project team

Project management
Kilian Marty (CertX)
Michael Mäder (HEIA-FR/ROSAS)

Members
Loan Bétend (CertX)
Alexia Schmid (CertX)
Gabriel Python (CertX)
Denis Rosset (HEIA-FR/ROSAS)
Urban Willi (HEIA-FR/ROSAS)
Tony Licata (HEIA-FR/ROSAS)

Accompanying Commission

President
Bertrand Ndzana

Members
Jolanda Geringer
Sophie Nägeli – [from project start until 01.03.2024]
Bettina Mavrommatis – [from 01.03.2024 until project end]
Patricia Egger
Florian Leibenzeder
Samuel Rossier
Erik Wilhelm
Christoph Tschudin
Bruno Vuillemin
Marc-Antoine Matthey

Applicant

Working Group Mobility 4.0 (MB4)

Source

This document is available for free download at http://www.mobilityplatform.ch

Table of contents

Summary

Introduction and project objectives

Cooperative Intelligent Transport Systems (C-ITS) and Vehicle-to-anything (V2X) communications are transforming mobility by enabling vehicles, infrastructure and road users to exchange information for safer and more efficient transport. However, as their adoption grows and because of their exposure, these systems become increasingly attractive targets for cyber threats. C-ITS being part of critical national infrastructure, their cybersecurity is paramount and requires both proactive and reactive risk management. A previous Mobility 4.0 (MB4) call MB4_20_02C_01 [41] focused on proactive measures addressing early-stage threat analysis and risk assessment. This report focuses on reactive measures, particularly the establishment of a national Security Operations Center (SOC) for C-ITS.

The project's objectives are to assess the necessity of a national SOC tailored to the C-ITS context, to explore viable models for its establishment and operation, and to provide a practical roadmap for implementation within the Swiss context.

C-ITS overview

C-ITS represent an evolution of traditional ITS, enabling real-time information exchange between vehicles, infrastructures and road users to enhance safety and efficiency. Unlike conventional ITS, C-ITS relies on extensive interactive communication (Vehicle-to-Vehicle or V2V and Vehicle-to-Infrastructure or V2I), making cybersecurity a critical concern as the attack surface expands.

The C-ITS ecosystem is complex, involving multiple stakeholders, including government agencies, transportation authorities, technology providers, telecommunication companies, public and private sector partnerships, automotive manufacturers, research institutions and end users.

Regulatory landscape and key authorities

The C-ITS environment involves a combination of international standards, European frameworks (GDPR [1], NIS2 [11], CRA [2], revised ITS Directive [12]) and Swiss national law. The revised ITS Directive introduces requirements for secure communications with a PKI-based trust model aligned with the European Certificate Trust List (ECTL) [19], interoperable and machine-readable traffic data format, National Access Point (NAP)-style data sharing [18], GDPR-compliant privacy safeguards and cross-border incident response plans. These regulations and directives are to be carefully considered during the development of the SOC to ensure alignment with them.

Switzerland's regulatory landscape includes the ICT minimum standard for critical sectors, which is aligned with the NIST Cybersecurity Framework [23]. It also contains the nFADP [4], which is compliant with GDPR, and the FAISC [5], which sets mandatory cybersecurity requirements for critical infrastructures, including C-ITS. Additionally, effective from April 1st, 2025, the Swiss Federal Council has introduced a mandatory reporting requirement for cyberattacks targeting critical infrastructure. Reports must be received by the NCSC [42] within 24 hours.

Key national authorities include the National Cyber Security Centre (NCSC), which is the federal competence center for cybersecurity and the first point of contact for businesses, public services and critical infrastructure operators regarding cyber incidents. Another important agency is the Federal Roads Office (FEDRO), the authority on road infrastructure at the national level. FEDRO plays a central role in C-ITS policy, deployment and guidance, developing reference documents on C-ITS management, national communication network for C-ITS, and OT security.

SOC necessity

The C-ITS environment comprises a diverse set of interconnected assets, including roadside infrastructure, centralized management systems and communication networks. The latter are typically divided into IT and OT components, each with unique cybersecurity needs. Growing interconnectivity increases the attack surface and risk of incidents, which can lead to major disruptions. The complexity is heightened by diverse asset ownership, legacy systems, and fragmented incident response responsibilities.

To address these challenges, the establishment of a centralized SOC is proposed as a pillar for C-ITS cybersecurity. By providing continuous monitoring, threat detection and coordinated response across all critical C-ITS assets, the SOC would act as the structure enabling the efficient collaboration of these multiple entities.

SOC functions and structure

The primary functions of the SOC are closely aligned with the core functions of the NIST Cybersecurity Framework:

- Govern: Establishes the necessary framework for all other functions to operate cohesively, providing strategic direction, policies and governance structures, managing risk and overseeing security controls;
- Identify: Maintains an up-to-date understanding of C-ITS assets, resources and associated cybersecurity risks, providing the basis for risk management;
- Detect: Continuously monitors systems and networks to identify cybersecurity events;
- Respond: Coordinates actions to contain and mitigate detected incidents, ensuring impact minimization;
- Protect and Recover (supporting functions): Implements protective measures to ensure the provision of essential services and support resilience and restoration services post-incident.

These core functions are enabled by three foundational pillars (*Fig. 1*):

- Processes: Defined procedures for monitoring, detection, incident response and escalation, tailored to C-ITS environments;
- Technologies: Tools for asset discovery, threat detection, event correlation, response automation and more, covering both the IT and OT domains;
- Human resources: Skilled personnel ensuring effective SOC performance.

By integrating these three pillars with the guidance of the NIST Cybersecurity Framework, the proposed SOC ensures a comprehensive and structured approach aligned with international best practices in cybersecurity.

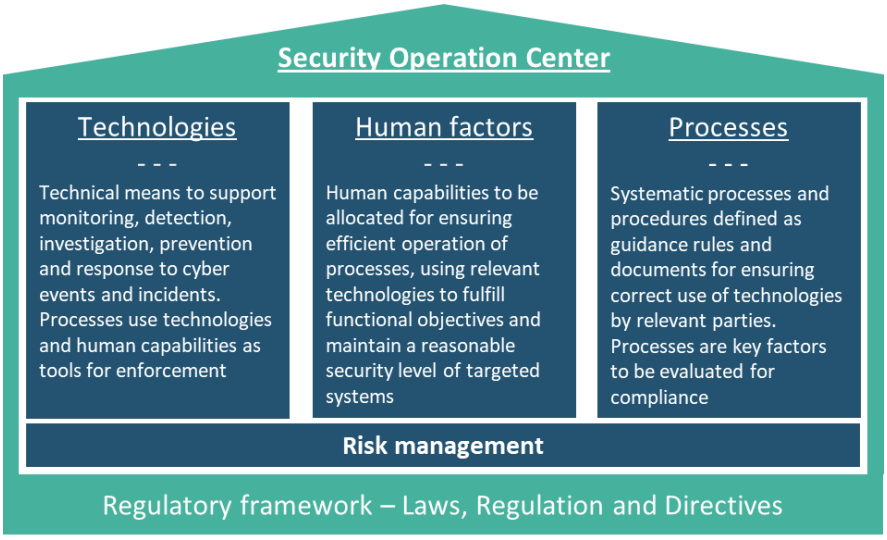


***Fig. 1** SOC 3 pillars.*

Swiss SOC for C-ITS

In planning a SOC for C-ITS in Switzerland, the main discussions centered around identifying the best organizational structure and deployment approach.

Three main organizational models were considered:

- In-house SOC: All monitoring, detection, and response activities are managed internally, offering maximum control and data sovereignty but requiring significant investment in personnel, infrastructure and ongoing operational costs;
- Outsourced SOC (MSSP): All SOC functions are delegated to a Managed Security Service Provider, leveraging external expertise and being cost-effective, but introducing challenges regarding data confidentiality, regulatory compliance and loss of direct oversight;
- Hybrid SOC: Core SOC functions such as sensitive incident management and decision-making are retained in-house while less sensitive tasks (e.g., global threat monitoring, log analysis) are outsourced to external providers, combining internal control and expertise with the scalability, tooling capabilities, and human resources of MSSPs.

A multi-criteria matrix was developed to objectively compare in-house, MSSP and hybrid SOC models. Assessment criteria included cost, governance and compliance, expertise, customization, scalability, implementation speed, technology adoption, operational complexity and long-term flexibility. The hybrid SOC model achieved the highest overall score. It was identified as offering the best balance between control and flexibility, placing sensitive operations under direct supervision while outsourcing selected functions to MSSPs for scalable support and specialized expertise. This model also ensures data sovereignty and facilitates compliance with regulations while optimizing costs and minimizing the burden of infrastructure and staffing.

Three primary deployment methods were considered:

- Geographical deployment: The SOC is deployed in phases based on physical locations, beginning for example with high-risk/ priority areas before expanding to other locations;
- Technological deployment: Deployment is organized around specific technologies or sensor type (e.g., traffic light RSUs, surveillance cameras or smoke detectors). Each technology is integrated and secured in stages with the SOC progressively adding security tools, data processing capabilities and incident response mechanisms for one technology before moving on to the next;
- Capability deployment: This approach focuses on the progressive development of the SOC's functional maturity. It starts with foundational capabilities such as data collection, moves on to anomaly detection and threat analysis and ends with full incident response and mitigation. Each phase improves the effectiveness and readiness of the SOC.

The chosen deployment strategy follows a hybrid approach, combining both technological (*Fig. 3*) and geographical (Fig. 2) approaches, while ensuring that all core capabilities (*Fig. 4*) (Identify, Detect, Respond) are operational from the outset. The initial implementation will focus on securing a single technology (e.g., traffic light RSUs) within a targeted urban area. As the SOC matures, it will scale through the addition of technologies and the integration of broader geographic areas (progressing from local to cantonal and national levels). Covering all capability phases from the beginning allows for rapid establishment of a minimum viable SOC, delivering immediate value. Scalability follows both in terms of technology integration and geographic coverage.

Fig. 2 *Geographic deployment example.*

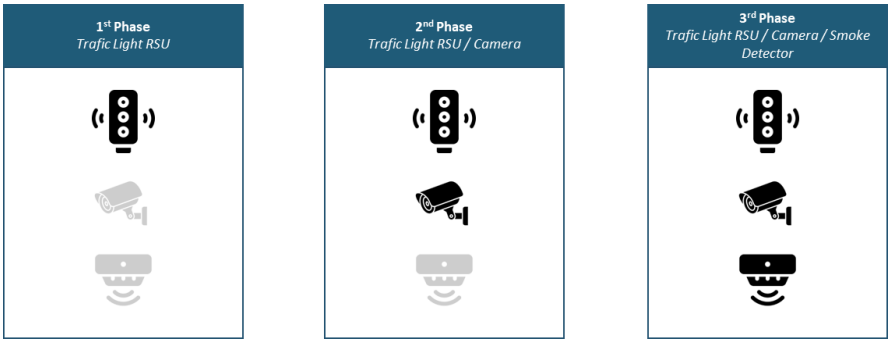


Fig. 3 *Technological deployment example.*

Fig. 4 *Capability deployment example.*

Roadmap for SOC implementation

The proposed SOC implementation roadmap for C-ITS is made up of 6 phases. The phases and their content are inspired by the ENISA report and literature on global SOC implementation strategies [43]. The roadmap ranges from foundational planning to continuous improvement, with initial operating capability expected after 18 months.

The foundation phase sets the base for the SOC. Key activities include defining the SOC's mission, objectives and key stakeholders, conducting a comprehensive needs assessment, securing initial funding and resources and establishing high-level requirements, policies and governance structures. This phase ensures all the prerequisites and guiding principles are in place before technical implementation begins.

The build-out phase establishes the physical and technical infrastructure required for SOC operations. This involves setting up the SOC facility, acquiring the necessary tools and technologies, defining and documenting operational processes, deploying the first targeted

C-ITS technology, and initiating the asset inventory process. The first operations of the SOC are conducted in this phase.

The initial operating capability phase marks the stage where the SOC becomes operational for the first time, providing full core capabilities (Identify, Detect, Respond) for the chosen technology within a selected urban area. At this stage, mandatory reporting mechanisms are in place. The SOC can manage security incidents and is ready to scale up.

The coverage extension and optimization phase focuses primarily on extending coverage to additional technologies and broader geographical areas, and secondarily on optimizing SOC processes, workflows and inter-organizational collaboration and on improving information sharing and threat intelligence capabilities. This is a longer phase in which the coverage of the SOC can be extended while existing operations, processes and workflows are refined.

The operation and continuous improvement phase, which is the final phase, focuses on maintaining and improving the SOC. This is achieved through regular reviews and updates of SOC operations, tools and processes, adapting them to changing security threats and regulatory requirements. Efforts in training, process improvement and technology upgrades ensure that the SOC can remain resilient, effective and aligned with best practices over time (*Fig. 5*).

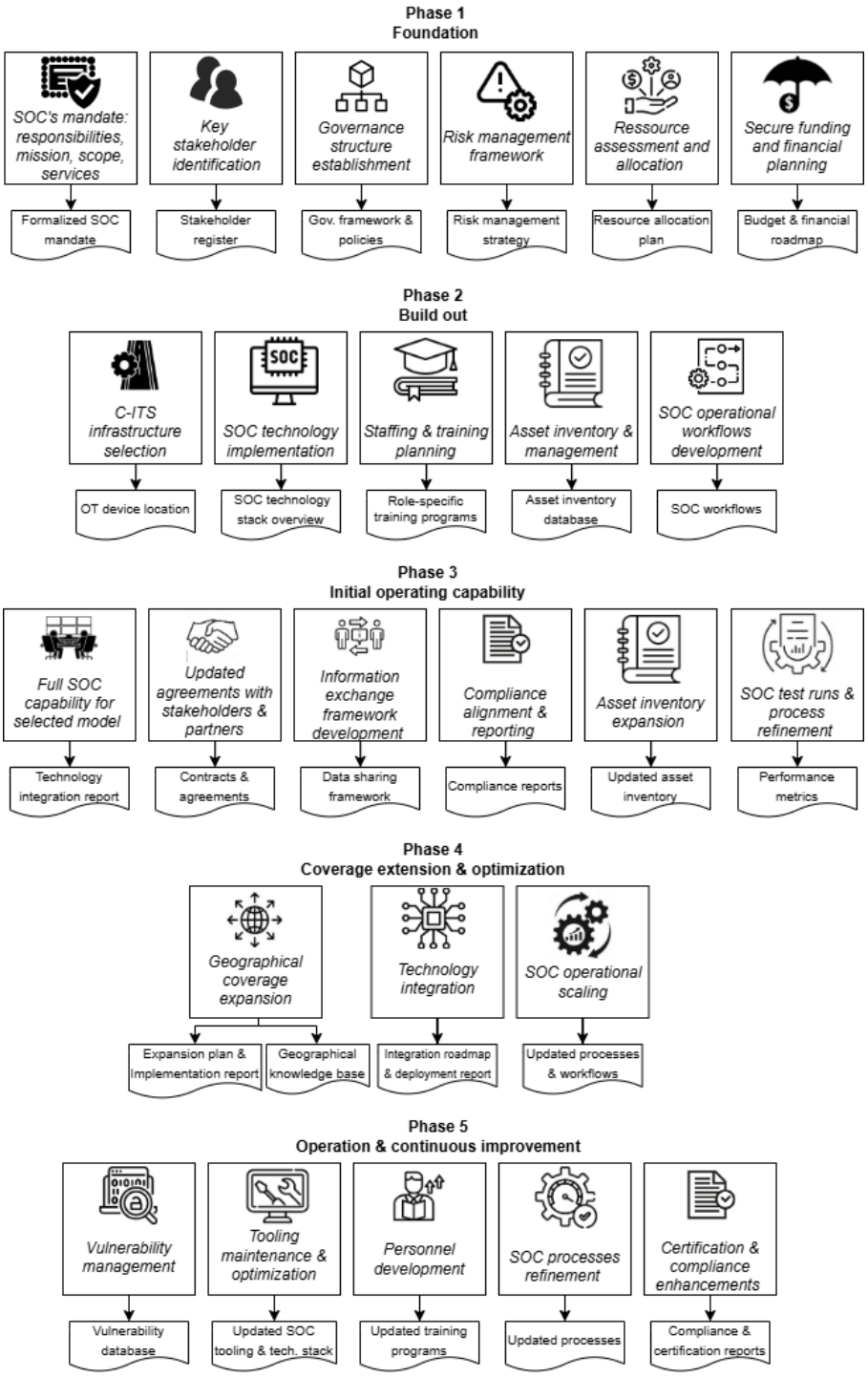


Fig. 5 *Phases summary.*

Implementation time frame and cost estimates

The national rollout (phases 1 to 4) is expected to be completed within 36 months, with ongoing operations (phase 5) continuing thereafter. Total implementation costs are estimated at CHF 6.2 million for the first 36 months, followed by recurring operational costs of approximately CHF 188’000 per month for continuous improvement and maintenance.

Key challenges

The development and anticipated implementation of the SOC roadmap for Swiss C-ITS revealed several strategic and operational challenges. Selecting the optimal organizational

model (in-house, MSSP or hybrid) and deployment approach (geographic, technological or capability-based) required careful consideration of trade-offs between control, flexibility, feasibility, resource allocation and compliance. While the roadmap outlines a phased implementation, it is anticipated that real-world execution will require overlapping activities and continuous adaptation to real-world constraints.

Technological integration is anticipated to be complex, given the mix of IT and OT systems, including legacy systems not designed with cybersecurity in mind. Building a comprehensive asset inventory is both essential and challenging, requiring coordination across multiple stakeholders and system owners. Without this comprehensive asset inventory, a correct risk analysis is not possible.

Prioritizing rollout-both geographically and technologically will require careful planning, balancing feasibility with a risk-based approach focusing on the most vulnerable and impactful areas first. Operational challenges such as budgeting, managing timelines and maintaining stakeholders will require ongoing attention throughout the project. Strong leadership, support from top management and specialized expertise, especially in the early phases, will be critical for ensuring successful implementation and long-term resilience.

Conclusion

A national SOC is essential to secure Switzerland’s C-ITS infrastructure, which is classified as critical infrastructure and subject to cybersecurity regulations. A decentralized or territorial SOC model was deemed unfeasible due to its operational complexity. Instead, a centralized SOC with a hybrid governance model combining MSSP and in-house operations was identified as the best option.

The roadmap outlines a phased implementation, starting with organizational and governance aspects, then developing full capabilities on a limited scale and expanding geographically and technologically over time. This approach ensures rapid initial readiness and sets a solid foundation on which to expand.

Résumé

Introduction et objectifs du projet

Les Systèmes de Transport Intelligents Coopératifs (C-ITS) et les communications Véhicule-à-Tout (V2X) révolutionnent la mobilité en permettant aux véhicules, aux infrastructures et aux usagers de la route de partager des informations en temps réel, rendant les transports plus sûrs et plus efficaces. Toutefois, à mesure que ces systèmes se généralisent et deviennent plus exposés, ils attirent davantage l'attention des cybercriminels. Étant donné que les C-ITS font partie des infrastructures critiques nationales, leur cybersécurité doit être assurée par une gestion proactive et réactive des risques. Un précédent appel Mobility 4.0 (MB4) MB4_20_02C_01 [41] a déjà traité des mesures proactives, telles que l'analyse précoce des menaces et l'évaluation des risques. Le présent rapport se concentre sur les mesures réactives, en particulier sur la création d'un Centre national des Opérations de Sécurité (SOC) dédié aux C-ITS.

Ce projet vise à évaluer la nécessité d'un SOC national adapté au contexte des C-ITS, à explorer des modèles organisationnels viables pour sa création et son fonctionnement, et à proposer une feuille de route pragmatique pour sa mise en œuvre en Suisse.

Présentation des C-ITS

Les C-ITS représentent une avancée majeure par rapport aux systèmes de transport intelligents traditionnels, en facilitant un échange d'informations dynamique entre véhicules, infrastructures et usagers de la route, dans le but d'améliorer la sécurité et l'efficacité du trafic. Contrairement aux ITS classiques, les C-ITS reposent sur des communications interactives étendues (Véhicule-à-Véhicule, V2V, et Véhicule-à-Infrastructure, V2I), ce qui rend la cybersécurité d'autant plus cruciale en raison d'une surface d'attaque élargie.

L'écosystème C-ITS est particulièrement complexe et fédère de nombreux acteurs : agences gouvernementales, autorités de transport, fournisseurs de technologies, opérateurs télécoms, partenariats public-privé, constructeurs automobiles, instituts de recherche et usagers finaux.

Cadre réglementaire et autorités clés

L'environnement C-ITS s'appuie sur un ensemble de normes internationales, de cadres européens (RGPD [1], NIS2 [11], CRA [2], directive ITS révisée [12]) et de la législation nationale suisse. La directive ITS révisée impose des exigences strictes en matière de communications sécurisées, avec un modèle de confiance basé sur une infrastructure à clés publiques (PKI) alignée sur la liste européenne de confiance des certificats (ECTL) [19], un format de données de trafic interopérable et lisible par machine, un partage de données via un Point d'Accès National (NAP) [18], des garanties de confidentialité conformes au RGPD, ainsi que des plans de réponse aux incidents transfrontaliers. Toutes ces réglementations doivent être intégrées dans la conception du SOC pour garantir la conformité.

Le cadre réglementaire suisse inclut la norme minimale TIC pour les secteurs critiques, alignée sur le NIST Cybersecurity Framework [23]. Il comprend également la nLPD [4], conforme au RGPD, et la FAISC, qui définit des exigences obligatoires en cybersécurité pour les infrastructures critiques, dont les C-ITS. À partir du 1er avril 2025, le Conseil fédéral suisse impose en outre une obligation de déclaration des cyberattaques visant les infrastructures critiques, avec un délai de signalement de 24 heures auprès du NCSC [42].

Les principales autorités nationales sont le Centre national pour la cybersécurité (NCSC), qui agit comme centre fédéral de compétences en cybersécurité et premier point de contact pour les entreprises, services publics et exploitants d'infrastructures critiques en cas d'incident, ainsi que l'Office fédéral des routes (OFROU), responsable des infrastructures

routières au niveau national. L'OFROU joue un rôle central dans la définition de la politique, le déploiement et l'orientation des C-ITS, en élaborant des documents de référence sur leur gestion, le réseau national de communication et la sécurité OT.

Nécessité d'un SOC

L'environnement C-ITS regroupe un large éventail d'actifs interconnectés : infrastructures routières, systèmes de gestion centralisés et réseaux de communication, eux-mêmes divisés en composantes IT et OT, chacune avec des exigences de cybersécurité spécifiques. Cette interconnexion croissante élargit la surface d'attaque et accroît le risque d'incidents susceptibles de provoquer des perturbations majeures. La diversité des propriétaires d'actifs, la présence de systèmes hérités et la fragmentation des responsabilités en matière de réponse aux incidents complexifient encore la situation.

Face à ces défis, la création d'un SOC centralisé s'impose comme un pilier essentiel de la cybersécurité des C-ITS. En assurant une surveillance continue, la détection des menaces et une réponse coordonnée sur l'ensemble des actifs critiques, le SOC permet une collaboration efficace entre tous les acteurs concernés.

Fonctions et structure du SOC

Les fonctions principales du SOC sont étroitement alignées sur celles du NIST Cybersecurity Framework :

- Gouverner : établir le cadre nécessaire pour que toutes les autres fonctions opèrent de manière cohérente, fournir une direction stratégique, des politiques et des structures de gouvernance, gérer les risques et superviser les contrôles de sécurité;
- Identifier : maintenir une compréhension à jour des actifs, ressources et risques associés aux C-ITS, fournissant la base de la gestion des risques;
- Détecter : surveiller en continu les systèmes et réseaux pour identifier les événements de cybersécurité;
- Répondre : coordonner les actions pour contenir et atténuer les incidents détectés, en minimisant leur impact;
- Protéger et restaurer (fonctions de soutien) : mettre en œuvre des mesures de protection pour garantir la continuité des services essentiels et soutenir la résilience et la restauration après incident.

Ces fonctions sont rendues possibles par trois piliers fondamentaux (*Fig. 6*) :

- Processus : procédures définies pour la surveillance, la détection, la réponse aux incidents et l'escalade, adaptées aux environnements C-ITS ;
- Technologies : outils pour l'inventaire des actifs, la détection des menaces, la corrélation d'événements, l'automatisation des réponses, couvrant les domaines IT et OT ;
- Ressources humaines : personnel qualifié garantissant l'efficacité du SOC.

L'intégration de ces trois piliers avec l'approche NIST permet d'assurer une démarche structurée et conforme aux meilleures pratiques internationales.

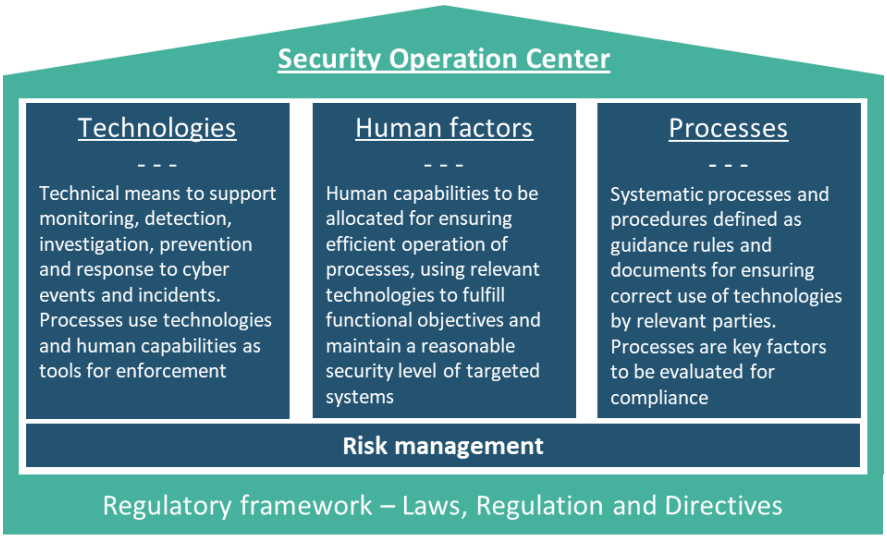


Fig. 6 *Trois piliers du SOC.*

Modèle suisse de SOC pour les C-ITS

La réflexion sur la mise en place d'un SOC pour les C-ITS en Suisse a porté sur l'identification de la structure organisationnelle et du mode de déploiement les plus adaptés.

Trois modèles organisationnels ont été analysés :

- SOC interne : gestion intégrale en interne, offrant un contrôle maximal et la souveraineté sur les données, mais nécessitant d'importants investissements en personnel et en infrastructures ;
- SOC externalisé (MSSP) : externalisation complète auprès d'un prestataire spécialisé, permettant de bénéficier d'une expertise avancée et de réduire les coûts, mais soulevant des enjeux de confidentialité, de conformité et de perte de contrôle direct ;
- SOC hybride : conservation en interne des fonctions sensibles (gestion des incidents critiques, prise de décision), avec externalisation des tâches moins sensibles (surveillance, analyse de logs), offrant ainsi un équilibre entre contrôle, flexibilité et expertise.

Une matrice multicritère a permis de comparer ces modèles sur des critères tels que le coût, la gouvernance, l'expertise, la personnalisation, l'évolutivité, la rapidité de mise en œuvre, la complexité opérationnelle et la flexibilité à long terme. Le modèle hybride s'est révélé le plus équilibré, combinant souveraineté des données, conformité réglementaire, maîtrise des coûts et accès à des compétences spécialisées.

Trois approches de déploiement ont été envisagées :

- Déploiement géographique : par phases selon les zones géographiques, en commençant par les plus sensibles ;
- Déploiement technologique : intégration progressive par type de technologie ou de capteur ;
- Déploiement par capacité : développement progressif des fonctionnalités du SOC, de la collecte de données à la gestion complète des incidents.

La stratégie retenue combine les approches technologique (*Fig. 8*) et géographique (Fig. 7), tout en veillant à ce que les capacités essentielles (*Fig. 9*) (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.

Fig. 7 *Exemple de déploiement géographique.*

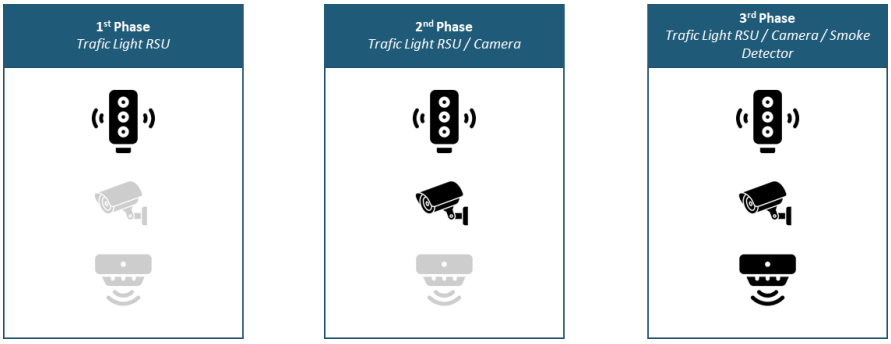


Fig. 8 *Exemple de déploiement technologique.*

Fig. 9 *Exemple de déploiement de capacités.*

Feuille de route pour la mise en œuvre du SOC

La feuille de route proposée comprend cinq phases (*Fig. 10*), inspirées des recommandations de l'ENISA et des meilleures pratiques internationales [43]. Elle va de la planification initiale à l'amélioration continue, avec une capacité opérationnelle de base attendue sous 18 mois.

- Phase de fondation : définition de la mission, des objectifs, des parties prenantes, évaluation des besoins, obtention des ressources et financement, établissement des politiques et structures de gouvernance.
- Phase de construction : mise en place de l'infrastructure, acquisition des outils, documentation des processus, déploiement de la première technologie C-ITS, lancement de l'inventaire des actifs.
- Capacité opérationnelle initiale : mise en service du SOC avec les fonctions essentielles pour la technologie et la zone pilote, mise en place des mécanismes de déclaration obligatoire.
- Extension et optimisation : élargissement à d'autres technologies et zones, optimisation des processus, renforcement de la collaboration et du partage d'informations.

- Exploitation et amélioration continue : maintien et amélioration du SOC par des révisions régulières, adaptation aux nouvelles menaces et exigences, formation continue et mises à niveau technologiques.

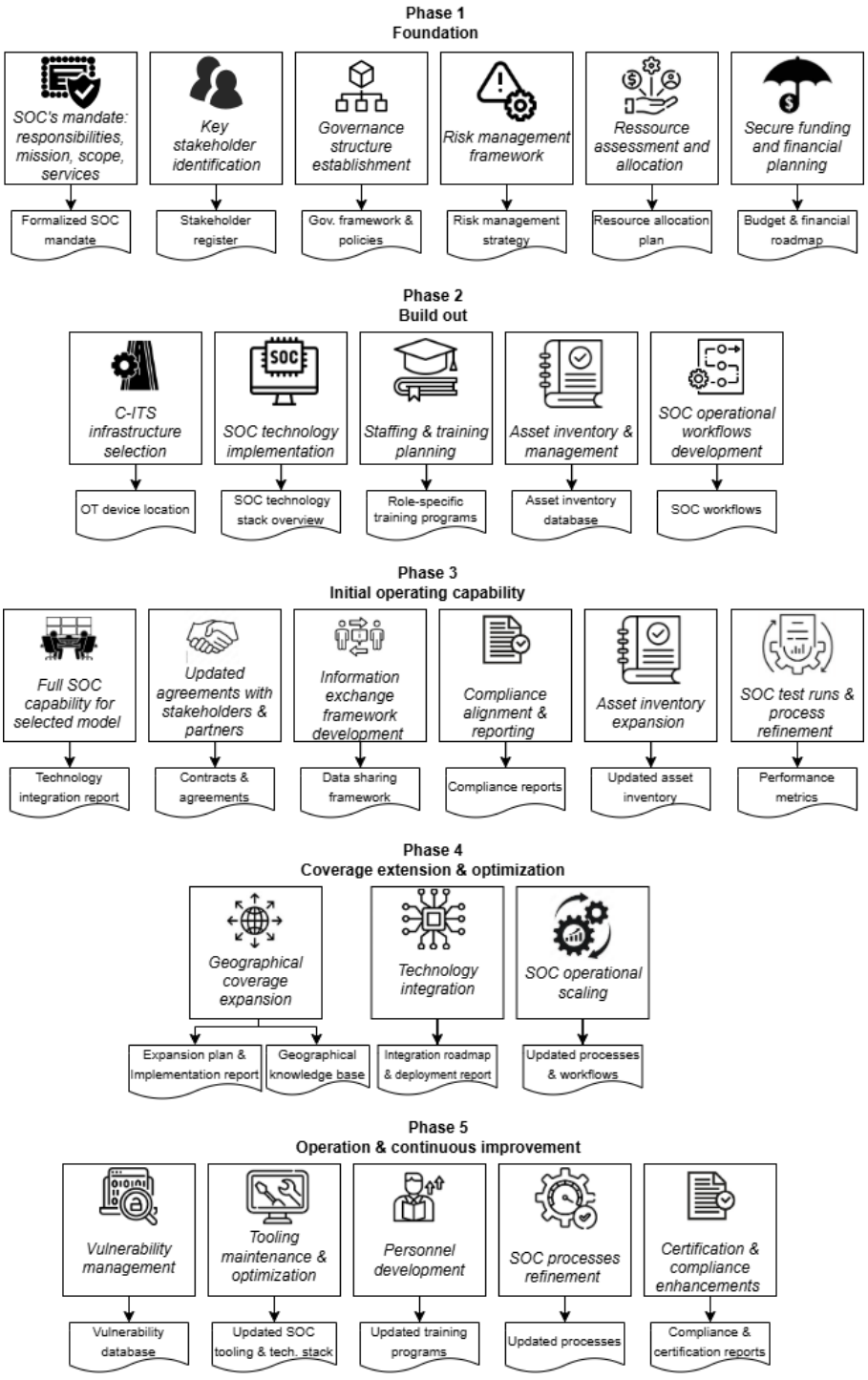


Fig. 10 *Résumé des phases.*

Délais de mise en œuvre et estimation des coûts

Le déploiement national (phases 1 à 4) devrait être achevé en 36 mois, l'exploitation continue (phase 5) se poursuivant ensuite. Le coût total de mise en œuvre est estimé à 6,2 millions de CHF pour les 36 premiers mois, suivi de coûts opérationnels récurrents d'environ 188 000 CHF par mois pour l'amélioration continue et la maintenance.

Principaux défis

L'élaboration et la mise en œuvre prévue de la feuille de route SOC pour les C-ITS suisses ont révélé plusieurs défis stratégiques et opérationnels. Le choix du modèle organisationnel optimal (interne, MSSP ou hybride) et de l'approche de déploiement (géographique, technologique ou par capacité) a nécessité une analyse approfondie des compromis entre contrôle, flexibilité, faisabilité, allocation des ressources et conformité. Bien que la feuille de route prévoie une mise en œuvre par étapes, il est probable que l'exécution réelle nécessite des activités qui se chevauchent et une adaptation continue aux contraintes du terrain.

L'intégration technologique s'annonce complexe, compte tenu du mélange de systèmes IT et OT, y compris des systèmes hérités non conçus pour la cybersécurité. Construire un inventaire complet des actifs est à la fois essentiel et difficile, nécessitant la coordination de nombreux acteurs et propriétaires de systèmes. Sans cet inventaire, une analyse correcte des risques n'est pas possible.

La priorisation du déploiement, tant géographique que technologique, exigera une planification minutieuse, en équilibrant faisabilité et approche basée sur les risques, en se concentrant d'abord sur les zones les plus vulnérables et à fort impact. Les défis opérationnels tels que la budgétisation, la gestion des délais et le maintien de l'engagement des parties prenantes nécessiteront une attention constante. Un leadership fort, le soutien de la direction et une expertise spécialisée, surtout dans les phases initiales, seront cruciaux pour garantir le succès de la mise en œuvre et la résilience à long terme.

Conclusion

Un SOC national est indispensable pour sécuriser l'infrastructure C-ITS de la Suisse, classée comme infrastructure critique et soumise à la réglementation en cybersécurité. Un modèle SOC décentralisé ou territorial a été jugé irréaliste en raison de sa complexité opérationnelle. À la place, un SOC centralisé avec une gouvernance hybride combinant MSSP et opérations internes a été identifié comme la meilleure option.

La feuille de route prévoit une mise en œuvre progressive, débutant par les aspects organisationnels et de gouvernance, puis le développement de toutes les capacités à petite échelle, avant une extension géographique et technologique. Cette approche assure une préparation rapide et pose des bases solides pour une expansion future.

Zusammenfassung

Einleitung und Projektziele

Kooperative intelligente Verkehrssysteme (C-ITS) und Fahrzeug-zu-Allem (V2X)-Kommunikation verändern die Mobilität, indem sie Fahrzeugen, Infrastrukturen und Verkehrsteilnehmenden ermöglichen, Informationen auszutauschen und so den Verkehr sicherer und effizienter zu gestalten. Mit zunehmender Verbreitung und Sichtbarkeit werden diese Systeme jedoch auch immer attraktivere Ziele für Angriffe, insbesondere Cyberangriffe. Da C-ITS Teil der kritischen nationalen Infrastruktur sind, ist ihre Cybersicherheit von zentraler Bedeutung und erfordert sowohl ein proaktives als auch ein reaktives Risikomanagement. Ein früherer Mobility 4.0 (MB4) Call MB4_20_02C_01 [41] konzentrierte sich auf proaktive Maßnahmen wie die frühzeitige Bedrohungsanalyse und deren Risikobewertung. Dieser Bericht legt den Fokus auf reaktive Maßnahmen, insbesondere auf die Einrichtung eines nationalen Security Operations Center (SOC) für C-ITS.

Die Ziele des Projekts sind die Bewertung der Notwendigkeit eines nationalen, auf den C-ITS-Kontext zugeschnittenen SOC, die Untersuchung tragfähiger Modelle für dessen Aufbau und Betrieb, sowie die Entwicklung einer praktischen Roadmap für die Umsetzung im Schweizer Kontext.

Überblick über C-ITS

C-ITS stellen eine Weiterentwicklung traditioneller ITS dar, indem sie den Echtzeit-Informationsaustausch zwischen Fahrzeugen, Infrastrukturen und Verkehrsteilnehmenden ermöglichen, um die Sicherheit und Effizienz zu erhöhen. Im Gegensatz zu konventionellen IST, basiert C-ITS auf umfangreicher, interaktiver Kommunikation (Vehicle-to-Vehicle, V2V, und Vehicle-to-Infrastructure, V2I), wodurch Cybersicherheit aufgrund der erweiterten Angriffsfläche zu einem entscheidenden Thema wird.

Das C-ITS-Ökosystem ist komplex und umfasst zahlreiche Akteure: Regierungsbehörden, Verkehrsbehörden, Technologieanbieter, Telekommunikationsunternehmen, Partnerschaften zwischen öffentlichem und privatem Sektor, Automobilhersteller, Forschungseinrichtungen und Endnutzer.

Regulatorischer Rahmen und Schlüsselbehörden

Das C-ITS-Umfeld basiert auf einer Kombination aus internationalen Standards, europäischen Rahmenwerken (DSGVO [1], NIS2 [11], CRA [2], revidierte ITS-Richtlinie [12]) und Schweizer Landesrecht. Die revidierte ITS-Richtlinie führt Anforderungen für sichere Kommunikation mit einem PKI-basierten Vertrauensmodell ein, das sich an der European Certificate Trust List (ECTL) orientiert [19]. Zudem werden interoperable und maschinenlesbare Verkehrsdatenformate, einen National Access Point (NAP) für den Datenaustausch [18], DSGVO-konforme Datenschutzmaßnahmen und grenzüberschreitende Notfallpläne erwartet. Diese Vorschriften und Richtlinien müssen bei der Entwicklung des SOC sorgfältig berücksichtigt werden, um die Einhaltung sicherzustellen.

Der Schweizer Rechtsrahmen umfasst den ICT-Mindeststandard für kritische Sektoren, der am NIST Cybersecurity Framework ausgerichtet ist [23]. Er beinhaltet außerdem das nDSG (neues Datenschutzgesetz) [4], das mit der DSGVO konform ist, sowie die FAISC [5], die verbindliche Cybersicherheitsanforderungen für kritische Infrastrukturen einschließlich C-ITS festlegt. Ab dem 1. April 2025 hat der Schweizer Bundesrat zudem eine Meldepflicht für Cyberangriffe auf kritische Infrastrukturen eingeführt. Meldungen müssen innerhalb von 24 Stunden beim Nationalen Zentrum für Cybersicherheit (NCSC), oder neu Bundesamt für Cybersicherheit (BACS) eingehen [42].

Dieses bundesweite Kompetenzzentrum für Cybersicherheit (NCSC) stellt die erste Anlaufstelle für Unternehmen, öffentliche Dienste und Betreiber kritischer Infrastrukturen bei Cybervorfällen dar. Eine weitere bedeutende Behörde ist das Bundesamt für Straßen (ASTRA), das auf nationaler Ebene für Straßeninfrastruktur verantwortlich ist. ASTRA spielt eine zentrale Rolle bei der C-ITS-Politik, dem Rollout und der Entwicklung von Referenzdokumenten zum C-ITS-Management, zum nationalen Kommunikationsnetz für C-ITS und zur OT-Sicherheit.

Notwendigkeit eines SOC

Das C-ITS-Umfeld umfasst eine Vielzahl miteinander verbundener Anlagen, darunter Straßeninfrastruktur, zentrale Managementsysteme und Kommunikationsnetze. Letztere sind typischerweise in IT- und OT-Komponenten unterteilt, die jeweils spezifische Anforderungen an die Cybersicherheit stellen. Die zunehmende Vernetzung vergrößert die Angriffsfläche und das Risiko von Vorfällen, die zu erheblichen Störungen führen können. Die Komplexität wird durch unterschiedliche Eigentumsverhältnisse, Altsysteme und fragmentierte Zuständigkeiten weiter erhöht.

Um diese Herausforderungen zu bewältigen, wird die Einrichtung eines zentralisierten SOC als Grundpfeiler der C-ITS-Cybersicherheit vorgeschlagen. Durch kontinuierliche Überwachung, Bedrohungserkennung und koordinierte Reaktion auf allen kritischen C-ITS-Anlagen bildet das SOC die Struktur, die eine effiziente Zusammenarbeit der verschiedenen Akteure ermöglicht.

Funktionen und Struktur des SOC

Die Hauptfunktionen des SOC orientieren sich eng an den Kernfunktionen des NIST Cybersecurity Framework:

- Governance: Aufbau des erforderlichen Rahmens für die einheitliche Arbeitsweise aller anderen Funktionen, strategische Ausrichtung, Richtlinien und Führungsstrukturen bereitstellen, Risiken steuern und Sicherheitskontrollen beaufsichtigen;
- Identifikation: Aufrechterhaltung eines aktuellen Verständnisses der C-ITS-Anlagen, Ressourcen und damit verbundenen Risiken als Grundlage für das Risikomanagement;
- Erkennung: Kontinuierliche Überwachung von Systemen und Netzwerken zur Identifikation von Cybersecurity-Ereignissen;
- Reaktion: Koordination von Maßnahmen zur Eindämmung und Minderung erkannter Vorfälle, um Auswirkungen zu minimieren;
- Schutz und Wiederherstellung (unterstützende Funktionen): Umsetzung von Schutzmaßnahmen zur Sicherstellung essenzieller Dienste sowie Unterstützung von Resilienz und Wiederherstellung nach Vorfällen.

Diese Kernfunktionen werden durch drei zentrale Säulen ermöglicht (*Fig. 11*):

- Prozesse: Definierte Verfahren für Überwachung, Erkennung, Incident Response und Eskalation, zugeschnitten auf C-ITS-Umgebungen;
- Technologien: Tools zur Anlagen-Erkennung, Bedrohungsdetektion, Ereigniskorrelation, Automatisierung der Reaktion etc., sowohl im IT- als auch im OT-Bereich;
- Personal: Qualifizierte Fachkräfte, die eine effektive SOC-Performance gewährleisten können.

Durch die Integration dieser drei Säulen mit dem NIST Cybersecurity Framework stellt das vorgeschlagene SOC einen umfassenden und strukturierten Ansatz sicher, der internationalen Best Practices entspricht.

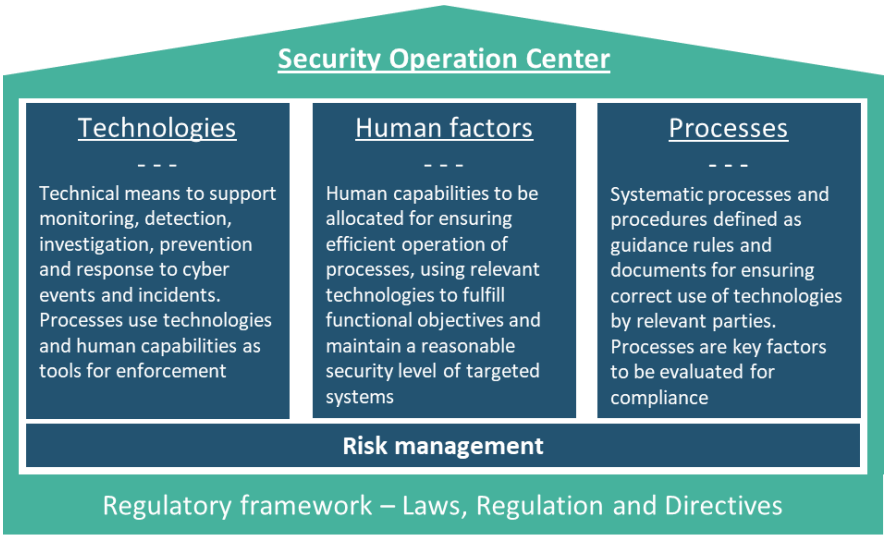


Fig. 11 *SOC 3 Säulen.*

Schweizer SOC für C-IST

Bei der Planung eines SOC für C-IST in der Schweiz lag der Schwerpunkt auf der Identifikation der optimalen Organisationsstruktur und des besten Einführungsansatzes.

Drei Hauptmodelle wurden betrachtet:

- Internes SOC: Alle Überwachungs-, Erkennungs- und Reaktionsaufgaben werden intern durchgeführt, was maximale Kontrolle und Datensouveränität bietet, jedoch erhebliche Investitionen in Personal, Infrastruktur und Betriebskosten erfordert;
- Outgesourctes SOC (MSSP): Alle SOC-Funktionen werden an einen Managed Security Service Provider ausgelagert, wodurch externe Expertise genutzt und Kosten gesenkt werden, jedoch Herausforderungen hinsichtlich Datenschutz, Compliance und Kontrollverlust entstehen;
- Hybrides SOC: Kritische SOC-Funktionen wie das Management sensibler Vorfälle und Entscheidungsfindung verbleiben intern, während weniger sensible Aufgaben (z. B. globale Bedrohungsüberwachung, Log-Analyse) an externe Dienstleister ausgelagert werden. Dies kombiniert interne Kontrolle und Fachwissen mit der Skalierbarkeit und den Ressourcen von MSSPs.

Eine Multikriterien-Matrix wurde entwickelt, um interne, MSSP- und hybride SOC-Modelle objektiv zu vergleichen. Bewertet wurden Kosten, Governance und Compliance, Expertise, Anpassungsfähigkeit, Skalierbarkeit, Implementierungsgeschwindigkeit, Technologie-akzeptanz, operative Komplexität und langfristige Flexibilität. Das hybride SOC-Modell erzielte die höchste Gesamtbewertung. Es bietet die beste Balance zwischen Kontrolle und Flexibilität, indem sensible Operationen unter direkter Aufsicht bleiben und ausgewählte Funktionen für skalierbare Unterstützung und Spezialwissen ausgelagert werden. Dieses Modell sichert zudem die Datensouveränität und erleichtert die Einhaltung von Vorschriften bei gleichzeitiger Optimierung der Kosten und Minimierung des Aufwands für Infrastruktur und Personal.

Drei Hauptmethoden für die Einführung wurden betrachtet:

- Geografische Einführung: Phasenweise Einführung nach Standorten, beginnend mit Hochrisiko- oder Prioritätsbereichen;
- Technologische Einführung: Einführung nach spezifischen Technologien oder Sensortypen, wobei jede Technologie schrittweise integriert und gesichert wird;
- Einführung nach Fähigkeiten: Stufenweise Entwicklung der funktionalen Reife des SOC, beginnend mit Datensammlung, über Anomalie-Erkennung und Bedrohungsanalyse bis hin zur vollständigen Incident Response und Schadensbegrenzung.

Die gewählte Strategie kombiniert technologische (*Fig. 13*) und geografische (Fig. 12) Ansätze und stellt sicher, dass alle Kernfähigkeiten (*Fig. 14*) (Identifikation, Erkennung, Reaktion) von Anfang an verfügbar sind. Die erste Umsetzung konzentriert sich auf die Absicherung einer einzelnen Technologie (z. B. Ampel-RSUs) in einem ausgewählten urbanen Gebiet. Mit zunehmender Reife des SOC wird die Integration weiterer Technologien und geografischer Bereiche erfolgen (lokal, kantonal, national). Die Abdeckung aller Fähigkeitsphasen von Beginn an ermöglicht die schnelle Etablierung eines Minimum Viable SOC und liefert sofortigen Mehrwert. Die Skalierbarkeit erfolgt sowohl hinsichtlich der Technologieintegration als auch der geografischen Ausweitung.

Fig. 12 *Geographic deployment example.*

Fig. 13 *Technological deployment example.*

Fig. 14 *Capability deployment example.*

Roadmap für die SOC-Implementierung

Die vorgeschlagene Roadmap für die SOC-Implementierung bei C-ITS umfasst fünf Phasen (*Fig. 15*), inspiriert vom ENISA-Bericht und der Literatur zu globalen SOC-Strategien [43]. Die Roadmap reicht von der Grundlagenplanung bis zur kontinuierlichen Verbesserung, wobei die erste Betriebsfähigkeit nach 18 Monaten erwartet wird.

- Grundlagenphase: Definition der Mission, Ziele und Stakeholder des SOC, umfassende Bedarfsanalyse, Sicherstellung von Ressourcen und Finanzierung, Festlegung der Anforderungen, Richtlinien und Governance-Strukturen.
- Aufbauphase: Aufbau der physischen und technischen Infrastruktur, Beschaffung der Werkzeuge, Definition und Dokumentation der Betriebsprozesse, Einführung der ersten C-ITS-Technologie, Start des Asset-Inventars.
- Phase der ersten Betriebsfähigkeit: SOC wird erstmals mit allen Kernfunktionen (Identifikation, Erkennung, Reaktion) für die ausgewählte Technologie in einem urbanen Pilotgebiet in Betrieb genommen. Meldepflichten sind implementiert.
- Erweiterungs- und Optimierungsphase: Erweiterung auf weitere Technologien und geografische Gebiete, Optimierung der Prozesse, Verbesserung der Zusammenarbeit und des Informationsaustauschs.
- Betrieb und kontinuierliche Verbesserung: Regelmäßige Überprüfung und Anpassung des SOC an neue Bedrohungen und regulatorische Anforderungen, kontinuierliche Weiterbildung und technologische Weiterentwicklung.

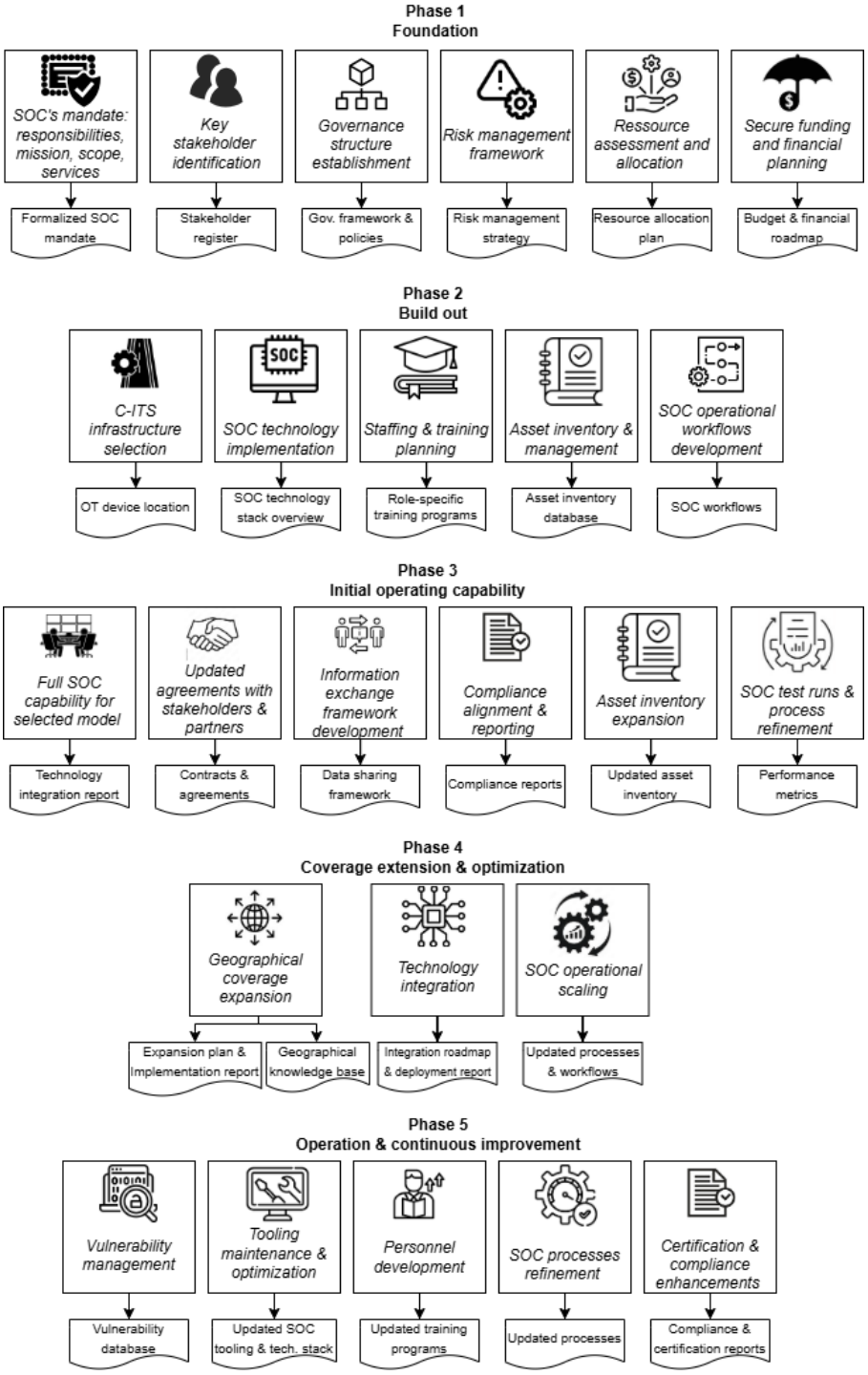


Fig. 15 *Zusammenfassung der Phasen.*

Zeitplan und Kostenschätzung

Der nationale Rollout (Phasen 1 bis 4) soll innerhalb von 36 Monaten abgeschlossen sein, der Betrieb läuft anschließend weiter. Die Gesamtkosten für die ersten 36 Monate werden auf 6,2 Millionen CHF geschätzt, gefolgt von laufenden Betriebskosten von ca. kCHF 188 pro Monat für Wartung und kontinuierliche Verbesserung.

Zentrale Herausforderungen

Die Entwicklung und geplante Umsetzung der SOC-Roadmap für C-ITS in der Schweiz hat verschiedene strategische und operative Herausforderungen aufgezeigt. Die Wahl des optimalen Organisationsmodells (intern, MSSP oder hybrid) und der Einführungsstrategie (geografisch, technologisch oder fähigkeitsbasiert) erforderte eine sorgfältige Abwägung von Kontrolle, Flexibilität, Machbarkeit, Ressourceneinsatz und Compliance. Während die Roadmap eine schrittweise Einführung vorsieht, wird erwartet, dass in der Praxis Aktivitäten überlappen und eine kontinuierliche Anpassung an die Realitäten erforderlich ist.

Die technologische Integration ist komplex, insbesondere aufgrund der Mischung aus IT- und OT-Systemen, einschließlich Altsystemen ohne Cybersicherheitsdesign. Der Aufbau eines vollständigen Asset-Inventars ist essenziell und herausfordernd, da er die Koordination vieler Akteure und Systemverantwortlicher erfordert. Ohne dieses Inventar ist eine korrekte Risikoanalyse nicht möglich.

Die Priorisierung des Rollouts – sowohl geografisch als auch technologisch – erfordert sorgfältige Planung, um Machbarkeit und Risikoorientierung auszubalancieren und sich zunächst auf die verwundbarsten und wirkungsvollsten Bereiche zu konzentrieren. Operative Herausforderungen wie Budgetierung, Zeitmanagement und die Einbindung der Stakeholder erfordern während des gesamten Projekts kontinuierliche Aufmerksamkeit. Starke Führung, Unterstützung durch das Top-Management und spezielles Fachwissen, insbesondere in den Anfangsphasen, sind entscheidend für den Erfolg und die langfristige Resilienz.

Fazit

Ein nationales SOC ist unerlässlich um die C-ITS-Infrastruktur der Schweiz zu schützen, die als kritische Infrastruktur gilt und regulatorischen Anforderungen unterliegt. Ein dezentrales oder territoriales SOC-Modell wurde aufgrund der operativen Komplexität als nicht praktikabel eingestuft. Stattdessen wurde ein zentrales SOC mit hybrider Governance (Kombination aus MSSP und internen Operationen) als beste Option identifiziert.

Die Roadmap sieht eine schrittweise Umsetzung vor, beginnend mit organisatorischen und Governance-Aspekten, gefolgt von der Entwicklung aller Kernfähigkeiten im kleinen Massstab und einer anschließenden geografischen und technologischen Erweiterung. Dieser Ansatz gewährleistet eine schnelle Einsatzbereitschaft und schafft eine solide Grundlage für die zukünftige Weiterentwicklung.

1 Introduction and project scoping

The mobility ecosystem of today and tomorrow is defined by vehicles which do not only communicate with each other, but also with road infrastructure units and other road users. Cooperative Intelligent Transport Systems (C-ITS) and V2X communications already represent the assumed future of intelligent vehicle networking. The key to these systems is trustworthy and secure technology.

Though intended to enhance and strengthen mobility systems, C-ITS can also be seen as attractive targets for threat agents. In that context, two risk management approaches should be combined and followed by mobility stakeholders.

- **Proactive measures**: This approach addresses proactive methods to be applied in early deployment stages. Conceptual cyber threat analysis and risk assessment are used to identify critical zones and assets in given environments. The same project consortium (CertX and HEIA-FR/ROSAS) has proposed a pragmatic methodology for cyber threat analysis and risk assessment for C-ITS in the scope of a separate MB4 call identified as MB4_20_02C_01 [41].
- **Reactive measures**: Cybersecurity is a strongly dynamic field where new threats, vulnerabilities and attack tools are discovered and exploited every day. This aspect forces organizations to couple proactive activities with continual reactive methods for investigating, detecting and responding to new information and events, in order to maintain a reasonable and commonly accepted level of security for the entire length of operations.

The goal of this combined approach is to not only keep an up-to-date picture of cyber threats, current protection measures and risk levels, but also to provide capabilities to react to potential events and incidents which might have been omitted or unknown during preliminary early-stage analysis. *Fig. 16* below briefly illustrates such methods and simple interactions between them.

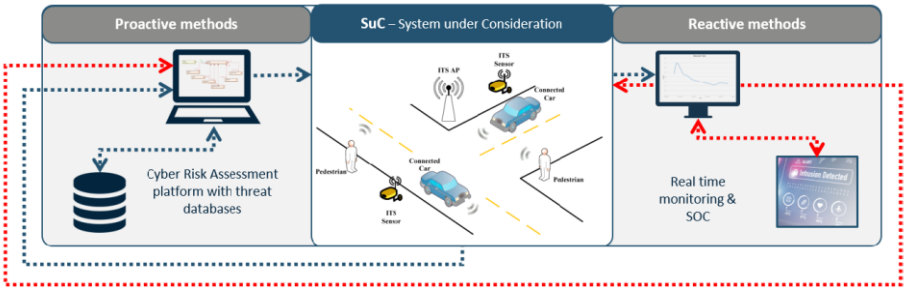


***Fig. 16** Proactive vs Reactive measures.*

This specific research project will focus on reactive measures, including the technologies, processes and human factors required to equip a C-ITS in the Swiss context with these capabilities. The following subsections will introduce three foundational questions to be answered in support of that research and with the aim of outlining a roadmap for Swiss authorities:

- **Why** are such reactive measures required today in the mobility sector and in the context of C-ITS?
- **What** are the specificities and usual behavior of Cooperative Intelligent Transport Systems (C-ITS)?
- **How** can governmental entities ensure that C-ITS are adequately provisioned with adequate investigation, detection and response capabilities?

1.1 Reactive measures as a prerequisite for a secure mobility sector

The current regulatory landscape is evolving. Notably, it now integrates cybersecurity requirements for critical and/or essential services, including services in the mobility and transport sectors. In addition to these normative trends, the proliferation of connected and even automated vehicles and infrastructure devices is increasing the risk of cyber-attacks both in terms of number and of severity. In the context of cybersecurity, this trend is referred to as a multiplication of attack vectors (means / path towards system breach) leading to a growing attack surface (result of the sum of attack vectors).

In the near future, connected and automated cars will rely on data and communications coming from mobility stakeholders to take decisions and adjust their behaviors. A vulnerability anywhere along the mobility chain might result in an insecure and unsafe transport network.

1.2 C-ITS as a set of critical assets to be protected

Cooperative Intelligence Transport Systems (C-ITS) are defined as a set of interconnected elements disseminated over a transport network for supporting a safe, secure and efficient mobility sector. As with any other computerized system, C-ITS have inherent cyber risks that must be addressed pragmatically to minimize the risk of critical consequences.

C-ITS are composed of multiple and heterogenous subsystems such as traffic lights and centralized traffic management services. These subsystems cooperate to provide high-level function, e.g., global traffic flow management over a city, congestion avoidance, etc. While cyber-attacks may target different parts of a common functional chain, different expectations and requirements must be connected to relevant subsystems. As an example, an incident detected in a traffic light system may be the consequence of the breach of the traffic light system itself, of its communications with surrounding systems, or even of the centralized system managing it.

Whereas cyber risks are applicable to the whole C-ITS scope, its elements can be bound to different actors and their respective responsibilities. Indeed, elements considered as onboarded on cars fall under the scope of vehicle manufacturer responsibility and are therefore already covered by Type Approval related rules. However, the elements deployed along roads and centralized at the regional or national level are currently free of cyber security considerations and shall be subject to additional effort to be continuously monitored, evaluated and maintained. In the case of cybersecurity events, adequate responses shall be triggered and managed for keeping the transport system reasonably secure.

1.3 SOC as a solution for monitoring and handling C-ITS incidents

Security Operation Centers (SOC) are centralized units on top of infrastructure and/or interconnected systems aiming to continuously monitor and respond to cyber security events. In the context of this research project, the focus of such a center would be to handle cyber risks. An SOC can also have other functions that can be added to its primary “cyber”-specific role in order to streamline incident management.

This research report introduces the primitives for a Security Operation Center for critical infrastructure tailored to C-ITS specificities (incl. regulatory context, technologies, processes and procedures). Doing so will facilitate the development of a pragmatic roadmap for establishing such capabilities and environment in Switzerland at the national and/or cantonal level.

1.4 Research methodology and documentation

This report is structured so that contextual information about C-ITS is documented first as a knowledge baseline. Considerations about reactive measures are then added, starting with generic SOC considerations first followed by a discussion of measures specifically tailored to mobility systems. The last parts of this report define the set of activities needed to attain SOC capabilities, in the form of a roadmap proposal. *Tab. 1* offers a summary of the report.

***Tab. 1** Research report overview*

Report sections	Summary
Section 1.x (present)	**Introduction and project scoping** – Context about SOC within mobility sectors, introducing project objectives *Keywords: SOC, C-ITS, reactive/proactive measures*
Section 2.x	**C-ITS context establishment** – Definition of Cooperative Intelligent Transport Systems (C-ITS), introducing standard network topologies, components and applications. This section also presents the growing convergence of Information Technologies (IT) and Operational Technologies (OT), based on major challenges raised by such trends. This part ends with the identification of the risks and opportunities to be addressed by reactive measures, and potential implementations of Security Operation Center capabilities. *Keywords: C-ITS, IT/OT, OBU, RSU, TMC/TMS, V2X, regulations, standards*
Section 3.x	**Cyber risks in a C-ITS environment** – Overview of cyber risks surrounding C-ITS, introducing a standardized framework for considering potential kill chains and anticipating adversarial attempts using established nomenclature and categories *Keywords: Cyber risk, MITRE AT&CK framework* [44]*, killchain* [45]
Section 4.x	**SOC context establishment** – Definition of Security Operation Centers, introducing processes, human factors and technological primitives for monitoring and maintaining secure Systems under Consideration (SuC). This section also presents rules and regulations applicable to SOC implementations on critical infrastructure. This part ends with examples of existing SOC implementations dedicated to heterogenous environments which might share some common elements with C-ITS. *Keywords: SOC capabilities, SIEM, SOAR, vulnerability, assets management, roles & responsibilities, organizational models, regulations, guidance*
Section 5.x	**SOC for C-ITS – Deployment strategy** – Based on the contextual knowledge of C-ITS documented in section 2.x and SOC capabilities / primitives documented in section 4.x, this part analyzes specific properties and prerequisites for the establishment of a SOC dedicated to C-ITS environments. This section aims to secure the key capabilities to be ultimately provided by a SOC for C-ITS. *Keywords: Authorities, prerequisites, limitations, challenges, trends*
Section 6.x	**SOC for C-ITS – Roadmap phases** – Definition of comprehensive phases for defining pragmatic steps towards SOC for C-ITS implementations, including effort, costs and objectives per set of activities (chunks) and phases. *Keywords: Chunks, tasks, priorities, prerequisites, efforts, costs, stakeholders*
Section 7.x	**SOC for C-ITS – Roadmap challenges & perspective** – This chapter outlines implementation considerations, key challenges encountered during the development of the SOC roadmap, and challenges expected during practical implementation. The chapter also describes research opportunities to support and guide the future development of the SOC. *Keywords: Timeline, project management, phases, sequencing, milestones, budget, recommendations*
Section 8.x	**SOC for C-ITS – Conclusions** – In this closing chapter, some perspective and conclusions on the proposed roadmap and strategy are offered. *Keywords: National SOC, summary of costs & times, SOC models*
Appendix	The following resources are provided as external documentation: • Demonstrator • Detailed budget • Multicriteria matrix

2 Cooperative Intelligent Transport System overview

2.1 From ITS towards Cooperative ITS (C-ITS)

Intelligent Transport Systems (ITS) aim to implement environmentally friendly, safe, and secure transportation processes utilizing advanced technologies in data detection, transmission and storage, communication, and control. Consequently, ITS are deployed to enhance safety, sustainability, efficiency, and comfort.

Cooperative Intelligent Transport Systems (C-ITS) refer to a collection of ITS technologies capable of delivering services facilitated by continuous, real-time information exchange among system components. As an example, C-ITS can provide drivers with real-time accident-related information, including traffic conditions, unforeseen events, and weather conditions.

Structurally, the components of ITS collaborate effectively to bolster transportation processes using digital technologies. These components can be strategically positioned roadside, within vehicles, at transportation hubs, or in the cloud. In summary, C-ITS encompass the collaborative elements of transportation processes, including users, vehicles, infrastructure, and operators.

The distinction between ITS and C-ITS lies in the level of interaction among system components such as users, vehicles, infrastructure, environment, and operators. In C-ITS, this interaction takes precedence, whereas in ITS, intelligence can be implemented within specific system modules without extensive interaction. As the amount of exchanged information increases, C-ITS functions become increasingly efficient. In that context, considering C-ITS as a combination of rules, procedures, systems, and subsystems facilitating cooperative service delivery, is crucial.

In a C-ITS environment, actors can communicate with each other to send, receive, and exchange information. Individual vehicles can communicate with other vehicles (V2V) or roadside stations/infrastructure (V2I), enhancing traffic flow safety, comfort, as well as for reducing vehicle emissions.

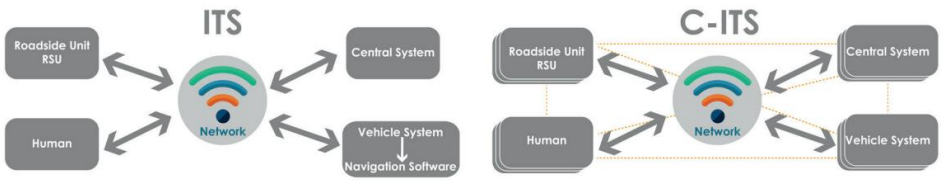


***Fig. 17** ITS vs C-ITS Systems **[46]**.*

As defined in *Fig. 17*, C-ITS are usually considered as a combination of elements interacting with each other, aiming to provide a high-level function which might either be fully data-oriented (e.g., traffic information sharing) or more physically active (e.g., barrier closure or modification of the behavior of traffic lights to reroute traffic).

From a cyber security and risk perspective, these two function types imply different considerations and strategies to maximize safe, secure and resilient operations. Thus, industries usually define two categories for functions dealing with information or physical processes respectively:

- **Information Technologies (IT);**
- **Operational Technologies (OT).**

This chapter uses this typology as a foundation to segregate C-ITS assets, or elements, and ultimately to define tailored processes to secure their operations.

Before detailing C-ITS systems and elements, the stakeholders and regulatory context involved in these innovative mobility ecosystems have to be clarified and established. This foundational step ensures that the expectations and requirements arising from current regulations, as well as emerging international trends, are thoroughly understood and integrated into the analysis.

2.2 ITS & C-ITS Stakeholder

A critical aspect of the successful implementation and operation of ITS and C-ITS is the involvement of various stakeholders. This chapter explores the key stakeholders in the ITS and C-ITS ecosystem, their roles, and their contributions to the development and deployment of these systems. Each stakeholder's role, contribution, and potential involvement in a SOC will be derived.

Government agencies

- **Role**: Government agencies at the local, regional, and national levels are pivotal in the planning, funding, and regulation of ITS and C-ITS projects. They establish policies, standards, and regulations that guide the development and deployment of these systems;
- **Contribution**: They provide the necessary infrastructure, funding, and legislative support to ensure the successful implementation of ITS and C-ITS initiatives;
- **Involvement**: Government agencies will be responsible for the SOC's behavior, based on potential legal requirements.

Transportation authorities

- **Role**: These entities are responsible for the management and operation of transportation networks, including roads, highways, and public transit systems;
- **Contribution**: They implement ITS and C-ITS solutions to improve traffic flow, enhance safety, and provide real-time information to travelers;
- **Involvement**: FEDRO could be the SOC operator for all national roads and accountable for non-national roads.

Automotive manufacturers

- **Role**: Automotive manufacturers play a crucial role in integrating ITS and C-ITS technologies into vehicles. They develop and deploy connected vehicle technologies that enable communication between vehicles and infrastructure;
- **Contribution**: They innovate and produce vehicles equipped with advanced sensors, communication systems, and automated driving capabilities, which are essential for the functioning of C-ITS;
- **Involvement**: Original Equipment Manufacturers (OEMs) are not within the project scope as they will adhere to specific regulations and will not transmit any information to public infrastructure.

Technology providers

- **Role**: These stakeholders include companies that develop hardware and software solutions for ITS and C-ITS. They provide the technological backbone that supports data collection, processing, and communication;
- **Contribution**: They offer innovative solutions such as traffic management systems, vehicle-to-everything (V2X) communication technologies, and cybersecurity measures to protect the integrity of ITS and C-ITS networks;
- **Involvement**: They will not have an active role in the SOC. However, during the tender process for building new infrastructure, weight could be given to manufacturers that provide monitoring APIs or solutions.

Telecommunications companies

- **Role**: Telecommunications companies provide the necessary communication infrastructure for ITS and C-ITS. They ensure reliable and secure data transmission between vehicles, infrastructure, and central systems;
- **Contribution**: They offer high-speed, low-latency communication networks, such as 5G, which are critical for real-time data exchange in C-ITS environments;
- **Involvement**: They will not have an active role in the SOC. However, metrics from potential network shortages could be monitored in the SOC.

Public and private sector partnerships

- **Role**: Collaboration between public and private sectors is essential for the successful deployment of ITS and C-ITS. These partnerships leverage the strengths and resources of both sectors to achieve common goals;
- **Contribution**: They facilitate the sharing of knowledge, expertise, and resources, leading to more effective and efficient implementation of ITS and C-ITS projects;
- **Involvement**: This stakeholder is out of context for this project as it is mainly used for the commercial aspect.

End users

- **Role**: End users, including drivers, passengers, and pedestrians, are the ultimate beneficiaries of ITS and C-ITS. Their feedback and engagement are crucial for the continuous improvement of these systems;
- **Contribution**: They provide real-world data and insights that help refine and optimize ITS and C-ITS solutions to better meet their needs and expectations;
- **Involvement**: End users could potentially raise alerts to the SOC in case of abnormal ITS and C-ITS behavior (for example, suspicious text on an LED panel on the highway).

Research institutions and academia

- **Role**: Research institutions and universities contribute to the advancement of ITS and C-ITS through research and development. They explore new technologies, conduct pilot projects, and evaluate the effectiveness of different solutions;
- **Contribution**: They provide valuable insights, innovative solutions, and evidence-based recommendations that drive the evolution of ITS and C-ITS;
- **Involvement**: Research projects at the European level have highlighted the C-ITS ecosystem and the potential security flaws. Therefore, their reporting can be taken as state-of-the-art.

2.3 C-ITS regulatory context

The regulatory context for C-ITS involves a mix of international standards, regional regulations, and national laws that may govern and be applicable to both deployment of C-ITS technologies and cybersecurity measures required to protect them. This section is focusing on international references first, to then be oriented on Swiss specificities. It will summarize those references at different levels, starting with legally binding requirements down to technical standards and guidance for best practice implementations.

References addressing in-vehicle systems, especially the ones related to vehicle type approval (e.g. UNECE WP.29 / R155 [6] and R156 [7], ISO/SAE 21434 [20], ISO 26262 [21] or ISO 24089 [22]) are excluded from this section due to their intended purpose and applicability to vehicle manufacturers. In addition to this vehicle-level exclusion, technological references (e.g., wireless spectrum allocation by country for C-ITS applications) is also considered as out of scope.

C-ITS as part of Critical Infrastructure

C-ITS is a critical component of modern transport systems and is therefore considered part of critical infrastructure. Critical infrastructure refers to the systems, facilities, and assets that are indispensable for the functioning of society and the economy, and whose disruption

could have significant repercussions on public safety, security, health and economic stability.

Switzerland, like many countries, has a precise list of its critical infrastructures and has established rules for managing them. Critical infrastructures in Switzerland are divided into ten sectors, including energy, finances, information & communication, public administration, public health, public safety, transport, food and water, and waste disposal. These sectors are themselves divided into 27 sub-sectors. Each element providing services in these sub-sectors, such as operating companies, IT systems, facilities, and buildings, is considered part of the critical infrastructure.

As a critical element of the transport sector, C-ITS is subject to cybersecurity regulations governing critical infrastructure. SOCs in C-ITS environments must therefore also comply with these regulations. The impact of these regulations on SOCs will be described in a later chapter.

2.3.1 International references & guidance

This section provides a comprehensive list of legal and technical documents related to cybersecurity that apply to C-ITS stakeholders.

European Union

GDPR: General Data Protection Regulation [1]

GDPR applies to any personal data processed within C-ITS, such as vehicle identification data or location data. C-ITS operators must ensure that data collection, storage, and processing comply with GDPR requirements, including obtaining user consent and implementing data protection measures.

NIS2: Network and Information Systems Directive (EU) 2022/2555 [11]

This directive aims to improve the cybersecurity of essential services, including transport infrastructure. It requires C-ITS operators, especially those managing critical infrastructure, to implement appropriate security measures and report significant cybersecurity incidents to national authorities.

CRA: Cyber Resilience Act (amending Regulation (EU) 2019/1020) [2]

These regulations aim to improve the cybersecurity of all products with digital elements sold in the EU and Switzerland. With this new regulation, all products will need to apply cybersecurity by design principle, be monitored and maintained to ensure their security. C-ITS equipment would fall under this scope. Therefore, security bulletins or information from product suppliers could be forwarded to the SOC.

“Revised ITS Directive” Directive (EU) 2023/2661 [12]

This directive updates Directive 2010/40, which provides a framework for the deployment of ITS in the field of road transport and for interfaces with other modes of transport. It emphasizes cybersecurity requirements, requiring data protection, secure communications, incident response and recovery measures. Directive 2023 introduces an important change by requiring Member States to guarantee data availability and ensure the deployment of specific ITS services. This measure aims to remedy fragmentation and improve geographical continuity, two factors that have hampered the development of ITS in the EU.

United States

CIRCIA: Cyber Incident Reporting for Critical Infrastructure Act – 2022 [8]

CIRCIA is a US federal law that requires critical infrastructure entities to report any cyber incidents or ransomware attacks to the Cybersecurity & Infrastructure Security Agency (CISA) within specific timelines.

CISA Guidelines

Following CIRCIA, CISA published guidelines, which are targeted guidance for Incident Response in critical infrastructure sectors, such as the water and wastewater sector [9]. These guidelines rely on established **NIST Special Publications** which provide guidance on how to deal with cybersecurity incidents [23].

2.3.2 Swiss references

In Switzerland, cybersecurity concerns are now addressed by the Federal Office for Cybersecurity (BACS – Bundesamt für Cybersecurity), formerly the National Cyber Security Centre (NCSC), to harmonize the approach for every office and/or department. Each office/department can tailor these requirements to specific domain needs. This section outlines the key Swiss legal and technical references relevant to C-ITS stakeholders.

ICT minimum standard – NCSC [24]

At the national level, an ICT minimum standard for critical sectors was published in 2024. This standard is designed as a baseline security standard, covering a range of topics such as identification, protection, detection, reaction and recovery. Due to legacy concerns, the Federal Office of Economy, which was responsible for the NCSC at that time, published this guidance. Although national roads are not yet classified as a critical sector, they are part of the infrastructure used by public transport, which is critical. In this context, road infrastructure elements such as road lighting, tunnels, and ventilation systems are highlighted.

The ICT standard is based mainly on NIST Cybersecurity Framework Core [23]. The NIST cybersecurity framework will be presented in a later chapter. It is used in this project as reference for SOC implementation as well.

FAISC: Federal Act on Information Security [5]

This federal act sets out specific requirements for critical infrastructure, including the transport sector. It includes mandatory requirements such as risk management, incident reporting and system stability measures. For C-ITS operators, classified as part of critical infrastructure, this means that they must report cyberattacks on C-ITS system to the BACS, implement measures to identify, mitigate and manage cybersecurity risks and perform regular testing and maintenance of C-ITS systems.

nFADP: New Federal Act on Data Protection [4]

Switzerland's nFADP has been recognized by the UE to be compliant with GDPR. The law defines data processing, handling and protection requirements. Swiss C-ITS operators must ensure that data collection, storage, and processing comply with these requirements.

FEDRO - Specific directives

The Federal Department of the Environment, Transport, Energy and Communications (DETEC), specifically the FEDRO, is responsible for roads in Switzerland. Consequently, all legal aspects fall under their jurisdiction. While these directives and laws primarily focus on road safety, some also pertain to the cybersecurity of OT and IT environments. The relevant directives are described below:

Instruction on OT Security governance - ASTRA 73006 v1.00 [13]**:**

This instruction describes how FEDRO deals with OT cybersecurity and especially with the operational and safety equipment (FR EES: *Equipment d'exploitation et de sécurité*, DE: *BSA Betriebs- und Sicherheitsausrüstung*en), which can be summarized as a part of the ITS and C-ITS infrastructure in this research report.

Directive on OT Security - ASTRA 13030 V2.0 [14]

This directive outlines the principles of a uniform security architecture for the operational and safety equipment, EES, of the FEDRO. It also offers a preliminary risk analysis. Additionally, a section about the development of a SOC for OT managed by FEDRO is included. While C-ITS systems are not specifically addressed, the general OT security principles, risk analysis and SOC development outlined in the directive may be relevant for C-ITS systems integrated into Switzerland's road infrastructure.

Instruction on Roles and requirements for EES management - ASTRA 73001 [15]

This instruction introduces a management system for Operating and Safety Equipment (ESS). It includes processes for identifying, listing and managing ESS, enabling planning and maintenance standardization nationwide. Key aspects such as risk-based maintenance, defined roles and responsibilities for ESS management and data management are outlined. These elements could provide significant value for organizing and managing the OT components of C-ITS systems.

Instruction on Management of operational and security equipment: roles, tasks, and requirements for user interfaces - ASTRA 73002 V1.01 [16]

This instruction lists all roles and tasks related to operational and safety equipment. While it lacks specific cybersecurity roles, its framework could be expanded to include them. The clear role definitions and tasks presented in this instruction are particularly relevant for C-ITS environments, as they are essential for effective system management. This document is also referenced in ASTRA 13030, underscoring its significance in the broader context of OT security initiatives.

DIRECTIVE on the IP EES Network ASTRA 13040 V1.3 [17]

This directive describes a uniform communication infrastructure used in Switzerland. This infrastructure would allow efficient communication between the EES network, regional networks, and national networks. The requirements for the operation of a EES IP network, such as technologies and network protocols, as well as standardization needs and network security are addressed. Requirements for the implementation and operation of EES IP networks are also defined. This infrastructure forms a robust foundation for C-ITS communication. The implementation of a SOC for C-ITS will benefit from this standardized communication network.

Summary

This analysis highlights that C-ITS and ITS are already integrated into the infrastructure managed by FEDRO under another name: Operational and Safety Equipment.

The multiple directives and instructions governing EES management, communication networks, and OT security provide a solid basis for the development of a SOC for C-ITS systems. Standardization of ESS processes throughout Switzerland will facilitate the integration of the SOC into existing frameworks. The IP EES network described in ASTRA Directive 13040 ensures scalability, availability and security for C-ITS communication. Additionally, ASTRA Directive 13030 outlines principles for OT security and includes plans for a SOC to manage EES security, which can be adapted for a specialized SOC in the C-ITS environment. These documents collectively form an essential basis for the solution considered in this project and ensure alignment with Switzerland's operational standards.

It is important to note that while these documents provide strong foundations for OT aspects, a C-ITS SOC must address the intersection of IT and OT systems. Additional IT-specific guidance from other documents will be essential to ensure a secure implementation.

2.3.3 C-ITS reference summary

Looking at the regulations, Switzerland's regulatory approach is relatively in line with international regulations and directives.

Regarding data protection and privacy, Switzerland's nFADP [4] has been recognized by the EU as GDPR-compliant. This alignment is essential for C-ITS systems, as it ensures compliance for cross-border data exchanges.

About cybersecurity regulations, FAISC [5] is broadly aligned with the NIS2 Directive [11], both of which address cybersecurity for critical infrastructures, requiring risk management, incident reporting and system stability measures. FAISC is, however, adapted to Switzerland's federal structure.

Switzerland lacks a direct equivalent to the EU's CRA [2]. Nonetheless, Swiss companies fall under CRA requirements if their products enter the European market. For C-ITS equipment such as on-board units and roadside devices, CRA compliance is likely to be necessary to ensure cross-border interoperability and security. Current C-ITS equipment in Switzerland, while not falling under the CRA, may still require upgrades to comply with it and in the future meet evolving interoperability requirements.

The EU's revised ITS Directive covers both IT and OT aspects of ITS, including ITS data protection and incident response. In comparison, Swiss FEDRO directives primarily focus on OT security, leaving IT-specific aspects less defined, with the exception of the ASTRA Directive on EES network communication infrastructure. This gap highlights the importance of aligning Swiss Directives with EU directives to ensure comprehensive coverage for the project's foundations.

Unlike the EU or US frameworks, Switzerland has on top of its FAISC an ICT minimum standard tailored to critical sectors that provides baseline security measures.

Tab. 2 summarizes all international and national documents that reference cybersecurity in the context of C-ITS and to which stakeholder these artefacts apply.

Tab. 2 *International rules and regulations*

References	Gov. Agencies	Transport Authorities	OEM	Tech. provider	Telecom. companies	End Users	Academic
GDPR [1]	x	x	x	x	x		
Directive (EU) 2022/2555 "NIS2" [11]	x	x		(x)			
"CRA" Cyber Resilience Act [2]	x		x	x			
Directive (EU) 2023/2661 "Revised ITS Directive" [12]				x	x		
CIRCIA (US) [8]	x	x		x	x		
CISA Guidelines	x	x		x	x		
FAISC (CH) [5]	x	x		x			
nFADP (CH) [4]	x	x	x	x	x		
Minimal ICT standard [24]	x	x					
OT Security governance ASTRA 73006 v1.00 [13]		x					
Directive on OT SECURITY ASTRA 13030 [14]		x					
Instructions on Roles and requirements for EES mgmt. ASTRA 73001 [15]		x					
Instruction on Management of operational and security equipment: roles, tasks, and requirements for user interfaces ASTRA 73002 V1.01 [16]		x					
DIRECTIVE on IP EES Network ASTRA 13040 V1.3 [17]		x					

Transport authorities are the primary stakeholders across most of these documents, given their responsibility for managing ITS systems. Government agencies, tech providers and telecom companies are also affected by these regulations due to their roles in governance, infrastructure, service provision and communication networks. This regulatory framework provides the foundation for developing a SOC for C-ITS. Specific SOC references and guidance will further support this foundation and will be detailed in a later chapter (4.2).

2.4 C-ITS architecture – Purdue model

As C-ITS continue to evolve, the convergence of IT and OT within these systems has become increasingly critical. Managing the complex interactions between data-driven decision-making processes and real-time control of physical infrastructure requires a robust architectural framework. The Purdue Enterprise Reference Architecture (PERA) [48], commonly known as the Purdue Model, offers a well-established structure for organizing and securing these interactions. Originally developed for industrial control systems, the Purdue Model provides a layered approach that separates different levels of operations, from enterprise-level IT systems to field-level OT devices. By applying the Purdue Model to C-ITS, transportation networks can effectively integrate IT and OT assets, ensuring seamless communication, enhanced security, and reliable operation of intelligent transport solutions. Such standard architecture provides several benefits described in *Tab. 3*. Furthermore, this model is also described in the technical standard ISA/IEC 62443 [25], which is referenced in the minimal standard for ICT published by the Swiss government.

***Tab. 3** Purdue model – Benefits*

Purdue model benefits	Information
Structured Approach to System Design and Operations	**Layered Architecture:** The Purdue Model provides a clear, hierarchical structure that separates different levels of operations, from high-level enterprise management down to the physical processes. This helps organizations design, implement, and manage complex systems by breaking them down into manageable layers. **Separation of Concerns:** By delineating layers based on function, the Purdue Model helps to clearly define the roles and responsibilities of different system components, making it easier to manage and optimize each part without impacting others.
Enhanced Security	**Defense-in-Depth:** The layered approach of the Purdue Model naturally supports a defense-in-depth security strategy. Each layer can be secured independently, ensuring that a breach at one level does not easily propagate throughout the entire system. **Segmentation and Isolation:** The model promotes network segmentation, particularly between IT (enterprise) and OT (operational) systems. By isolating critical OT systems from potentially vulnerable IT systems, the Purdue Model minimizes the risk of cyberattacks affecting essential infrastructure.
Simplified Integration and Interoperability	**Standardization:** The Purdue Model is a well-established framework, widely recognized across industries. Its adoption in C-ITS can standardize the way IT and OT systems are integrated, ensuring interoperability between different vendors and technologies. **Scalability:** The model's clear structure makes it easier to scale systems. As transportation networks grow or new technologies are integrated, the Purdue Model provides a roadmap for expanding or upgrading systems without disrupting existing operations.
Improved Operational Efficiency	**Focused Optimization:** By separating functions across different layers, the Purdue Model allows for targeted optimizations at each level. For example, real-time operational systems can be fine-tuned for performance without affecting enterprise-level data processing systems, and vice versa. **Centralized Management:** The model supports centralized management and monitoring of systems. For instance, a central traffic management center can oversee the entire C-ITS operation, with clear visibility into both IT and OT layers.
Compliance with Industry Standards	**Alignment with Best Practices:** The Purdue Model aligns with many industry standards and best practices for industrial control systems and cybersecurity. This can help organizations meet regulatory requirements and adhere to industry guidelines, particularly in sectors where safety and reliability are critical.
Resilience and Reliability	**Fault Isolation:** The hierarchical nature of the Purdue Model ensures that faults or failures in one part of the system can be isolated and managed without affecting the entire network. This is particularly important in C-ITS, where maintaining continuous operation of traffic control systems is crucial. **Robustness Against Threats:** The separation of layers, particularly with the security enhancements at Level 3.5, provides a robust defense against both cyber and physical threats, contributing to the overall resilience of the system.

Fig. 18 illustrates an example of the application of the PURDUE model to an organization that uses and manages a C-ITS infrastructure. Every level is described and illustrated with examples. Starting from Level 0, which is composed of field devices, up to Level 4/5, laptop and business software, definitions and examples are listed in *Tab. 4*.

The convergence of IT and OT domains presents significant challenges in assigning specific Purdue model levels to certain devices. Traditionally, levels within the Purdue model include devices and elements of a similar nature (e.g., Level 4/5 primarily consists of laptops, servers, and network devices). However, the increasing use of IT equipment for industrial applications (e.g., Industrial IoT) and the adoption of standard IP-based protocols blur these distinctions. As a result, categorizing devices into a single Purdue model level, particularly at the lower architectural levels, becomes complex.

To address these challenges and establish a common understanding of IT and OT similarities and differences, the following section outlines the specific characteristics of each category. It then presents C-ITS elements as examples from both domains. In this context, the term ‘asset’ refers to elements considered critical to protect in order to prevent significant damage scenarios.

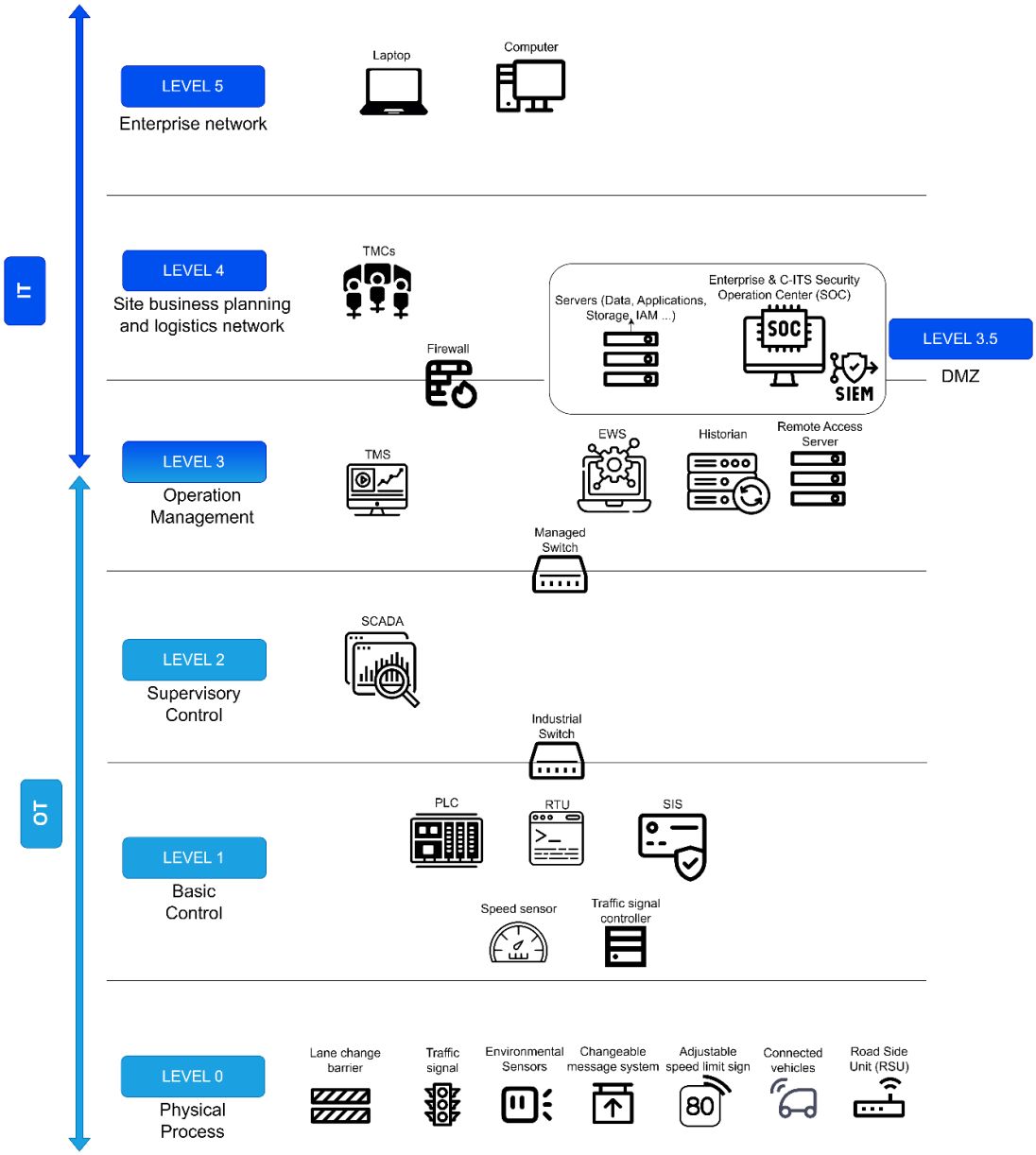


Fig. 18 *Purdue model applied to C-ITS context.*

***Tab. 4** Purdue model – architecture levels and examples*

Purdue model level	Roles and examples
Level 0 – Physical process	**Role** – The Physical Process level is the foundation of the Purdue Model, representing the actual physical systems and environments that the OT devices control and monitor **C-ITS Example** – This level includes vehicles on the road, pedestrians, and the road infrastructure itself. For example, sensors embedded in the road surface detect the presence of vehicles, while cameras monitor traffic conditions and relay this information back up the layers for analysis and control.
Level 1 – Basic control	**Role** – This layer consists of the basic control systems that directly interact with physical processes. These systems execute commands issued by the supervisory control systems and are responsible for the immediate control of devices in the field. **C-ITS Example** – Traffic lights controller, speed sensors, and pedestrian crossing signals controller are all part of this layer. For example, a traffic light controller might receive instructions from a SCADA system to change the light cycle based on the detected presence of vehicles or pedestrians.
Level 2 – Supervisory control	**Role** – At this level, supervisory control systems oversee the direct control of field devices, ensuring that the actions taken by these devices align with the operational goals set by Level 3. This layer typically includes SCADA systems or other supervisory systems. **C-ITS Example** – In a smart city, a SCADA system might monitor and control traffic lights, variable message signs (VMS), and environmental sensors. For instance, during peak hours, the system could dynamically adjust the timing of traffic lights to reduce congestion based on real-time data collected from road sensors and cameras.
Level 3.5 – Demilitarized Zone (DMZ)	**Role** – Level 3.5 in the Purdue Model is essential for securing and managing data from lower levels by establishing a Demilitarized Zone (DMZ). Acting as a buffer between OT and IT networks, the DMZ enables secure data monitoring and control. It serves as a centralized point for collecting traffic flow, vehicle movement, and incident data, providing the ideal location for implementing a SOC in C-ITS. Here, continuous security monitoring, threat detection, and response can occur to protect communications across all levels. **This layer is typically where Hybrid IT-OT Security Operation Centers are implemented and operating.** **C-ITS Example** – The DMZ is crucial for gathering real-time data from traffic sensors, cameras, and monitoring devices, creating a centralized view for the SOC. For example, data flows from traffic sensors and cameras are analyzed within this zone to detect intrusions, attacks, or threats to the network. This centralized collection helps identify anomalies or suspicious behaviors, triggering alerts if threats like hacking attempts, DDoS, or unauthorized access to traffic control systems are detected. By acting as a central point for data collection and filtering, the DMZ also safeguards communications with IT networks while enabling swift incident response.
Level 3 – Operation management	**Role** – This layer is where IT and OT converge to manage and monitor real-time operations. It includes systems that oversee traffic flow, control vehicle movements, and ensure that transportation services operate efficiently. **C-ITS Example** – A central traffic control center might use traffic management systems (TMS) to monitor and control traffic signals across a city in real-time. These systems can adjust signal timings based on current traffic conditions, provide priority to emergency vehicles, and manage incidents like accidents or road closures.
Level 4 – Site business planning and logistics network	**Role** – This layer connects the enterprise management systems with the operational control systems. It focuses on planning, scheduling, and logistics to ensure that day-to-day operations align with broader strategic goals. **C-ITS Example** – A regional traffic management center (TMC) might use data from the enterprise network to coordinate with local authorities and logistics companies. For example, during a large public event, this level could optimize traffic signal timings and coordinate freight deliveries to avoid congestion, aligning with the strategic objectives defined at the enterprise level.
Level 5 – Enterprise network	**Role** – The Enterprise Network is the topmost layer, where high-level data processing, business decisions, and long-term planning occur. This layer handles the management of overall transportation strategies, such as urban mobility planning, resource allocation, and performance monitoring. **C-ITS Example** – In a city's transportation department, enterprise-level systems might analyze data collected from various sources (e.g., traffic flow, weather conditions, and public transportation usage) to optimize urban traffic management strategies. For instance, data-driven decisions could lead to changes in public transit schedules or the allocation of resources for road maintenance.

2.5 C-ITS – Asset grouping

As briefly introduced above, the term "asset" refers to any resource, component, or information that holds value to an organization or system and, therefore, needs protection from potential threats (*Fig. 19*). Assets can be physical, digital, or even intangible, and their value is determined by their role in achieving the organization's objectives and the potential impact of their being compromised. In the realm of C-ITS, assets encompass a wide range of elements that are crucial for the safe, secure and efficient operation of transportation networks. These assets can be categorized into different types, each requiring specific cybersecurity measures and smart monitoring to protect them from threats and to detect any adversarial conditions.

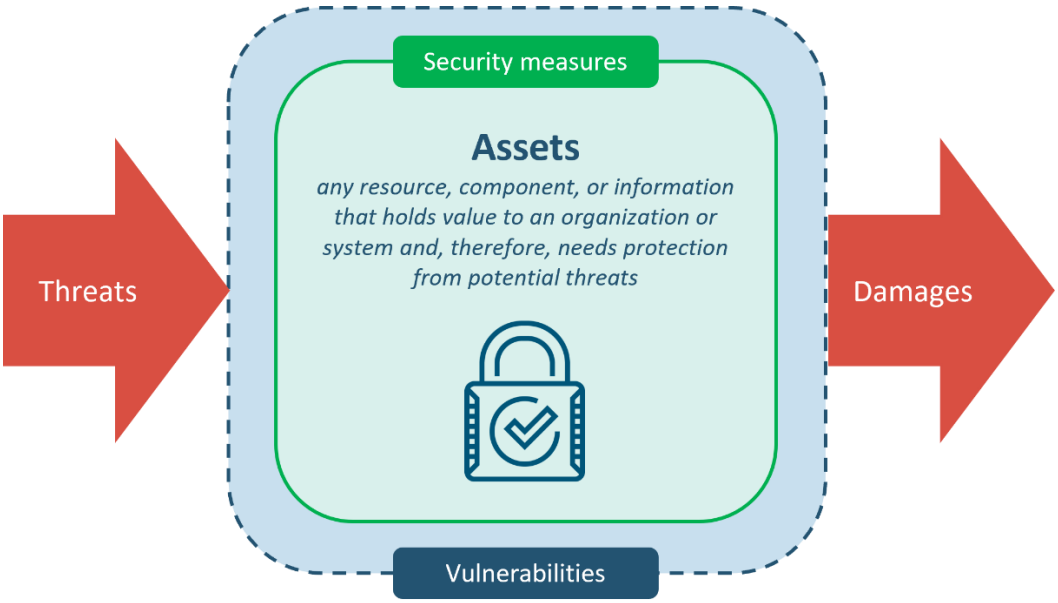


Fig. 19 *Introduction to assets – from threats to damages.*

This level of abstraction (asset-level) is also the one suggested by the MB4 Cyber Threat project [41] to be used as a baseline for cyber threat assessment. In the context of a targeted framework combining both proactive and reactive processes, the use of common nomenclature is key for communication and efficiency between stakeholders.

The heterogenous nature of assets to be used within C-ITS forces stakeholders to define categories and/or types for segregating them and connecting them to pertinent processes and activities (e.g., "*patching an operator laptop won't require the same level of precautions than for an embedded device managing traffic lights in a critical intersection*").

In the context of this report, two levels of grouping have been defined:

- **C-ITS asset categories**: IT assets and OT Assets (*Tab. 5*);
- **C-ITS asset types**: Information, Software and Hardware (*Tab. 6*).

Both grouping levels are introduced in dedicated sections below.

2.5.1 C-ITS asset categories

Tab. 5 *C-ITS asset categories*

Asset categories	Definition and examples
IT assets	**Definition** – IT assets are the components that manage data, support communication, and facilitate the overall operation of information systems within C-ITS. These assets are typically more software-oriented and are crucial for data processing, analysis, and decision-making **C-ITS Example** – Traffic / user / logs data, Traffic management system, data analytics platform, IT routing equipment, servers, workstations, databases… **Specificities** – Focused on Data Processing and Communication, scalability and flexibility, frequent update-upgrade, confidentiality / integrity / availability first, standardization and interoperability, accessibility, cyber security maturity
OT assets	**Definition** – OT assets are the components that directly interact with and control physical processes within C-ITS. These assets include the hardware and control systems that manage the operational aspects of transportation infrastructure **C-ITS Example** – Traffic Signal Controllers, Sensors, VMS, SCADA systems, PLCs, RSUs… **Specificities** – Focused on Control and Monitoring of Physical Processes, real-time operations, integrity / reliability / availability first, longevity and stability, safety-criticality, proprietary and specialized systems, limited connectivity and environmental constraints, legacy systems…

2.5.2 C-ITS asset types

Tab. 6 *C-ITS asset types*

Asset types	Definition and examples
Information assets	**Definition** – Information assets include data, databases, and any other forms of information that are valuable to the organization. These can range from personal data of users to critical traffic management information. **C-ITS Example** – Traffic flow data, vehicle identification numbers (VINs), and communication logs between vehicles and infrastructure. Protecting this information from unauthorized access or tampering is crucial to maintaining the integrity of C-ITS operations.
Software assets	**Definition** – Software assets encompass all applications, systems, and codebases that are used to manage, process, or interact with other assets. **C-ITS Example** – Traffic management software, real-time analytics platforms, and communication protocols between vehicles and infrastructure. Ensuring these software systems are secure against vulnerabilities is essential to preventing disruptions in traffic operations.
Hardware assets	**Definition** – Hardware assets are the physical devices and infrastructure that support the operation of a system. These include servers, networking equipment, sensors, and control devices **C-ITS Example** – Roadside units (RSUs), traffic signal controllers, sensors, and the physical servers hosting traffic management systems. These devices need to be protected from physical tampering and cyber intrusions to ensure their continued operation.

It has been decided not to consider humans as assets due to the objectives of this project to primarily monitor implemented systems. It is, however, crucial to consider human factors as part of the development of the Security Operation Center, including organizational structure, training, etc. This topic is addressed in section 4.9 SOC – Human factors.

2.6 C-ITS – Systems and application

This chapter provides a comprehensive overview of C-ITS systems and applications, mapped to the appropriate levels of the Purdue model defined in section 2.4 C-ITS architecture – Purdue model, as well as tagged with relevant categories and types as defined in section 2.5 C-ITS – Asset grouping. The chapter concludes with a review of the current state of C-ITS applications, both at the international and national levels.

TMS and TMC play a key role in C-ITS applications. They work together to ensure efficient and safe traffic flow. Here is an explanation of these terms and an example of their operations.

A **Traffic Management System** refers to the tools, technologies and infrastructure used to monitor, control and optimize traffic flow. It comprises a network of sensors, cameras, traffic lights and a software system constantly collecting data on traffic conditions. The data is analyzed and used to adjust traffic flow in real-time. Thus, a TMS includes both physical infrastructure and software systems.

A **Traffic Management Center** is a physical, operational facility that oversees a specific region or jurisdiction. Like a SOC, the TMC centralizes a vast amount of data, with one key source being traffic-related data coming from the TMS. This data is continuously monitored and analyzed by human operators. The TMC uses this information to take action, for example by making informed traffic management decisions, coordinating responses to incidents and communicating with emergency services and road users.

Example scenario

On the A9 highway late in the afternoon, the TMS detects a sudden slowdown near Versoix due to an accident involving multiple vehicles. The local TMC, based in Geneva, receives an alert related to the incident from the TMS. The TMC then takes the following immediate actions:

- Using cameras from the TMS, they assess the severity of the situation;
- They activate alert messages on the highway's message signs to warn drivers;
- They adjust the signal timing at highway entrances to prevent further congestion;
- They coordinate with emergency services, providing the exact location of the incident as obtained from the TMS.

In short, the difference between a TMS and a TMC is that a TMS is a technological infrastructure for data collection and restricted autonomous traffic optimization, whereas a TMC is a human-operated facility using TMS data to take further actions.

C-ITS components and systems

C-ITS rely on a range of interoperable components and supporting systems that enable seamless communication and cooperation between vehicles, roadside infrastructure, and central management platforms. By integrating advanced connectivity technologies and standardized protocols, these components facilitate the real-time exchange of safety-critical and operational information, supporting enhanced road safety, traffic efficiency, and the integration of future automated mobility solutions. *Fig. 20* and *Tab. 7* provide some examples of C-ITS architecture and traffic management applications.

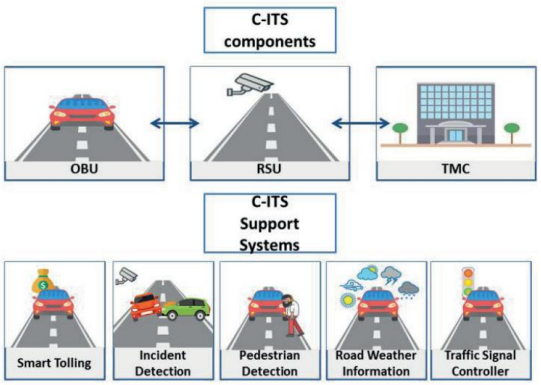


***Fig. 20** C-ITS components and systems **[46]**.*

Tab. 7** Traffic management applications **[47]

Dangerous situations

Warn drivers about roadworks, stationary vehicles, tail ends of traffic jams, etc

Traffic light priority

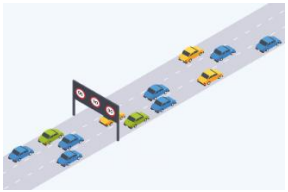
Let ambulances, police cars **and** firefighters move faster, more smoothly and safely in case of an emergency**.**

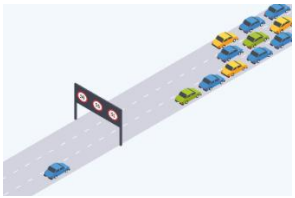
Traffic light information

Inform road users about the time-to-red and time-to-green.

Maximum speed

Display the applicable speed limit on every stretch of road.





Speed advice

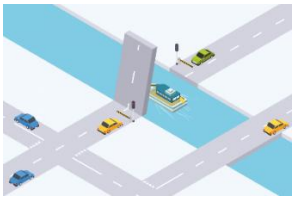
Make sure drivers can hit the brakes in time or start accelerating again.

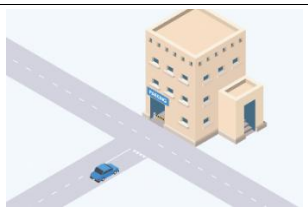
Traffic lane information

Notify drivers about which lanes are open and closed or how fast they can drive.

Bridge openings

Help users avoid open bridges or tell them how long it will take for the bridge to go down again.



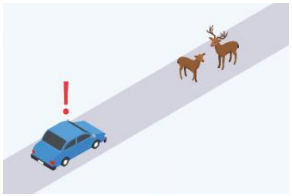


Parking space availability

Guide drivers to parking areas in the neighborhood with free spots.

Animal warnings

Elk, deer or any other large animals on the loose? Alert users to be in a state of readiness.



2.6.1 Purdue model: L0 to L2 – C-ITS systems

The foundational layers (L0-L2) that focus on the physical processes and direct control mechanisms are represented in *Tab. 8*. Level 0 encompasses the road infrastructure, vehicles, and sensors embedded in physical environments, capturing essential traffic and environmental data. Levels 1 and 2 then process and respond to this data in real-time through basic and supervisory control systems, such as traffic light controllers and SCADA systems, managing immediate, on-the-ground transportation dynamics.

***Tab. 8** C-ITS systems and applications [Purdue – L0 to L2]*

System and/or application [*Category* | *Type*]	**Definition and applicable references**
Vehicle-to-Everything / V2X communication *[IT/OT | Information]*	**Definition** – Refers to the technology that enables vehicles to communicate with various entities in their environment, including other vehicles (V2V), infrastructure (V2I), pedestrians (V2P), and the cloud (V2C). This interconnected network enhances road safety, traffic efficiency, and overall transportation management by allowing vehicles to share real-time information about traffic conditions, potential hazards, and navigational data. V2X communication leverages advanced wireless communication protocols, such as Dedicated Short-Range Communications (DSRC) and Cellular Vehicle-to-Everything (C-V2X), to facilitate seamless interactions, ultimately contributing to the development of smarter, safer, and more sustainable transportation systems. **Applicable references** • SN ISO 21217 [26] • SAE J2735 [27]
Road-Side Units / RSU *[OT | Software]* *[OT | Hardware]*	**Definition** – An RSU is a device installed alongside or integrated into road infrastructure, such as traffic lights, signs, or poles. Its main function is to communicate with On-Board Units (OBUs) deployed on vehicles and other RSUs to provide synthesized information and services to vehicles. RSUs collect data such as traffic flow, road conditions, and weather from the surrounding environment. They transmit that information to relevant parties using V2X communications. They can also receive commands or requests from OBUs, such as traffic signal priority requests from emergency vehicles, and coordinate responses accordingly. **Applicable references** – none
Traffic Signal Controller / TSC *[OT | Software]* *[OT | Hardware]* 	**Definition** – This is the safety critical heart of a traffic signal system. The controller ensures that no two colliding lanes ever have a green light at the same time. Newer systems are equipped with a microcontroller and can be connected to C-ITS. Older systems are closed systems. They are typically connected to upper-level network via cellular connectivity. **Applicable references** • SN 640 832 [28] • SN 640 844 3 [29]
Mobile Traffic Signals *[OT | Software]* *[OT | Hardware]* 	**Definition** – For temporary signaling solutions. Typically used during construction work. Newer models may be equipped with cellular connectivity. Typically, the lights can be operated locally by the workers with a radio control. **Applicable references** • SN 640 832 [28] • SN 640 844 3 [29]
Pre-emption device *[OT | Software]* *[OT | Hardware]* 	**Definition** – Interacting with traffic signals and working in pairs. One unit is mounted to the traffic signal, the other to a vehicle. These devices allow high priority vehicles like first responders to pass easily. When an approaching vehicle is detected, crossing lanes are stopped with red light, creating a “green wave” that can reduce response time significantly in crowded urban environments. The device may detect approaching high-priority vehicles with a variety of sensors, such as radio signals, infrared or GPS data transmitted by cellular signal. The communication with the traffic signal is typically wired. **Applicable references** – none

Changeable Message System *[OT | Software]* *[OT | Hardware]* 	**Definition** – Display text messages. Commonly seen on highways, these message boards inform the passing traffic about the length of traffic jams or public safety announcements. The connection to the user interface may be wired or wireless. **Applicable references** • SN EN 12966 [30]
Adjustable Speed Limit Sign *[OT | Software]* *[OT | Hardware]* 	**Definition** – Remotely change speed limits. Used to adapt the traffic speed to current conditions such as the weather or to increase the fluidity of traffic. The connection to the user interface may be wired or wireless. **Applicable references** – none
Railway Crossing Barriers *[OT | Software]* *[OT | Hardware]* 	**Definition** – Block a lane in front of a railway crossing. Used to keep people away from the rails when a train is passing. They may also be connected to C-ITS systems; however, traditionally they are closed systems operating solely with sensors on the railway. **Applicable references** • SN 671 510 [31]
General Transmitter Unit *[IT | Software]* *[IT | Hardware]* 	**Definition** – Can be used to communicate any signal or information collected from the roadside to vehicles and central servers. They can be used to retrofit non-connected infrastructure to the C-ITS network or to connect sensors to the network which are not available as C-ITS components. Uses cellular connection. **Applicable references** – none
Traffic Camera *[OT | Software]* *[OT | Hardware]* 	**Definition** – Provide visual information as an additional source of information for traffic control centers. They can also serve safety purposes such as in tunnels, providing live information to firefighters. The connection to the user interface may be wired or wireless. **Applicable references** • SN 671 971 [32] • SN 671 972 [33] • SN 671 973 [34]
Detector Systems *[OT | Software]* *[OT | Hardware]* 	**Definition** – Gain additional information from various sensors. Different detector systems exist to provide traffic control centers with vehicle counts or information about occupancy of specific lanes. The information may also be about the weather, as seen in the picture to the left. The connection to the user interface may be wired or wireless. **Applicable references** – none
Speed Display *[OT | Software]* *[OT | Hardware]* 	**Definition** – Automatically display the speed of oncoming vehicles. They typically are not connected and serve the only purpose of reminding the drivers of their speed. Some models are connected and share information with a central server. **Applicable references** – none
Supervisory Control and Data Acquisition / SCADA *[IT/OT | Information]*	**Definition** – SCADA (supervisory control and data acquisition) is a control system architecture comprising computers, networked data communications and graphical user interfaces for high-level supervision of machines and

	processes. It also covers sensors and other devices, such as programmable logic controllers, which interface with process plants or machinery. **Applicable references** • ISA112, SCADA Systems [35]

2.6.2 Purdue model: L3 and L3.5 – C-ITS systems

Levels 3 and 3.5 mark the convergence of IT and OT within the C-ITS structure and are represented in *Tab. 9*. Level 3 oversees real-time operations, where traffic flow management, incident response, and vehicle movement controls are centralized. Level 3.5, the DMZ, secures data exchange between OT and IT networks, facilitating the implementation of a SOC. In this hybrid IT-OT space, data can be analyzed to detect and respond to security threats, such as intrusions or attacks, ensuring robust communication across all system levels.

***Tab. 9** C-ITS systems and applications [Purdue – L3 and L3.5]*

System and/or application [*Category* | *Type*]	**Definition and applicable references**
Enterprise / C-ITS SOC *[IT | Information]* *[IT | Software]* *[IT | Hardware]*	**Definition** – The SOC is often a physical room within the organization's office where several employees continually monitor network traffic, alerts, and visualized information that could be used to respond to a potential cyber-incident. This entity is usually composed by numerous software platforms supporting all SOC activities (see details in section 4), including SIEM for equipment monitoring and logs management, SOAR for orchestrating incident-response processes and enhancing SOC lifecycle by adding automation. **Applicable references** • MITRE [44]
Servers (Data, Applications, Storage, IAM) *[IT | Software]* *[IT | Hardware]*	**Definition** – Servers are typically implemented in organizations to store data, manage various applications, control access permissions, and handle account and rights management. They play a vital role in centralizing and securing data, supporting application performance, and ensuring that only authorized users have access to necessary resources, thus strengthening overall IT infrastructure and security. **Applicable references** – none
Historian *[IT | Software]* *[IT | Hardware]*	**Definition** – A historian is a specialized database system designed to collect, store, and retrieve time-series data from various operational processes, particularly in industrial settings. **Applicable references** – none
Remote Access Servers *[IT | Software]* *[IT | Hardware]*	**Definition** – Remote Access Servers (RAS) are critical components of an organization's IT infrastructure, allowing employees to securely connect to the internal network from remote locations. Unlike servers placed in a DMZ, which are intended for external access, RAS are typically located within the internal network to enhance security and protect sensitive data. **Applicable references** – none
EWS *[IT | Software]* *[IT | Hardware]*	**Definition** – An Engineering Workstation (EWS) is a specialized computer designed for configuring, monitoring, and managing devices across various layers of a communication or control system, particularly in industrial and automotive applications. **Applicable references** – none
Traffic Management System / TMS *[IT/OT | Information]* *[IT/OT | Software]* *[IT/OT | Hardware]*	**Definition** – TMS cover a wide array of services associated with traffic oversight and control. This includes monitoring traffic conditions, managing traffic signals and addressing congestion issues. TMS integrate both physical components, like traffic signals and surveillance cameras, and software solutions designed for data analysis and informed decision-making. **Applicable references** – none

2.6.3 Purdue model: L4 to L5 – C-ITS systems

The uppermost levels (L4-L5) extend the C-ITS model to enterprise-wide planning and long-term strategic oversight and are represented in *Tab. 10*. These layers integrate business planning, logistics, and resource allocation, aligning day-to-day transport operations with broader goals. For instance, Level 4 can optimize traffic flow during large events by coordinating with logistics and city authorities, while Level 5 uses data analytics to inform long-term urban mobility and infrastructure development strategies.

***Tab. 10** C-ITS systems and applications [Purdue – L4 to L5]*

System and/or application [*Category* | *Type*]	**Definition and applicable references**
Traffic Management Center (TMC) *[IT/OT | Information]* *[IT | Software]* *[IT | Hardware]*	**Definition** – The primary purpose of a TMC is to oversee and manage various aspects of transportation systems, including monitoring traffic conditions, coordinating incident responses, providing traveler information, managing infrastructure, and optimizing traffic flow. TMCs typically operate at a regional or municipal level and serve as centralized control centers for transportation management. TMS encompasses a broader range of services related to traffic management, including traffic monitoring, incident detection and response, traffic signal control, congestion management, and transportation planning. This system may be considered as a container of application which is documented further after this table. **Applicable references** – none
IT devices *[IT | Software]* *[IT | Hardware]*	**Definition** – IT devices enable personnel to interact with real-time data, manage traffic flows, monitor incidents, and make informed decisions regarding transportation strategies. They provide access to essential software tools that facilitate the analysis of traffic patterns, incident reports, and environmental data, ensuring that employees can efficiently oversee and coordinate transportation operations. **Applicable references** – none

2.6.4 Other key systems interacting with C-ITS

In addition to the foundational and operational layers of the C-ITS outlined in the Purdue Model, various other key systems interact with C-ITS to enhance its overall functionality and effectiveness. These systems are described in *Tab. 11*. While these systems may fall outside the primary scope of C-ITS, their integration is essential for comprehensive traffic management and operational efficiency.

***Tab. 11** C-ITS systems and applications*

System and/or application	**Definition and applicable references**
On Board Units / OBU *[OT | Software]* *[OT | Hardware]*	**Definition** – An OBU is a device installed inside vehicles. Its primary role is to facilitate communication between the vehicle and surrounding road infrastructure. Equipped with various sensors, processors, and communication modules, the OBU collects data on the vehicle's state, driving conditions, and other relevant information, transmitting it to other system components. It can also receive data from roadside infrastructure or other vehicles, such as traffic conditions or safety warnings, enabling the vehicle to make informed decisions while on the road.
Pedestrians' Smartphones *[IT | Software]* *[IT | Hardware]*	**Definition** – Smartphones are widely used communication devices. They collect a variety of information and may interact with parts of a C-ITS to support decision-making and to enrich inputs. This data may be used for real-time information, e.g., in navigation and mapping systems. Smartphones use cellular connections.
All end-applications may be considered here, such as parking management systems, fleet management, etc. A single example is provided below to illustrate the principle.	
Parking Management Systems *[OT | Software]* *[OT | Hardware]*	**Definition** – These systems monitor parking availability and guide drivers to open spaces. They can communicate with vehicles to provide real-time parking information, reducing congestion caused by searching for parking.

2.6.5 C-ITS Application landscape

Swiss C-ITS initiatives

The transformation towards more connected road networks is already underway. Bigger networks are best positioned for benefitting from the efficiency increases and are most likely to have the funds available to push the technology forward. One such project in Switzerland is the Swiss National Traffic Management Office in Emmenbrücke (part of the Swiss Federal Roads Office FEDRO), which is partnering with EBP to develop the Swiss TM application. This program unifies many different traffic management systems currently in use on the Swiss national highways and creates an interactive map of current traffic volumes. The application will also be able to forecast traffic. Information can then be passed on to police and radio stations [49].

Apart from unifying existing traffic management systems, opportunities also present themselves when designing new systems. Such is the case in Neuchâtel, where the company Mobility installed a new traffic supervision system for the two-lane highway traversing the city. Many sections of this highway are in tunnels. After the installation in 2016, the connected sensors, unified across the canton, started providing data for traffic management with the help of calculated rules and pre-programmed scenarios. The architecture of the traffic management system is fully virtualized and used as a digital twin for testing scenarios and running simulations [50].

Indeed, tunnels are critical pieces of infrastructure that benefit from specialised operation centers. The multidisciplinary UNECE group of experts on tunnel safety recommend that operation centers should monitor traffic in normal operation with the help of video streams, congestion reports, and traffic volumes, as well as control the correct functioning of the infrastructure in aspects such as ventilation. In the event of an incident, operators can respond accordingly by directing traffic, turning the light signals at the entrance to red, communicating with first responders and transmitting information to the public via radio. Tunnels are thus an early and small-scale example of a working C-ITS infrastructure and demonstrate the safety benefits these systems can generate. Furthermore, the same group of experts suggest implementing a new type of C-ITS component for tunnels that would check for overheated cargo vehicles [51].

While C-ITS is in rapid development around the world, a related industry – railway systems – has been using similar concepts in traffic management for years. Swiss Federal Railways (SBB), for example, has extensive experience in managing complex rail traffic using an effective traffic management system. In the following section, their Rail Control System (RCS), launched in 2005, is presented. This example highlights how intelligent systems can optimize complex transport networks. RCS has managed to significantly improve reliability and reduce electricity consumption using data from various peripheral systems such as train position sensors (comparable to RSUs) at a rate of several hundred messages per second. Not only is the situation monitored in real time, but forecasts are calculated up to two hours in advance. This foresight allows for considerable optimization and gives time for incident response before the train even leaves the station. SBB also exploits the available information to plan optimum speeds in advance, which are then communicated to the OBUs on each train. These optimizations not only reduce energy consumption, but also minimize wear on both the infrastructure and the trains. Another key component of the RCS is RCS-ALEA, the Alarm and Incident Assistant. This tool enables efficient communication between all parties involved, by organizing and providing case-specific information [52].

Since 2016, SBB has merged dozens of its traffic control sites into 4 main operation control centers. This centralization, in addition to the automation of many repetitive tasks, such as movement optimization algorithms for high-traffic areas, has had a positive impact on the system's efficiency. However, by creating critical hubs (high-value targets) in the system, it has also introduced new vulnerabilities. The growing reliance on these operation control centers underlines the importance of strong security measures.

As part of Switzerland's critical infrastructure, SBB's traffic management system is a prime target for cyber security threats. To counter this, the infrastructure is designed as a modular

system with many redundancies to guarantee resilience. In addition, the network traffic is monitored around the clock by the SBBs information security management system [53], which is in compliance with ISO 27001 [36].

International C-ITS initiatives and pilot projects

C-ITS systems may also include OBUs, which are the responsibility of vehicle manufacturers. For example, some Audi cars already available in resale are equipped with OBUs that receive the time-to-green at intersections from compatible interactive traffic lights. The geographic distribution of interactive traffic lights shows that their greatest coverage is in metropolitan areas of the United States, but also in some parts of Europe, notably Germany. Apart from keeping drivers calm by informing them of upcoming green lights, the OBU also provides a recommended driving speed (based on time to green) to reduce unnecessary acceleration and braking due to the next traffic light. This improves fuel efficiency and therefore also air quality in urban areas. Additionally, these optimizations help to keep traffic more fluid [54].

The deployment of 5G technology is set to enhance C-ITS capabilities. 5G's much greater bandwidth compared to older mobile networks enables more reliable and faster data transfer between RSUs and OBUs. This increased capacity allows for the collection of much larger volumes of data, which is essential for the efficiency and scalability of C-ITS applications. Different pilot projects exploring the potential of 5G have been launched, such as 5G Open Road in France [55].

OBUs are still rare in vehicles today. To meet this challenge and accelerate the adoption of connected technologies, Transport Infrastructure Ireland (TII), together with the European Union, has launched a pilot project for connected vehicles, relying on both OEM-installed OBUs and smartphones. The messages normally displayed on changeable message systems will be sent directly to road users' phones and tablets. These safety alerts include information about collisions, congestions, road work or poor weather [56].

In short, global C-ITS initiatives are enabling significant advances in traffic management systems, safety, security and efficiency. National and international projects demonstrate the potential of connected vehicles, 5G technology and intelligent infrastructure in general.

3 Approaching C-ITS security concerns

As C-ITS become more integrated into national transportation networks, their dependence on digital communication and automation makes the risks posed by cyberattacks grow exponentially. C-ITS elements, whether IT or OT, as well as various information, software, and hardware components, are particularly susceptible to a range of cyber threats that can compromise safety, disrupt services, and expose sensitive data.

Security best practices emphasize the importance of establishing Threat Analysis and Risk Assessment (TARA) prior to any system deployment. This preliminary level of analysis is a key security factor as it ensures the integration of relevant cybersecurity considerations right from the foundations of new systems and infrastructure, which is in line with the **Security-by-Design principle**.

That being said, early-stage or proactive identification of cyber threats may be complex and requires deep understanding of attacker techniques and methodologies. It is for this reason that this project's consortium has already completed a research project specifically targeting establishment of a pragmatic approach to C-ITS threat identification. The research report defined a systematic approach, supported by relevant tools and guidance, to evaluate cyber security risks considered relevant to specific C-ITS use cases. As a conclusion, the report also outlined the need for combining proactive approaches with monitoring and reactive capabilities for all potential threats, even those not currently posing a significant risk, due to the dynamic nature of cybersecurity, a domain in which new attacks and vulnerabilities emerge daily.

With that perspective, this section will outline the key cybersecurity risks associated with C-ITS, referencing major recent cyber-incidents that illustrate the need for a comprehensive and standardized nomenclature to approach and categorize such threats.

3.1 C-ITS cybersecurity – threats and trends

As introduced in section 0 of this report, C-ITS are complex environments with many inherent challenges, including the interoperability of heterogeneous subsystems, the important variety of stakeholders, and the potential for critical safety and societal consequences in case of malfunctions or misbehavior.

The case of the "Dutch traffic lights hack", as described by Ruetir [58], NLTimes [57] and many others, illustrates the potential impact of a security breach and may be used to crystalize the cybersecurity issues entailed by connected road infrastructure. In this October 2024 event, a single ethical hacker acquired the capability to potentially hack tens of thousands of traffic lights in the Netherlands, simply by abusing legacy systems and "naïve" communication protocols implemented in an era when the digital world was not as hostile as today.

The leak was discovered by 29-year-old ethical hacker Alwin Peppels. Peppels investigated the way traffic lights connect to emergency services, and how wireless communications between parties lead to traffic light behavior adjustment. In brief, when emergency services approach traffic light systems, these turn green automatically, while the other lights in the intersection turn red. This system is mostly used to give priority transit to public transport vehicles, to speed-up traffic light switching and to communicate expected arrival time to relevant parties.

The system was based on short-range radio (KAR - *korte afstands radio* - 427–430 MHz) communications used in Netherlands and Belgium since 2005 to control traffic lights via radio signals, as well as for tracking bus and tram positions, assist operators and feed real-time information displays situated at passenger stops. By developing a simple SDR system (Software Defined Radio) using commercially available equipment, Peppels was able to bundle a portable device allowing him to turn any traffic light green at the press of a button.

What makes these types of attacks even more dangerous is that the compromised communication protocols have a range of up to 3-to-4 kilometers depending on

environmental conditions. This means that this adversarial tool, coupled with specificities of the communication protocol used, may allow an attacker to manipulate and/or freeze traffic lights within a significant perimeter.

In this case, thanks to an ethical hacker, the risk was identified before any attack could be carried out, and mitigation measures were soon implemented. Root cause analysis traced the vulnerability back to outdated equipment and demonstrated the need for large-scale product replacement. The number of affected and potentially compromised devices is so high, in fact, that, according to some estimates, it will take until 2030 to fully replace these outdated traffic light systems and to eliminate the vulnerability.

This traffic light hack, though not leading to a direct known incident so far, reveals a lack of foresight and cybersecurity awareness at the time the first traffic light control systems were deployed. If the Dutch Public Transport authority had identified the cybersecurity risks at an earlier stage, it would have been able to define cybersecurity requirements for product manufacturers and integrators, both at the implementation level in terms of a security concept and viable security mechanisms, and at the monitoring level to continuously watch for potential abuse.

Similar incidents potentially targeting road infrastructure were described in a study conducted at the University of Applied Sciences of Western Switzerland (Fribourg), which documented how a simple consumer-grade device may be able to fool an automated vehicle interacting with a connected traffic light [59].

Tab. 12 summarizes the best-known cyber security incidents of the last decade. The list is not exhaustive, but it covers a wide range of incidents impacting various assets.

***Tab. 12** Kown cybersecurity events and incidents impacting C-ITS*

Cybersecurity event / incident	Descriptions
MadRadar hack – towards self-driving cars hallucination (2024)	**Descriptions** – The MadRadar hack bypasses the anti-spoofing protections in the radars of self-driving cars and can trick targets into imagining vehicles that are not there – or hiding other ones that are. While being focused on vehicle-level attack, this illustrates the growing importance of holistic security for mobility ecosystems. **References** – [60]
Toronto Transit Commission – Ransomware (2021)	**Descriptions** – Operational systems normally used to communicate with vehicle operators were compromised and maliciously encrypted, forcing the agency to use a backup radio system that was potentially vulnerable to further attack. The attack appears to have been wide-ranging and affected multiple systems. **References** – [61]
Traffic light hack through cyclist app (2020)	**Descriptions** – Vulnerabilities in an ITS that would allow attackers to influence traffic lights (tested in at least 10 different cities in the Netherlands) over the internet. This hack would spoof nonexistent bicycles approaching an intersection, tricking the traffic system into giving those bicycles a green light and showing a red light to any other vehicles trying to cross in a perpendicular direction. **References** – [62]
Deutsche Bahn - WannaCry (2017)	**Descriptions** – German rail operator Deutsche Bahn announced its systems had been compromised and maliciously encrypted in a global cyberattack that caused computer turmoil in nearly 100 countries. **References** – [63]
San Francisco Municipal Transport Agency - HDDCryptor malware (2016)	**Descriptions** – Hackers managed to infect and take over more than 2000 computers that operated San Francisco's public transport system. Gates had to be opened to allow passengers to ride for free. **References** – [64]

Tab. 12 illustrates current adversarial trends, mostly targeting regular IT infrastructure and systems, and leading to operation disruption and misbehavior. It is important to note that the relatively low number of reported cyber-incidents is explained not by a generally high level of security in C-ITS, but by the very limited number of operational C-ITS as of today.

The risk of critical vulnerabilities in C-ITS should not be underestimated. The deployment of C-ITS assets and related functions in the near future, coupled with a global proliferation of automated systems in vehicles and an increasing number of interactions with road infrastructure, should be understood as a multiplication of attack vectors resulting in a growing attack surface. Based on that, the following high-level consequences may be projected:

- **Traffic disruptions**: Manipulation of V2X data could cause false traffic signals or incorrect information about road conditions, leading to traffic jams or accidents, including:
    - **Disruption of emergency services**: Spoofed or intercepted messages could prevent emergency vehicles from receiving real-time priority at intersections, delaying response times and endangering lives.
- **Loss of trust in system integrity**: If communication data between vehicles and infrastructure is tampered with, users may lose confidence in the system's reliability, reducing adoption of C-ITS services;
- **Vehicle malfunctions**: Attackers manipulating V2V or V2I messages could cause vehicles to make incorrect driving decisions (e.g., sudden braking, acceleration, or lane changes), especially considering upcoming automated vehicles, leading to accidents or traffic chaos;
- **Data breaches**: Sensitive vehicle, passenger, or traffic data could be intercepted, leading to privacy violations and data breaches;
- **System downtime**: A successful DoS attack on C-ITS components (e.g., traffic control centers, RSUs) could render them inoperative, leading to widespread traffic disruptions and gridlock;
- **Interruption of critical functions**: Key safety features such as collision warnings or adaptive traffic control could be disabled, increasing the likelihood of accidents;
- **Sabotage or data theft**: Employees with access to C-ITS infrastructure could intentionally compromise systems, causing disruptions or exfiltrating sensitive data, including traffic patterns, vehicle data, or personal information;
- **Undetected malicious activity**: Insider knowledge of the system's architecture and security protocols could allow attackers to bypass defenses and plant malware or manipulate data without immediate detection;
- **Destruction of physical infrastructure**: Attackers could physically damage RSUs, traffic signals, or other roadside infrastructure, disrupting communication between vehicles and the C-ITS ecosystem;
- **Loss of system availability**: Physical attacks targeting key infrastructure components (e.g., traffic management centers or sensor networks) could lead to system outages and a complete loss of traffic management capabilities;
- **Increased repair costs**: The need for physical repairs and replacement of compromised components could result in significant costs, as well as extended downtime during the repair process.

The heterogeneity of C-ITS assets, threats and potential consequences forces stakeholders to share a common knowledge baseline and nomenclature to address cyber -risks. In this context, The MITRE ATT&CK framework [44] offers a comprehensive, open-source knowledge base that catalogs the behaviors, techniques, and methods cyber-adversaries use in real-world attacks. Developed by MITRE Corporation, it stands for Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK), and it is designed to help organizations understand, detect, and defend against a wide range of cybersecurity threats.

3.2 Core Concepts of MITRE ATT&CK

At its core, MITRE ATT&CK organizes cyber threats around the concept of Tactics, Techniques, and Procedures (TTPs):

Tactics:

- These represent the adversary's goals or the "why" behind an attack. Tactics describe high-level objectives attackers are trying to achieve during different stages of an attack. Examples include gaining initial access, maintaining persistence, or exfiltrating data. Tactics are structured in a sequential model called the ATT&CK matrix, representing different phases of an attack, from the initial breach to achieving the end goal
- Two sequences for IT and OT targets respectively:
    - ***IT**: Reconnaissance; Resource Development; Initial Access; Execution; Persistence; Privilege Escalation; Defense Evasion; Credential Access; Discovery; Lateral Movement; Collection; Command and Control; Exfiltration; Impact.*
    - ***OT**: Initial Access; Execution; Persistence; Privilege Escalation; Evasion; Discovery; Lateral Movement; Collection; Command and Control; Inhibit Response Function; Impair Process Control; Impact.*

Techniques:

- Techniques describe the "how" of an attack. They explain the specific methods or actions adversaries use to achieve their objectives (tactics). For example, to achieve the tactic of gaining "initial access," adversaries might use the technique of phishing or exploiting public-facing applications;
- Techniques can vary across different environments (IT, OT, cloud, mobile), and the ATT&CK framework provides a detailed breakdown of how techniques are applied in each scenario;
- More than 280 techniques are documented. These are spread over different targeted environments (IT, OT, cloud, mobile).

Procedures:

- Procedures are the detailed implementations of techniques. These are the specific methods attackers use in real-world operations. For instance, a procedure may describe how a particular threat group uses spear-phishing emails to deliver malware;
- The MITRE ATT&CK framework continually evolves, documenting adversary procedures based on actual incidents, making it highly relevant for security teams.

The MITRE framework is accessible through dedicated platforms providing a navigation pane as presented in *Fig. 21*.

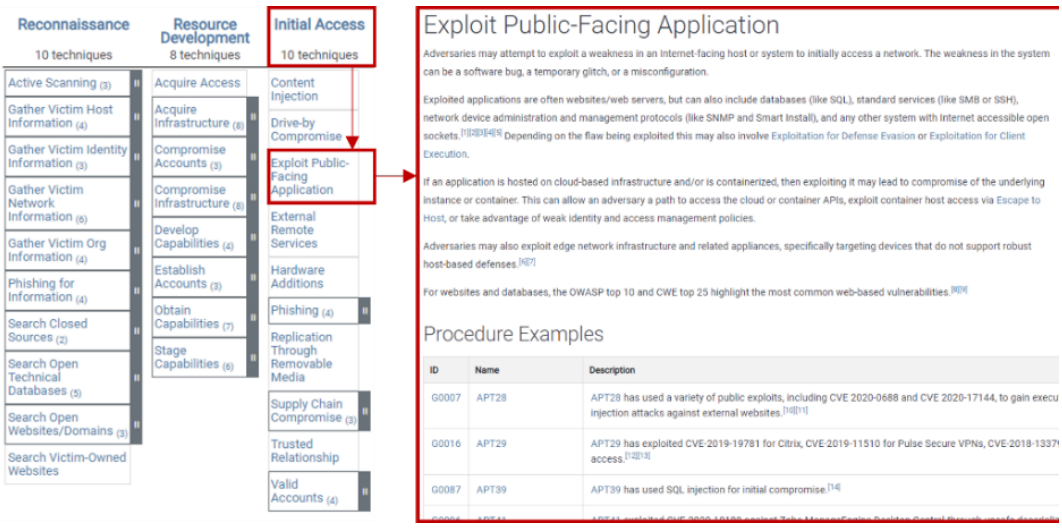


***Fig. 21** Introduction to assets – from threats to damages [44].*

As defined within both the IT and OT frameworks, tactics are a logical sequence an attacker might follow, starting from initial active and/or passive reconnaissance, down to exfiltration and final impact on targeted systems, which here means C-ITS and their stakeholders (see *Fig. 22* below illustrating the IT matrix)

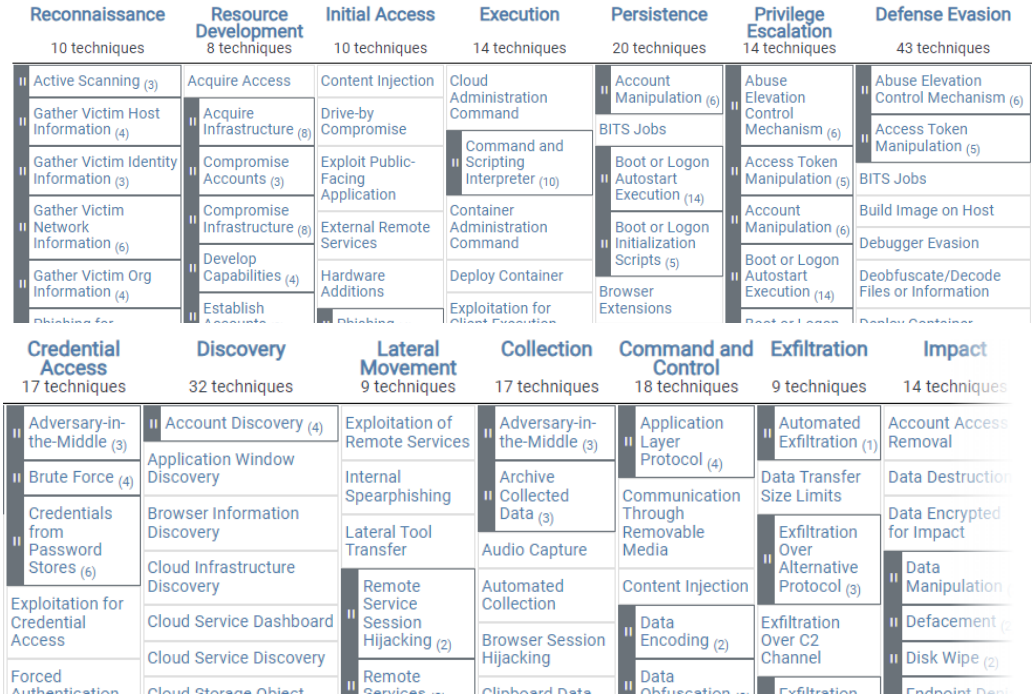


Fig. 22 *MITRE ATT&CK – IT matrix with tactics as headers [44].*

Tab. 13 offers an example of an attack chain that would impact traffic light control over a TMS:

Tab. 13 *Example of Kill Chain connected to ATT&CK framework (OT)*

Kill Chain steps [ATT&CK Tactics]	**Example of applied adversarial methods [ATT&CK Techniques]**
#1 – Initial Access	*[T0862 – Supply Chain Compromise]* *Adversaries may compromise a supply chain to gain control systems environment access by means of infected products, software, and workflows. This might be through the use of an infected library within TMS ecosystem.*
#2 – Execution	*[T0821 – Modify Controller Tasking]* *Adversaries may modify the tasking of a controller to allow for the execution of their own programs. The attacker could then execute their own programs and adjust / modify rules for traffic management.*
Persistence	*Kill chains do not systematically use all tactics stages. In our context, the attacker would not target any persistence or invest any effort to persist within targeted systems.*
#3 – Evasion	*[T0856 – Spoof Reporting Message]* *Adversaries may spoof reporting messages in control system environments for evasion and to impair process control. The attacker may inject reporting messages / logs demonstrating consistent and correct configurations to hide execution of their own program.*
#4 – Discovery	*[T0840 – Network Connection Enumeration]* *Adversaries may perform network connection enumeration to discover information about device communication patterns. The attacker may identify recurrent communications to remote road infrastructure, allowing them to identify side systems directly interacting with such targets.*
#5 – Lateral Movement	*[T0866 – Exploitation of Remote Services]* *Adversaries may exploit a software vulnerability to take advantage of a programming error in a program, service, or within the operating system software or kernel itself to enable*

	remote service abuse. After a vulnerability scan as an insider, the attacker may take control of a side system and move towards its final target (traffic light management).
#6 – Command & Control	*[T0885 – Commonly Used Port]* *Adversaries may communicate over a commonly used port to bypass firewalls or network detection systems and to blend in with normal network activity, to avoid more detailed inspection. The attacker may exploit a vulnerable service kept open on the targeted system.*
#7 – Privilege Escalation	*[T0890 – Exploitation for Privilege Escalation]* *Adversaries may exploit software vulnerabilities to elevate privileges. The attacker may become root after a vulnerability exploitation.*
#8 – Inhibit Response Function	*[T0878 – Alarm suppression]* *Adversaries may target protection function alarms to prevent them from notifying operators of critical conditions. The attacker would disable the system's capability to monitor and report unexpected modifications.*
#9 – Impact	*[T0831 – Manipulation of Control]* *Adversaries may manipulate physical process controls within the industrial environment. Methods of manipulating control can include changes to set point values, tags, or other parameters.* ***At this final stage, the attacker may alter traffic light control without raising any alarm in the Traffic Management System.***

MITRE framework(s) support security operation activities by offering tactics as categories and techniques and procedures as guiding information. This serves as a standard and globally accessible knowledge base of adversarial methods based on real-world observations.

The following is a summarized list of elements and activities MITRE ATT&CK framework can leverage within SOC operation:

- **Threat intelligence integration** - Use the framework to map known threat actors and their techniques to your environment. This allows you to prioritize defenses against the most relevant threats;
- **Gap analysis and coverage improvement** - Assess your current detection and response capabilities against the ATT&CK matrix. Identify gaps in your security controls and develop new use cases to address uncovered techniques;
- **Enhanced detection rules** - Develop and refine detection rules based on specific ATT&CK techniques. This approach ensures your SOC is focusing on detecting real-world attack methods;
- **Incident response enhancement** - Align your incident response playbooks with ATT&CK tactics and techniques. This improves your team's ability to respond effectively to various attack scenarios;
- **Continuous improvement** - Regularly update your SOC processes, detection rules, and response procedures based on new additions to the ATT&CK framework. This ensures your defenses evolve with the threat landscape;
- **Team training and skill development** - Use the framework to train your SOC team on adversarial behaviors, improving their threat hunting and incident analysis skills;
- **Risk prioritization** - Leverage the ATT&CK matrix to identify and prioritize the most critical security gaps, allowing for more efficient resource allocation;
- **Collaborative defense** - Share insights and findings mapped to ATT&CK techniques with the broader security community, fostering collaboration and collective defense;
- **Metrics and reporting** - Use the framework to create meaningful metrics for SOC performance, demonstrating coverage and improvements over time.

As a rule of thumb, as tactics evolve and attackers make progress against targeted systems (from left to right on the IT and OT matrixes), the complexity and costs related to detection, incident containment and eradication also increase rapidly. It follows from this principle that a Security Operation Center has to provide the capabilities to detect and react to diverse types of events and attempts, ideally as early in the attack chain as possible.

3.3 Approaching C-ITS with the MITRE ATT&CK framework

As introduced in 2.5 C-ITS – Asset grouping, C-ITS infrastructure can be segmented into different categories of assets (IT or OT) and types (Information, Software, or Hardware). On *Tab. 14*, the primary risks for each category are presented as examples, along with their relevant MITRE ATT&CK tactics and techniques.

***Tab. 14** High-level threat mapping using MITRE ATT&CK framework*

Assets	Threats	ATT&CK Tactic	Techniques
IT Assets: Information (Data at Rest or in Transit)	**Data Breaches and Theft**: C-ITS systems collect vast amounts of data, including personal, vehicle, and infrastructure-related information. Attackers could target this information for theft, leading to privacy breaches and identity theft.	*Exfiltration*	*Exfiltration Over Alternative Protocol*
	Data Manipulation: Attacks involving the alteration of traffic data (e.g., vehicle locations, traffic signals) can cause widespread disruption	*Impact*	*Data Manipulation*
	Eavesdropping/Interception: Weak encryption or unsecured communication channels between C-ITS components (V2V, V2I) make systems vulnerable to eavesdropping	*Collection*	*Network Sniffing*
IT Assets: Software (Applications, Middleware, Firmware)	**Software Exploitation**: Vulnerabilities in C-ITS software, especially legacy or unpatched systems, can be exploited to gain unauthorized access to critical functions, such as vehicle control or traffic management	*Initial Access*	*Exploitation of Vulnerability*
	Malware Insertion: Software components can be targeted by malware, which can disrupt system functions, spy on communications, or facilitate data exfiltration	*Execution*	*Malicious Code*
	Supply Chain Compromise: Attackers may introduce malicious software components or backdoors during the supply chain process, which could later be activated within C-ITS systems	*Initial Access*	*Supply Chain Compromise*
OT Assets: Hardware (Roadside Units, Traffic Lights, Sensors	**Physical Damage via Cyber-Physical Attacks**: Adversaries may exploit vulnerabilities in RSUs or connected vehicles to cause physical harm, such as manipulating traffic lights to create accidents	*Impact*	*Manipulation of Control*
	Denial of Service (DoS): Disruption of OT assets such as traffic lights, sensors, or communication infrastructure through DDoS attacks can paralyze entire transportation networks	*Denial of Service*	*Network DoS*
	Unauthorized Command Execution: Attackers may intercept and manipulate commands between vehicles and infrastructure, potentially gaining control over critical systems	*Command and Control*	*Command and Scripting Interpreter*
OT Assets: Communication Channels	**Man-in-the-Middle (MitM) Attacks**: Attackers could intercept and modify communications between C-ITS components, altering sensor data or command transmissions	*Credential Access*	*MitM Attack*
	Jamming or Signal Interference: C-ITS heavily relies on wireless communications. Attackers could use jamming techniques to interfere with these communications, leading to a failure in the exchange of vital traffic information	*Impact*	*Wireless Signal Jamming*
	Replay Attacks: In this scenario, previously captured valid communication signals are replayed, deceiving the system and causing it to act on outdated or malicious instructions	*Credential Access*	*Replay Attack*

To minimize these risks and strengthen the operation of C-ITS, a SOC would be the key entity in charge of continuously monitoring and having a clear visibility of real-time risks, detecting deviating and/or unexpected events and behavior, and reacting accordingly to reduce consequences for stakeholders.

The next section carries out an investigation of SOCs, their key components and primitives, and major considerations to have in mind when elaborating a pragmatic roadmap towards an efficient implementation of a SOC for C-ITS.

4 Security Operation Center overview

Previous sections of this report illustrated different risks and threats that could affect C-ITS availability, integrity, and confidentiality, potentially leading to safety and operational issues on Swiss roads. This section will now illustrate how to monitor and react if an intrusion is detected in a C-ITS environment. These actions will be performed by the SOC, which will be described in detail in this section.

The SOC's main objectives are monitoring, detecting, and responding to cybersecurity incidents within the C-ITS ecosystem. By leveraging advanced technologies and well-defined processes, the SOC aims to protect critical assets and maintain the integrity of the transport infrastructure. To support these objectives, key components of the SOC (its pillars) include technologies, human factors, and processes. The NIST Cybersecurity Framework 2.0 [23] will be introduced as a guiding nomenclature. This framework helps in categorizing and utilizing a well-established nomenclature and vocabulary within cybersecurity systems. By understanding how a SOC works, stakeholders can acknowledge its critical role in safeguarding the C-ITS and, by extension, the broader road infrastructure in Switzerland. This overview sets the stage for a detailed exploration of each core function and the methodologies employed to achieve a secure and resilient transport system.

4.1 SOC organization

A SOC can be seen as a department within an enterprise. It is composed of different teams tasked with different functions whose global aim is to monitor and respond to any potential security event. The various teams, or functions, of the SOC must communicate with each other. As mentioned in section 3.

Approaching C-ITS security concerns the earlier a potential threat is identified, the easier it will be to respond to it and the less damage it will cause (shift left principle). Therefore, the first team to mention is the monitoring team, which is responsible for detecting any potential threats in the system. Next is the task force, the team that is responsible for investigating and containing security incidents. This team is also responsible for mitigating further damage to reduce their impact on business or operations. Finally, there is the recovery team, which is responsible for potentially restoring the system and conducting lessons learned and potential post-mortem investigations to reduce the likelihood of similar incidents in the future. *Fig. 23* illustrates the nominal lifecycle SOC organizations are continuously running through to handle security events and incidents.

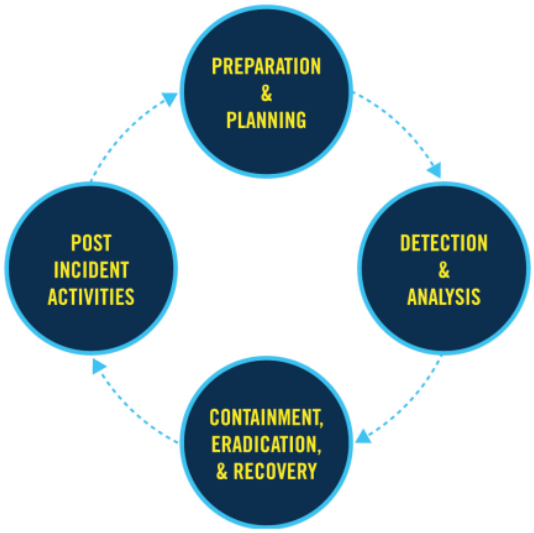


Fig. 23 *SOC Organization nominal lifecycle [65].*

4.1.1 NIST Cyber Security Framework 2.0 as a nomenclature

The NIST Cybersecurity Framework (NIST CSF) is a well-established framework in the cybersecurity environment for both IT and OT domains. The research team chose to use this framework as a nomenclature reference to ease the understanding of the different SOC functions. This framework will therefore serve as the foundation to whose core functions the SOC's activities will be mapped (see *Tab. 15*).

Tab. 15 *NIST Cyber Security Framework 2.0 – Core functions*

Core functions	Descriptions
GV – GOVERN	*The organization's cybersecurity risk management strategy, expectations, and policies are established, communicated, and monitored*
ID – IDENTIFY	*The organization's current cybersecurity risks are understood*
PR – PROTECT	*Safeguards to manage the organization's cybersecurity risks are used*
DE – DETECT	*Possible cybersecurity attacks and compromises are found and analyzed*
RS – RESPOND	*Actions regarding a detected cybersecurity incident are taken*
RC – RECOVER	*Assets and operations affected by a cybersecurity incident are restored*

4.1.2 SOC functions

The SOC is a critical component in the cybersecurity framework of any organization, particularly within the context of C-ITS. The primary objectives of the SOC are to ensure the security, integrity, and availability of the C-ITS infrastructure by proactively monitoring, detecting, responding to, and recovering from cybersecurity incidents.

The GOVERN function plays a foundational and proactive role in the SOC, providing strategic direction and influencing all activities and core functions at a higher level. It provides the necessary framework for all other functions to operate cohesively, by setting and communicating the organization's policies, managing risk and overseeing security controls.

- **GOVERN**: This overarching function focuses on proactive measures. It establishes policies, procedures, and governance structures to support effective SOC operations. It oversees strategic planning, coordinates cybersecurity efforts across all core functions, and ensures that security practices align with business objectives and regulatory requirements. Through continuous monitoring and oversight, GOVERN enables the SOC to adapt to evolving risks by adjusting its cybersecurity strategy.

The primary functions of the SOC are closely aligned with the core functions of the NIST Cybersecurity Framework: IDENTIFY, DETECT and RESPOND.

- **IDENTIFY**: This function involves understanding the business context, resources, and cybersecurity risks to systems, assets, data, and capabilities. It helps in developing an organizational understanding to manage cybersecurity risk;
- **DETECT**: This function defines the appropriate activities to identify the occurrence of a cybersecurity event in a timely manner. Continuous monitoring and detection processes are crucial here;
- **RESPOND**: This function includes the activities perform in response to a detected cybersecurity incident. It supports the ability to contain the impact of a potential cybersecurity incident.

The SOC also engages to a lesser extent with the secondary core functions PROTECT and RECOVER.

- **PROTECT**: This function outlines appropriate safeguards to ensure the delivery of critical infrastructure services. It supports the ability to limit or contain the impact of a potential cybersecurity event;

- **RECOVER**: This function identifies appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. It supports a timely reestablishment of normal operations and reduces the impact of a cybersecurity incident.

Each core function is supported by specific technologies, processes, and roles which will be detailed in subsequent chapters.

4.1.3 SOC objectives

The major SOC objectives are described below. The list of objectives is voluntarily defined at a high level, with the understanding that multiple sub objectives contribute to fulfill the high-level objectives (e.g., asset management is a prerequisite to most higher-level objectives).

- **Log collection**: The SOC collects and correlates log data from various sources (traffic systems, connected devices, computers, network infrastructure). This data is essential for monitoring activities, threat detection, forensic investigations and compliance;
- **Continuous monitoring**: The SOC is responsible for the continuous surveillance of the C-ITS environment to identify potential security threats and vulnerabilities. This involves real-time monitoring of network traffic, system logs, and other relevant data sources;
- **Incident detection**: The SOC monitors assets to detect signs of malicious activity, promptly identifying potential threats;
- **Incident response**: In the event of detected security incidents, the SOC promptly implements measures to mitigate risks, minimize impact and restore normal operations;
- **Alert management**: Security incidents are filtered based on their severity and prioritized, allowing critical threats to be dealt with first. This is an essential activity considering the high volume of alerts, helping to focus on critical risks;
- **Root cause investigation**: For severe incidents, a detailed investigation is carried out to determine when, why and how an incident occurred. This analysis helps to identify the root cause and improve long-term security, as well as for forensic purposes;
- **Threat intelligence**: The SOC gathers and analyzes threat intelligence to stay ahead of potential cyber threats. This involves understanding the latest attack vectors, threat actors, and emerging vulnerabilities that could impact the C-ITS infrastructure;
- **Continuous improvement**: The SOC is committed to continuous improvement by regularly reviewing and updating its processes, technologies, and strategies. This includes conducting post-incident reviews and lessons learned sessions to enhance future responses.

By fulfilling these functions and objectives, the SOC ensures a robust defense against cybersecurity threats, thereby safeguarding the C-ITS infrastructure and contributing to the overall safety and resilience of road infrastructure in Switzerland.

Tab. 16 summarizes the mapping of SOC objectives to the relevant NIST Cybersecurity Framework core functions.

***Tab. 16** Mapping between core functions and objectives*

Core functions	SOC Objectives
GOVERN	*Continuous Improvement*
IDENTIFY	*Threat Intelligence*
DETECT	*Log Collection* *Continuous Monitoring* *Incident Detection* *Alert Management* *Threat Intelligence*
RESPOND	*Incident Response* *Root Cause Investigation*

Note: Continuous Improvement is primarily associated with the GOVERN function due to the proactive nature and strategic importance of the objective, which aligns well with the core function. However, this key objective extends to all the core functions of the NIST CSF as it aims is to improve all aspects of cybersecurity operations, making it a general principle.

4.1.4 SOC pillars

In addition to the previously-described SOC NIST objectives, the SOC would have four major operational objectives:

- Ensure compliance with applicable cybersecurity rules and regulations for secure mobility and transport systems;
- Continuously monitor C-ITS systems and infrastructure to maintain a reasonably high level of security;
- Support incident detection, analysis and response using the monitored data to trigger appropriate mitigation measures;
- Collaborate with internal and external stakeholders to ensure comprehensive security.

To fulfill these objectives, a risk-oriented approach must be implemented that identifies the key tools and resources necessary for effective SOC operations. These tools and resources can be categorized into three foundational components of the SOC, known as pillars: Technologies, Human Factors, and Processes. *Fig. 24* represents the SOC Framework, highlighting and describing these three pillars.

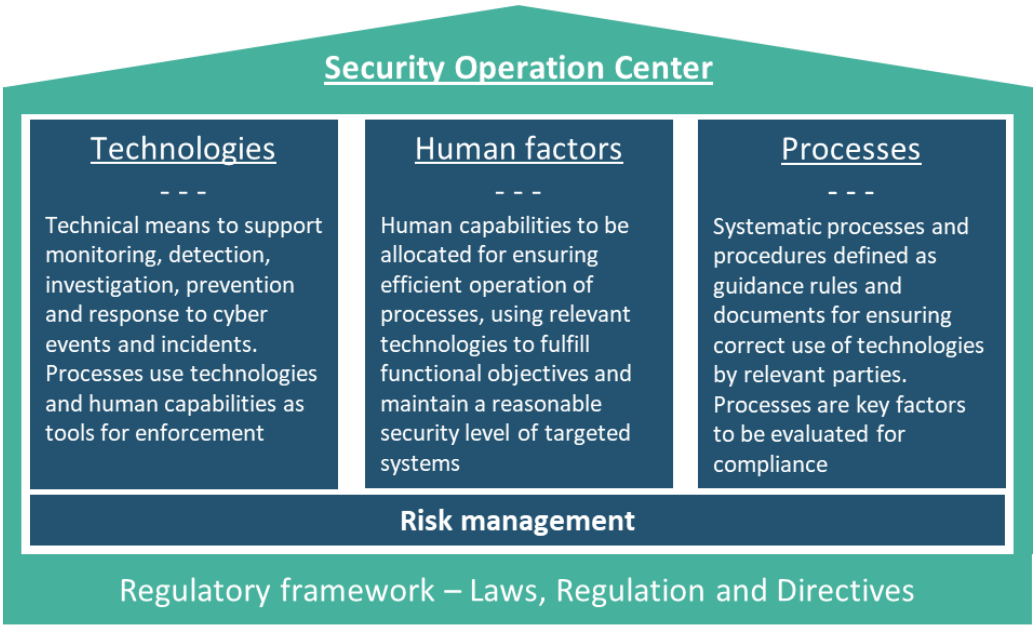


***Fig. 24** Security Operation Center Framework.*

As explained in the previous sections of the chapter, the NIST CSF defines essential functions for managing cybersecurity risk that can be implemented within the SOC. Subsections 4.3 to 4.8 will examine how the Technologies and Processes pillars integrate with the core functions of the NIST CSF. The Human Factors pillar, which encompasses the various roles within the SOC, will be described at the end of the chapter. Each role will be mapped to one or several core functions in a summary table, providing a comprehensive overview of each role's contribution to SOC operations.

4.2 SOC references and guidance

The implementation of a SOC requires alignment with recognized frameworks and guidelines to ensure standardized and effective operations and processes. These references serve as essential tools for structuring SOC processes, focusing on best cybersecurity practices.

Key SOC frameworks serve multiple purposes in design and operations:

The **MITRE ATT&CK framework** [44] is a globally recognized resource providing a comprehensive knowledge base of real-world adversarial behavior, detailing their TTPs throughout the attack lifecycle. The framework evolves continually as new malicious activities are uncovered, making it a reliable reference for defending against current threats. Using this framework in a SOC has key benefits, including improving threat detection, supporting threat hunting activities, improving incident response and allowing gap identification between SOC defense systems and the ATT&CK matrix.

The **NIST Cybersecurity Framework** [23] is a structured framework providing comprehensive guidance on improving an organization's cybersecurity capabilities. Through its five core functions (Identify, Protect, Detect, Respond, and Recover), it covers all aspects of cybersecurity management and provides good guidance for SOCs in establishing processes for handling cybersecurity incidents. Furthermore, it offers a standardized approach, with a systematic methodology for managing cybersecurity risks, ensuring consistency across security operations.

In addition to MITRE ATT&CK and NIST CSF, below is a non-exhaustive list of international standards providing essential principles for managing SOC activities:

- **ISO/IEC 27001:2022** [36] serves as the baseline for Information Security Management System, offering governance and risk management principles for SOCs;
- **ISO/IEC 27035:2023** [37] focuses on incident management processes, an essential activity for SOC to detect, respond to and recover from security incidents;
- **NIST SP 800-61** [23] offers guidance for computer security incident handling, helping SOC establish standardized processes for incident response;
- **FIRST CSIRT** [66] provides guidelines for Computer Security Incident Response Teams (CSIRT), helping SOC in organizing and optimizing incident response capabilities;
- **ISA/IEC 62443-2-1** [25]: Handles security concerns specific to OT/ICS environments, relevant for SOCs managing industrial environments or critical infrastructure.

These frameworks and standards, summarized in *Tab. 17*, provide clear guidance for setting up and strengthening SOC capabilities, helping to establish strong processes. While this section focuses on frameworks that form the foundation of SOC operations, section 4.11 will introduce compliance requirements and regulations specific to SOCs that support C-ITS as critical infrastructure.

***Tab. 17** Summary of SOC references and guidance*

Framework/Standard	Description
MITRE ATT&CK [44]	*Knowledge base of adversarial tactics, techniques and procedures*
NIST CSF [23]	*Framework of cybersecurity standards and best practices*
ISO/IEC 27001:2022 [36]	*Information Security Management System (ISMS) standard*
ISO/IEC 27035:2023 [37]	*Standard for incident management processes*
NIST SP 800-61 [23]	*Computer security incident handling guide with recommendations*
FIRST CSIRT [66]	*Guidelines for organizing incident response teams*
ISA/IEC 62443-2-1 [25]	*Security standards for OT/ICS environments*

4.3 Core function - GOVERN

The GOVERN function involves establishing cybersecurity policies, managing risks, and overseeing security controls to ensure that security practices align with organizational objectives. This category is process-driven and supported by tools that help with governance, risk, and compliance (GRC). High-level functions to be provided are represented in *Tab. 18*.

***Tab. 18** SOC for C-ITS – GOVERN – Objectives*

Objectives	Descriptions
Establish Cybersecurity Governance	*Define roles, responsibilities, and accountability within the SOC and C-ITS infrastructure to ensure oversight of cybersecurity operations*
Regulatory Compliance	*Ensure that C-ITS operations meet local, national, and international regulatory requirements (e.g., ITS standards) and industry best practices*
Support Risk Management	*Provide cybersecurity insights to the organization's risk manager, to guide risk assessment and ensure alignment with the organization's governance strategy and operational priorities in the C-ITS environment*

4.3.1 Core function - GOVERN – Technologies

Mostly concerned with GRC tools, the following points highlight how these solutions streamline compliance processes and support alignment with industry standards and business goals.

- GRC tools help organizations manage policies, risk assessments, and compliance with standards (like ISO 27001, NIST, GDPR). These solutions ensure that security practices align with business objectives and regulatory requirements;
- Examples: RSA Archer, ServiceNow GRC, OneTrust, Chief Information Security Officer (CISO) Assistant, VANTA.

4.3.2 Core function - GOVERN – Processes

Processes under the GOVERN function focus on establishing and maintaining governance structures, policies, and compliance across C-ITS infrastructure. These processes ensure alignment with industry regulations and organizational objectives.

Policy development and enforcement:

- Develop cybersecurity policies covering both IT and OT, including C-ITS-specific standards (e.g., vehicle-to-infrastructure communication protocols, roadside unit security, etc.);
- Enforce policies through regular training and reviews to ensure compliance across all stakeholders involved in C-ITS management. New or modified standards might also ask for modifications in policies that are already in place.

Regulatory and compliance management:

- Track and comply with relevant transportation and cybersecurity regulations/standards (e.g., EU ITS Directive, Swiss minimum ICT requirements ISO 27001 [36] for information security management, ISA/IEC 62443-2-1 [25] for critical environment);
- Implement continuous compliance checks to ensure adherence to local, national, and international regulatory frameworks.

Risk alignment process:

- Share SOC-generated cybersecurity and threat intelligence insights with the organization's risk manager to enhance its understanding of the current landscape;
- Provide high-level input for risk assessments, summarizing information on cyber threats, vulnerabilities and their potential impact on C-ITS infrastructure;
- Align SOC activities with the organization's governance strategy and operational priorities in the C-ITS environment.

4.4 Core function - IDENTIFY

The IDENTIFY function focuses on understanding and managing cybersecurity risks to systems, assets, data, and capabilities. This category includes technologies that provide visibility into the organization's assets and identify vulnerabilities or potential threats. The key objectives are represented in *Tab. 19*.

***Tab. 19** SOC for C-ITS – IDENTIFY – Objectives*

Objectives	Descriptions
Asset Discovery and Classification	*Maintain an up-to-date (if possible automated) inventory of all IT and OT assets, including roadside units, traffic control systems, communication nodes, and data repositories. Classify assets based on their criticality and keep this inventory and classification updated.*
Vulnerability Identification	*Continuously scan and assess vulnerabilities in both IT and OT systems, ensuring critical systems like traffic signals or vehicle communication modules are protected from emerging threats.*
Threat Intelligence Integration	*Gather and integrate threat intelligence specific to C-ITS (e.g., threats to V2X communications, sensor spoofing, or malware targeting vehicle systems).*
Support Risk Assessment	*Provide asset and vulnerability data to the organization's risk manager to support comprehensive risk assessment and inform risk management strategies.*

4.4.1 Core function - IDENTIFY – Technologies

Asset discovery/management:

In engineering and manufacturing, a Bill of Materials (BOM) serves as a comprehensive inventory of components required to build a physical or virtual product. It includes details such as part numbers, quantities, descriptions, versions, and suppliers. While traditionally associated with physical manufacturing, the concept of BOM extends to both hardware and software domains. Both Hardware and Software BOM play pivotal roles in the operation of the SOC.

The **Hardware Bill of Materials (HBOM)** serves as a foundational inventory for constructing physical systems. It meticulously catalogs the components running in the infrastructure, including their specifications, quantities, and sourcing details. While traditionally associated with manufacturing, the concept of BOM extends beyond the factory floor to critical domains such as security infrastructure.

The **HBOM** encompasses various elements:

- **Servers:** The backbone of SOC operations, servers house critical security applications, databases, and monitoring tools;
- **Network devices:** Routers, switches, and firewalls form the communication fabric, ensuring data flows securely;
- **Storage systems:** Robust storage solutions store logs, incident data, and backups;
- **Physical security equipment:** Cameras, access control systems, and alarms protect the SOC premises;
- **Hardware to run the server:** All the hardware used to manage the Security Operation Center server such as uninterruptible power supplies (UPS), cooling system, and the switchgear cabinet.

Therefore, the HBOM is crucial for SOC operations for several reasons:

- **Inventory management:** Maintaining an accurate inventory of hardware assets is paramount. The Hardware BOM enables efficient tracking, maintenance, and scalability. SOC teams can swiftly identify available resources and plan for expansion or replacement;
- **Security assurance:** Documenting hardware components allows the SOC to assess their security posture. Vulnerabilities in hardware (e.g., outdated firmware) directly

impact overall security. Regular audits based on the BOM ensure timely updates and patches;
- **Incident response:** During security incidents, knowledge of the hardware components facilitates targeted responses. SOC analysts can swiftly identify affected systems, isolate them, and mitigate threats;
- **Ownership management:** Documenting a person responsible for every asset to know who takes the decision specific to a device in emergency situations such as applying a patch.
- **Supply chain:** The origin of all elements in the BOM must be traceable. An up-to-date supply chain is important and necessities accurate supply chain management.

The **Software Bill of Materials (SBOM)** is a critical artifact in modern software development and security. It provides a detailed inventory of software components used in an application or system. Software version might change very quickly and often, therefore an automatic SBOM should be the goal. Within the context of a SOC for C-ITS, the SBOM serves as a valuable resource for keeping track of all ecosystem components, such as C-ITS-specific software, security tools and C-ITS monitoring tools.

Within a SOC, the SBOM encompasses the following:
- **Security tools:** Intrusion detection systems, SIEM (Security Information and Event Management) software, and vulnerability scanners;
- **Monitoring Software:** Tools for real-time monitoring, log analysis, and threat detection;
- **Third-Party applications:** Any software integrated into the SOC ecosystem, including opensource libraries;
- **Build tools:** All the tools used to build and operate a solution**.**

SBOMs play a significant role in the following SOC operations:
- **Vulnerability management:** The SBOM aids in identifying vulnerabilities within the software stack. SOC teams can track security patches, updates, and known vulnerabilities associated with specific software components;
- **Supply chain risk:** Understanding software dependencies is crucial. Vulnerabilities in third-party components can significantly impact overall security. The SBOM helps SOC teams assess and mitigate supply chain risks;
- **Incident investigation:** When analyzing security incidents, knowledge of the software components is essential. SOC analysts can trace attack vectors, understand the impact of vulnerabilities, and tailor responses accordingly.

Examples: SolarWinds Network Configuration Manager, Spiceworks Inventory, ManageEngine AssetExplorer, Qualys Asset Inventory

Vulnerability management:

A Vulnerability Scanning and Management tool is a software solution that provides insights into cybersecurity vulnerabilities in an organization's infrastructure. These tools are used to prepare for, prevent, and identify cybersecurity threats that could exploit weaknesses in valuable data systems. In addition to identifying vulnerabilities, these tools can be described as offering evidence-based knowledge about adversaries, including their motives, intents, capabilities, and methods of operation.

Vulnerability scanning and management tools function as proactive extensions to incident response efforts by leveraging outputs from existing cybersecurity monitoring tools. They reduce exposure to internal and external threats, understand the organization’s attack surface, and minimize the time from infection to detection. These tools are also good for enumerating the time required for containment and preventing the spread of threats, thereby estimating the number of breaches and infections that could occur.

Some features of these tools include:
- **Automated vulnerability detection**: Continuously scans for vulnerabilities across various systems, providing up-to-date data that is critical for maintaining network security;

- **Integration with SOC operations**: Vulnerability scanning results are important inputs for SOC activities, contributing to incident analysis and threat hunting;
- **Patch compliance monitoring**: Tracks and reports the coverage and installation penetration of (critical) patches in the infrastructure. Coverage targets, such as 90% patched within 7 days for routine patches, must be prepared and constantly monitored;
- **Scalability and efficiency**: Efficiently handles large datasets, automating scan scheduling and reporting, and reducing manual tasks. Ensures scalability by supporting distributed scanning across networks;
- **Risk and compliance assessment**: Helps in calculating security risk and compliance status by evaluating the patch level, installed software, and security-relevant configurations of constituent assets, and all this in consideration of the BOM.

Incorporating vulnerability scanning into a SOC enables organizations to keep a detailed inventory of network maps and system diagrams and track IT changes. The combination of these tools and practices allows for a defense strategy that not only reacts to threats but also proactively manages potential vulnerabilities before they can be exploited.

Examples: Tenable Nessus, Rapid7 Nexpose, Qualys VM

Threat intelligence and risk assessment support

Threat intelligence is used to extend the analysis of potential threats to the system under consideration. This allows for the monitoring of different sources of information to understand the threats other stakeholders might face. These tools are often linked to existing vulnerability databases (e.g., ASRG, BOSCH CS company).

4.4.2 Core function - IDENTIFY – Processes

Processes in the IDENTIFY function involve the discovery, classification, and assessment of all assets and vulnerabilities in the C-ITS infrastructure. These processes provide visibility into the security landscape and help prioritize risks.

Asset inventory and classification:

- Continuously maintain an inventory of all IT and OT assets within the C-ITS infrastructure, such as roadside units, communication systems, traffic control centers, and sensors;
- Wherever possible, automated updating and collection of the inventory must be considered. The processes for this automation must be well documented. Description of inventory gathering infrastructure should be documented in “interface contracts”;
- Categorize assets based on criticality, function, and security requirements to help prioritize security efforts.

Vulnerability management and assessment:

- Regularly conduct vulnerability scans and assessments to identify weaknesses in both IT and OT systems (e.g., traffic signals, RSU, PLC, etc.);
- Implement vulnerability management processes to track, prioritize, and remediate vulnerabilities based on their risk to C-ITS operations.

Threat intelligence and risk assessment support:

- Establish processes for gathering threat intelligence, focusing on threats relevant to C-ITS infrastructure (e.g., vehicle hijacking, data spoofing in V2X networks);
- Share asset inventory, vulnerability data and threat intelligence with the organization’s risk manager to provide a better view of the C-ITS infrastructure’s security posture.

4.5 Core function - DETECT

The DETECT function revolves around implementing solutions that enable the timely detection of cybersecurity events, potential threats, and anomalous behavior. This category includes monitoring tools that allow SOC teams to detect and respond to threats in real-time. The key objectives are represented in *Tab. 20*.

***Tab. 20** SOC for C-ITS – DETECT – Objectives*

Objectives	Descriptions
Continuous Security Monitoring	*Establish 24/7 monitoring of all C-ITS systems (IT and OT) using SIEM, Extended Detection and Response (XDR), or other monitoring tools, ensuring threats are detected across both traffic control systems and connected vehicles.*
Anomaly Detection and Alerting	*Develop detection rules and use cases to identify abnormal behavior in C-ITS networks, such as unexpected communication patterns or suspicious changes in traffic control systems.*
Network Traffic Analysis (NTA)	*Monitor network traffic, particularly in vehicle-to-infrastructure communications, to detect malicious traffic, data exfiltration attempts, or spoofing.*
Threat Hunting and Proactive Detection	*Conduct proactive threat hunting exercises focused on identifying undetected threats in the C-ITS infrastructure.*
Alert Management	*Filter and prioritize incident handling based on the severity of the alerts.*

4.5.1 Core function - DETECT – Technologies

Threat Intelligence Platforms (TIPs):

The primary role of Threat Intelligence Platforms is to provide real-time threat data and Indicators of Compromise (IOCs), enable anomaly detection and continuously monitor the threat landscape. While TIPs are primarily associated with the DETECT core function, they also support aspects of other core functions such as IDENTIFY, PROTECT, RESPOND and RECOVER.

A TIP is a software solution designed to aggregate, correlate and analyze threat data from multiple sources in real-time, providing capabilities to understand, anticipate and respond to cyber threats. TIPs can also be described as systems that deliver evidence-based knowledge about general adversary motives, TTPs as well as their capabilities and operational environments. TIPs integrate and correlate high volumes of adversary-related data, including IOCs. This enables organizations to better manage threats by answering critical questions, such as whether a specific adversary has been encountered before, what activities were exploited, and which tactics or techniques have been reported by others.

Leveraging a TIP within a SOC is particularly beneficial as it supports correlation, linkage, tracking, and knowledge management of cyber threats beyond just incident-focused tracking. TIPs allow SOCs to maintain a history of campaigns, track adversary activities, and analyze trends. Furthermore, they can integrate with other high-scale data processing environments like SIEM systems or big data platforms. This integration supports data enrichment, workflow optimization, and enables more efficient threat detection and response.

When selecting a TIP, SOCs should consider several factors:

- **Workflow and organization:** A TIP should facilitate collaboration, repeatability, and structured knowledge capture, particularly in handling Cyber Threat Intelligence (CTI) artifacts. It should support tracking adversary campaigns and indicator linkages with case management features;
- **Data integration:** The TIP must be capable of ingesting, persisting, correlating, and interfacing with various CTI tools and feeds, both open-source and commercial. It should also support both real-time and batch data processing, with integration into the SOC's existing analytic architectures;
- **Scalability:** Given the large volumes of IOCs that a SOC might encounter, a TIP should efficiently handle data at scale, allowing quick correlations, queries and analysis;
- **Confidentiality and source tagging:** A TIP should support tagging and metadata management for artifacts, enabling data pedigree tracking, and handling caveats. It should also ensure compliance with data-sharing protocols like the Traffic Light Protocol (TLP);
- **User pivoting and auditing:** The platform should enable analysts to pivot through adversary activities, maintain a history of associations, and support change management to track and revert changes as necessary.

By implementing a TIP, organizations can reduce their exposure to threats, improve their understanding of attack surfaces, and better manage incidents from detection through containment. Identifying the attacker's digital footprint and analyzing adversary behaviors provide the strategic and tactical information necessary for effective cybersecurity defense.

Examples: CrowdStrike Falcon Intelligence, Anomali, ThreatConnect, IBM X-Force Threat Intelligence, Recorded Future

Security Information and Event Management (SIEM):

SIEM is a security solution that helps organizations detect, analyze, and respond to security threats before they can harm business operations. It combines security information management (SIM) and security event management (SEM) into one system. SIEM collects event log data from various sources, identifies unusual activity in real-time, and takes appropriate action. Key outputs from SIEM are represented in *Fig. 25*.

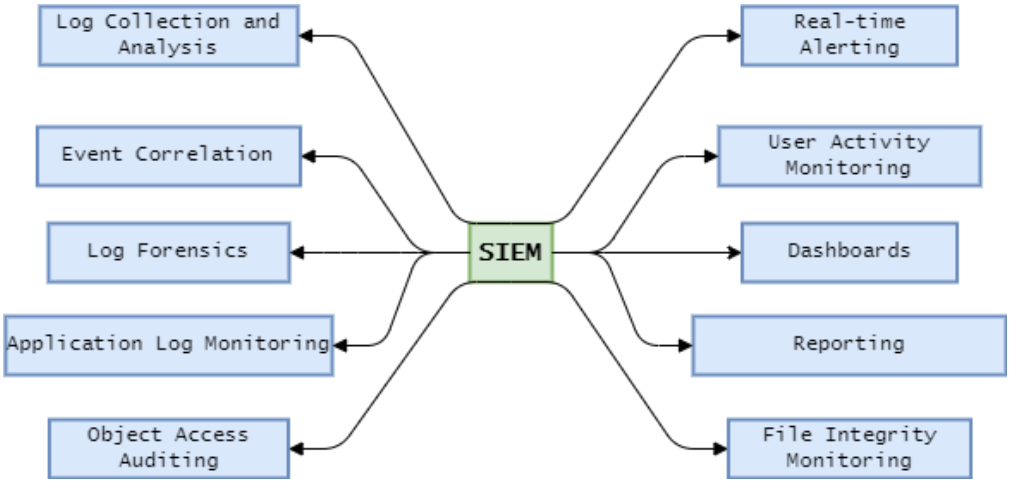


***Fig. 25** SIEM outputs.*

SIEM gives organizations visibility into their network activities, allowing them to respond quickly to cyberattacks and meet compliance requirements. Over the past decade, SIEM technology has evolved with artificial intelligence to make threat detection and incident response smarter, faster and automatable.

Setting up an on-premises SIEM is usually straightforward and can be done in a day or two, while cloud-based SIEMs can be deployed in minutes. Within a few weeks, initial data feeds can be connected and tuned, providing quick gains. However, fully integrating the system with the right data, tuning it, creating content, training users, and embedding it into operations can take several months. Getting reliable, sustained log feeds from data owners can also be a politically challenging process.

SIEM platforms are essential tools in modern SOCs, helping organizations manage and analyze large amounts of security data in real-time. They aggregate, filter, store, and correlate data from sources like firewalls, endpoint devices, and intrusion detection systems to detect both internal and external security threats.

The main function of SIEM is to provide a comprehensive view of security events by collecting logs from various systems and analyzing them for patterns that indicate potential threats. By combining real-time monitoring with historical analysis, SIEMs enable immediate incident detection and post-event forensic investigations. They act as a force multiplier, allowing a small team of skilled analysts to manage vast amounts of security data effectively.

Key features and use cases of SIEM include:

- **Advanced persistent threat (APT) detection**: Detecting advanced persistent threats by piecing together indicators like lateral movement, remote access, and data exfiltration from multiple sources;
- **Incident analysis and forensics**: Storing large amounts of historical log data for detailed forensic investigations and retrospective analysis;

- **Workflow and escalation**: Tracking incidents from detection to resolution, integrating with ticketing systems to ensure proper handling;
- **Threat hunting and trend analysis**: Analyzing long-term trends and hunting for threats by searching for patterns in collected data over time;
- **Compliance monitoring**: Providing pre-built reports to help organizations comply with regulations like PCI [67], SOX [68], and FISMA [69].

One of SIEM's biggest strengths is its ability to enrich raw and unstructured log data with additional information, such as vulnerability scan results or threat intelligence feeds. This gives analysts deeper context and enables more informed decision-making. SIEM also improves SOC efficiency by automating alert prioritization and enabling correlation across different data sources. However, SIEM platforms are resource-intensive to manage and require significant time and money investments. They are typically expensive to purchase, operate, and maintain, and their complexity requires continuous content tuning, rule adaptations/updates, and log management. Dedicated teams are needed to keep the system up-to-date and effective.

Examples: Splunk, IBM QRadar, LogRhythm, ArcSight, ELK-Stack

Extended Detection and Response (xDR):

DR is the next level of security technology, building on what EDR does but covering a lot more ground. While EDR focuses on spotting and dealing with threats on devices like laptops and servers, xDR looks at the bigger picture. It keeps an eye on everything from networks and cloud environments to email systems and identity solutions.

XDR pulls together data from all sorts of security tools into one place, giving you a clear view of potential threats across your whole IT and OT setup. This helps security teams catch complex threats that might start with something like a phishing email and then spread through the network. By connecting the dots from different sources, xDR makes it easier to spot and respond to threats quickly.

While xDR and SIEM have overlap in functionalities, they are different but complementary tools for security operations. SIEM is centered on log management and analysis to detect potential threats while xDR is more focused on automated threat detection and response across multiple domains.

XDR works in the following way:

- **Data collection and correlation**: xDR gathers information from various security sources like network traffic, endpoints, cloud apps, and identity systems. By looking at all this data together, it can spot suspicious behavior that might be missed if you only look at one piece of the puzzle;
- **Automated detection and response**: Like EDR, xDR uses automation to tackle threats. But XDR can take action across different parts of your IT environment, like blocking bad network traffic, isolating compromised devices, and revoking hacked user accounts;
- **Threat visibility and investigation**: xDR gives you a deep look into threats at both the endpoint and network levels. It helps security analysts see how an attack is unfolding, making it easier to investigate and track the attack across your infrastructure.

While EDR is great for dealing with threats on specific devices, xDR's strength is in connecting data from different parts of your security setup. For example, if a threat targets a cloud service and then moves to devices, EDR might miss it. xDR, on the other hand, gives you a unified view that helps uncover these complex attacks.

Here are some benefits of xDR:

- **Enhanced detection**: By analyzing data from multiple sources, xDR can catch advanced threats that might slip past traditional security tools;
- **Faster response**: xDR platforms offer automated, coordinated responses across endpoints, networks, and other assets, helping to contain threats quickly;
- **Holistic security view**: xDR provides a single, comprehensive view of your entire security landscape, making it easier for security teams to manage incidents;
- **Reduced complexity**: Instead of juggling multiple, disconnected security tools, xDR simplifies things by bringing detection and response into one platform.

Examples: CrowdStrike Falcon xDR, Palo Alto Networks Cortex XDR, Microsoft Defender for Endpoint, McAfee MVISION XDR

Intrusion Detection Systems (IDS):

An IDS is a security software that monitors the company environment for suspicious or unusual activity and alerts the administrator if something comes up. IDS is an essential tool for IT departments in organizations to gain insights into potentially malicious activities that happen within their technological environments.

IDS serves as an essential component of a broader cybersecurity strategy, complementing other technologies such as Firewalls, Antivirus, and Message Encryption by offering deeper visibility into network and host activities. This allows for the secure and trusted transfer of information between departments and organizations.

In the context of a SOC, IDS typically generates alerts that signal potential security incidents based on predefined signatures or anomaly detection methods. These alerts are then analyzed by SOC analysts who determine whether they indicate an actual threat or a false positive. This process is crucial, as a typical SOC may collect, analyze, and store millions to billions of security events daily. IDS alerts help to filter out potentially harmful activities from the vast number of routine events logged, such as user connections to file shares or web server requests.

While IDS provides valuable detection capabilities, it has its limitations, particularly concerning the volume of false positives it can generate. This challenge has led to the evolution of Intrusion Prevention Systems (IPS), which not only detect but also actively block detected threats in real time. However, many SOCs struggle to fully implement IPS in an in-line, blocking mode due to concerns about operational disruptions or a lack of confidence in signature tuning. The next section contains a more complete description of IPS.

Over time, network intrusion detection systems (NIDS), which were a primary focus of SOC monitoring efforts in the late 1990s, have evolved. Although the standalone NIDS is becoming less common, their functionality has been integrated into more comprehensive security solutions such as Network Detection and Response (NDR) systems and next-generation firewalls. These modern solutions merge traditional IDS/IPS capabilities with advanced network security features, including NetFlow analysis, traffic metadata collection, and malware detonation.

Despite these advancements, signature-based detection methods alone are no longer sufficient to protect against the wide range of attack vectors in today's threat landscape. Client-side attacks, such as phishing, have become more prevalent, necessitating a combination of IDS with other security technologies and practices, including content analysis and behavioral detection, to ensure robust network defense.

Examples: ManageEngine Log 360, Snort, Suricata, Cisco Firepower, Zeek

Network sensors:

Network sensors are passive security devices or software that monitor, capture and analyze network traffic in real-time to detect suspicious activity and threats. They enable Network Traffic Analysis (NTA) by providing visibility into data flows, allowing the identification of anomalies and potential attacks that may not be visible through endpoint or log monitoring alone. Network sensors can function independently or as part of broader security technologies such as Intrusion Detection Systems, Network Detection and Response, and Extended Detection and Response platforms.

Example: Zeek, Wireshark (not a real-time network sensor but a packet analyzer), Suricata and Snort (which are network sensors that function as IDS/IPS)

4.5.2 Core function - DETECT – Processes

The DETECT function revolves around real-time monitoring and detecting threats across the C-ITS infrastructure. These processes ensure that potential incidents are identified before they cause harm.

Security monitoring and log management:
- Continuously collect and analyze logs from various C-ITS systems, including traffic control, communication systems, and vehicles, to detect anomalies or malicious activity;
- Implement centralized log management and correlation through SIEM solutions.

Threat detection and alerting:
- Deploy processes for real-time detection of suspicious activities within C-ITS networks, focusing on potential attacks targeting OT systems (e.g., signal spoofing, DoS attacks on traffic lights);
- Develop use cases and rules tailored to detecting specific C-ITS threats, such as anomalous vehicle behavior or unusual traffic control data.

Network Traffic Analysis (NTA):
- Establish continuous network traffic analysis processes to monitor for unusual patterns in vehicle-to-infrastructure communication, such as data exfiltration attempts or protocol violations;
- Use anomaly-based detection to spot deviations from normal network behavior in OT environments.

Alert management:
- Implement a triage process to filter and prioritize alerts based on their severity and potential impact on C-ITS operations;
- Establish a procedure to ensure rapid processing of high-priority alerts requiring immediate attention.

4.6 Core function - RESPOND

The RESPOND function focuses on acting when cybersecurity incidents are detected, from containing the threat to eradicating the attacker's foothold and conducting forensic investigations. The key objectives are represented in *Tab. 21*.

***Tab. 21** SOC for C-ITS – RESPOND – Objectives*

Objectives	Descriptions
Incident Response Planning and Playbooks	*Develop incident response playbooks specific to C-ITS infrastructure, such as playbooks for compromised vehicle-to-infrastructure communications or traffic control systems.*
Real-Time Incident Containment	*Implement procedures for isolating and containing incidents in real-time, ensuring that the SOC can respond immediately to attacks targeting critical systems (e.g., switching traffic systems to manual mode if compromised).*
Threat Mitigation and Recovery	*Ensure that mitigation strategies are in place to address specific attack vectors (e.g., disabling compromised communication nodes, rerouting traffic in case of system outages).*
Incident Communication and Stakeholder Coordination	*Establish clear communication channels between the SOC and stakeholders, including transportation authorities, law enforcement, and third-party vendors, during incident response.*
Root Cause Investigation	*Ensure that a post-incident forensic investigation is conducted for severe incidents to identify root causes and learn from incidents affecting C-ITS infrastructure.*

4.6.1 Core function - RESPOND – Technologies

Security Orchestration, Automation, and Response (SOAR):

SOAR platforms are software solutions that help security teams integrate and coordinate their tools into streamlined workflows for threat response. They focus on detecting and responding to threats at the endpoint level by providing better visibility into activities, identifying potential security incidents, and facilitating swift response and containment measures.

SOARs are typically composed of three components that work together to find and stop attacks:

- Orchestration;
- Automation;
- Incident response.

Orchestration connects both internal and external tools, including out-of-the-box and custom integrations, so everything can be accessed from one central place. This consolidation of data and processes sets the stage for automation. Automation involves programming tasks to execute on their own through playbooks, which are collections of workflows that automatically run when triggered by a rule or incident. These playbooks help automate tasks, manage alerts, and create responses to threats and incidents.

Incident management is a key function of SOAR platforms. They consolidate incidents from multiple systems, offering a unified view for managing alerts. This “single pane” approach simplifies and improves alert management. SOAR platforms also automatically gather and add information to alerts with threat intelligence, vulnerability information, and details about the entities involved, helping prioritize alerts and providing analysts with more context for decision-making.

Automated responses are another key feature. SOAR platforms can initiate predefined actions like running queries, sending files for analysis, collecting vulnerability data, disabling user accounts, or blocking network connections, which allows for faster response times. They also standardize workflows across the SOC, enabling less experienced analysts to follow procedures established by senior staff, leading to faster triage times and more consistent incident investigations.

The benefits of SOAR are clear. They boost efficiency by automating repetitive tasks, freeing up analysts to focus on more complex issues. They improve response times by automating common actions, helping to contain and resolve threats faster. They also help SOCs scale their operations without needing to hire more staff, and ensure consistency in handling incidents, which is great for training junior analysts and sticking to best practices. Plus, SOAR systems usually come with APIs that integrate with existing security tools, making it easier to automate responses across different platforms without a lot of custom coding.

However, SOAR platforms are most useful when a SOC has well-defined incident response processes. They work best when integrated with other tools like SIEM threat intelligence solutions and case management platforms, which help track and manage incidents. When starting with SOAR, it is advisable to focus on automating repetitive tasks like alert triage, so analysts can concentrate on more complex tasks like threat hunting.

Examples of SOAR platforms include Splunk SOAR, Cyware, Microsoft Sentinel, IBM QRadar SOAR, Palo Alto Networks Cortex XSOAR, Fortinet FortiSOAR, Swimlane

Incident response platforms:

These tools assist in coordinating and managing the response to cyber incidents, helping teams follow structured playbooks and ensuring the timely containment and recovery of affected systems.

Examples: Swimlane, Cybereason, Cofense Triage.

Forensic analysis tools:

These tools are used to investigate security breaches, collect digital evidence, and analyze compromised systems to understand the attack, assess the damage, and ensure proper remediation.

Examples: EnCase, Autopsy, FTK (Forensic Toolkit), Wireshark, Volatility.

4.6.2 Core function - RESPOND – Processes

Processes in the RESPOND function are designed to ensure the SOC can swiftly and effectively respond to incidents in the C-ITS infrastructure, minimizing disruption and containing threats.

Incident response planning and playbooks:
- Develop general incident response playbooks that outline standardized procedures for handling common cybersecurity threats and incidents;
- Create incident response playbooks tailored to C-ITS scenarios, such as compromised roadside units, communication spoofing between vehicles and infrastructure, or traffic system failures due to cyberattacks;
- Ensure SOC operators are trained to execute these playbooks effectively during an incident.

Incident containment and mitigation:
- Implement processes for immediate containment of incidents affecting C-ITS infrastructure, such as isolating compromised OT systems or cutting off malicious traffic to protect critical operations;
- Ensure rapid deployment of mitigation actions (e.g., switching traffic control to manual mode) to prevent cascading failures across the transportation network.

Communication and coordination:
- Establish communication protocols between the SOC, transportation authorities, and other stakeholders to coordinate response efforts during a cybersecurity incident;
- Engage in multi-agency coordination for incidents that affect public safety or require emergency responses.

Post-incident forensics:
- Define processes for conducting forensic investigations after an incident, focusing on the collection of evidence and understanding the root cause of the compromise;
- Ensure forensic processes cover both IT and OT environments, such as analyzing compromised traffic signals or communication nodes;
- Ensure feedback loop from the insights gained to update and improve the detection and respond pillars.

4.7 Core function - PROTECT

The PROTECT function focuses on implementing safeguards to protect critical assets and ensure the resilience of services against attacks. This involves technologies that help prevent unauthorized access, protect data, and harden systems against cyber threats. The key objectives are represented in *Tab. 22*.

***Tab. 22** SOC for C-ITS – PROTECT – Objectives*

Objectives	Descriptions
Identity Access Control and Privileged Access Management	*Ensure that only authorized individuals and systems can interact with critical C-ITS components (e.g., traffic control centers, communication systems). Make sure that access is secured by security roles.*
Network Security and Segmentation	*Implement network security controls and segmentation across both IT and OT systems, limiting access to sensitive components such as connected vehicle networks or traffic management systems.*
Data Encryption and Privacy Protection	*Ensure that sensitive C-ITS communications (vehicle-to-vehicle, vehicle-to-infrastructure, infrastructure-to-infrastructure) are encrypted, and that data privacy is protected in compliance with regulations.*
Endpoint and System Hardening	*Continuously harden and secure endpoints, such as roadside units, traffic control consoles, and communication nodes, against malware and unauthorized access (also physical access).*
Patch Management and Software Updates	*Implement a patch management process to ensure timely updates of all systems, including vehicle firmware, traffic management software, and communication protocols.*

4.7.1 Core function - PROTECT – Technologies

Firewall and Next-Generation Firewalls (NGFW):

Firewalls enforce network boundaries, help to segmentize the network and prevent unauthorized access to networks. NGFWs provide advanced filtering, threat intelligence integration, and application-level protection. Firewalls also generate a lot of log information that must flow into SIEM systems to detect and predict anomalies in the network

Examples: Palo Alto Networks, Cisco ASA, Fortinet.

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS):

An IPS is a proactive security tool designed to monitor a network for suspicious activities and take real-time actions to prevent or block malicious activity. Unlike its counterpart, the IDS, which only detects and alerts on threats, an IPS actively responds to potential threats, making it a big part of modern cybersecurity defenses.

Often IDS and IPS are the same systems that can be configured to work only in the detection mode or to actively take measures to mitigate detected attacks. Thus, the functionalities of an IDS can also be found in an IPS.

An IPS usually has the following functions:

- **Automated response**: IPS can automatically block or mitigate threats by terminating services, dropping malicious packets, or updating firewall rules, often without the need for operator intervention;
- **Signature-Based detection**: IPS relies heavily on signature-based detection, using predefined attack patterns (signatures) to identify threats. It is particularly effective at preventing well-known attacks with established signatures;
- **Real-Time threat prevention**: By operating in line with network traffic, IPS systems can detect and block malicious activity as it happens, preventing damage before it can spread through the network.

The most common challenges encountered by IPS/IDS are the following:

1. **False positives and tuning**: One of the main challenges with IPS/IDS is the high rate of false positives, where legitimate traffic may be incorrectly flagged as malicious. This risk requires careful signature tuning. SOCs often run IPS in an alert-only mode (only the IDS mode) for several days or weeks before enabling blocking mode (IPS) to minimize the risk of inadvertently causing a denial of service (DoS) by blocking legitimate traffic. Additional tuning is required to minimize false negatives in IPS/IDS systems.
2. **Response actions**: IPS can react to detected threats in various ways. The most effective method is dropping malicious packets and preventing further communication between the attacker and target. However, improper configurations, such as relying on TCP resets, can alert attackers to the presence of an IPS and allow them to adjust their attack tactics.
3. **Network placement and impact**: Proper placement of IPS within the network is very important to ensuring effective threat prevention without disrupting legitimate operations. Incorrect placement or configuration can introduce latency, throttle bandwidth, or inadvertently block critical services. This is especially true for high-bandwidth environments, where undersized or poorly configured IPS systems can cause performance issues, for instance, when they are inadvertently set to analyze every single network packet.
4. **Signature context and analysis**: IPS/IDS systems that provide detailed signature information and context help SOC analysts understand why a specific threat was detected or even blocked. Access to detailed session data, such as packet capture (PCAP) alongside signatures, can reduce false positives and enhance the accuracy of threat detection. This is a continuous process.

In today's threat landscape, where attacks are becoming more sophisticated, IPS is essential for real-time threat prevention. While traditional signature-based detection remains effective for known threats, modern IPS systems often integrate with advanced detection methods such as anomaly detection, behavioral analysis, and machine learning to identify zero-day attacks or new, previously unknown threats. Additionally, IPS has evolved into more comprehensive solutions that merge with other security functions, such as NDR and next-generation firewalls, providing a unified defense against a wide range of attack vectors. Despite its challenges, including potential performance impacts and false positives, IPS remains a must for network defense, offering a first line of automated defense against intrusions and attacks.

Examples: Snort, Suricata, Cisco Firepower, Palo Alto Networks NGFW

Encryption tools:

Encryption tools ensure that sensitive data is protected both at rest and in transit by converting data into a secure format that unauthorized parties cannot access.

Examples: BitLocker, VeraCrypt, AWS KMS (Key Management Service).

Identity and Access Management (IAM):

IAM solutions manage digital identities and enforce access controls for both users and machine entities, ensuring that only authorized personnel and systems can access critical C-ITS systems and data.

Examples: Okta, Microsoft Azure Active Directory (AD), IBM Security Identity Governance

4.7.2 Core function - PROTECT – Processes

PROTECT processes are focused on implementing security measures that safeguard the C-ITS environment from threats. This includes managing access, securing communication, and protecting data.

Operational access control and authentication management:

- Implement processes for controlling access to C-ITS systems, ensuring that only authorized personnel and systems can interact with traffic management systems, vehicle communications, and control networks;
- Establish robust identity verification protocols, including those for human-to-machine (H2M) and machine-to-machine (M2M) interactions, applicable across both OT and IT environments, and incorporate certificate-based authentication for V2X communication.

Strategic IAM planning:

- Define and manage processes for authenticating users and devices that interact with critical C-ITS systems, ensuring only authorized entities can access critical data and systems;
- Implement robust machine identity management by assigning unique identifiers to devices and systems. This enables secure authentication for M2M interactions. Enforce advanced control mechanisms, including role-based access control (RBAC) and attribute-based access control (ABAC), complemented by multi-factor authentication (MFA) to protect critical assets;
- Establish lifecycle management processes for human and machine identities, starting with provisioning access (Joiner), managing changes like role or attribute changes (Mover), and finishing by deprovisioning access (Leaver).

Network security monitoring and hardening:

- Harden network defenses for IT and OT components in C-ITS, including vehicle communication links, traffic control systems, and roadside infrastructure;
- Implement processes for regularly updating firewalls, network segmentation, and encryption to protect sensitive communications.

Data encryption and integrity management:

- Ensure processes are in place to encrypt all critical communications between C-ITS components (V2V, V2I, and V2X) both in transit and at rest;
- Monitor data integrity by verifying that sensitive information (e.g., traffic control data) has not been tampered with.

Endpoint hardening:

- Instantiate a process for hardening description and review, based on known standards (e.g., NIST hardening guideline);
- Harden devices before they go to production. A well-defined and automized process for the hardening must be applied;
- Hardening should be reevaluated and tested on a periodical basis, ideally in an automated process.

Patch management and system updates:

- Establish patch management processes that prioritize critical updates for both IT and OT assets, particularly for traffic control systems and roadside units;
- Ensure timely deployment of security patches for all systems involved in C-ITS operations.

Security awareness and training programs:

- Continuously train personnel involved in the management and operation of C-ITS infrastructure on emerging threats and best practices for protecting IT/OT systems;
- Conduct regular phishing and social engineering drills to raise awareness among all stakeholders;
- On-board new employees and train them accordingly to raise the awareness level to a defined baseline.

4.8 Core function - RECOVER

The RECOVER function focuses on ensuring that organizations can resume normal operations after a cybersecurity incident, minimizing downtime and ensuring resilience. The key objectives are represented in *Tab. 23*.

***Tab. 23** SOC for C-ITS – DETECT – Objectives*

Objectives	Descriptions
System Restoration and Backup	*Implement processes for restoring critical C-ITS subsystems (traffic management, vehicle communications) from backups in case of a cybersecurity incident, ensuring minimal downtime.*
Disaster Recovery and Continuity Planning	*Develop disaster recovery and business continuity plans to ensure that transportation services can continue in the event of a cyberattack.*
Post-Incident Review and Continuous Improvement	*Conduct post-incident reviews to identify gaps and improve the SOC's processes and defenses, ensuring that lessons learned from incidents are used to prevent future occurrences.*
Service Continuity for Critical Operations	*Ensure that critical services, such as vehicle-to-infrastructure communications and traffic control systems, can continue to function during and after an incident.*
Public Communication and Transparency	*Develop processes for communicating with the public and stakeholders during recovery efforts, providing transparent information on the status of transportation systems and ongoing recovery efforts.*

4.8.1 Core function - RECOVER – Technologies

Backup and disaster recovery solutions:

These tools create regular backups of critical data and systems, allowing organizations to recover quickly in the event of data loss, ransomware attacks, or other incidents.

Examples: Veeam Backup & Replication, Acronis, Rubrik

Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP) platforms:

BCP and DRP platforms help organizations develop and execute recovery plans to minimize disruption to operations following an incident.

Examples: Zerto, Arcserve, Plan4Continuity

Data integrity monitoring:

These tools monitor data and system integrity, ensuring that any changes or corruption to critical systems or data are detected and corrected during the recovery process.

Examples: Tripwire, CimTrak, Veritas

4.8.2 Core function - RECOVER – Processes

RECOVER processes are essential for restoring normal operations after an incident, ensuring the continuity and resilience of C-ITS.

Business Continuity and Disaster Recovery (BC/DR) planning:

- Establish BC/DR plans for critical C-ITS services, such as traffic management systems, ensuring minimal disruption to transport services in the event of a cyber incident;
- Regularly test disaster recovery processes to ensure readiness in restoring essential functions after an attack.

Backup and system restoration:

- Define processes for regularly backing up critical data and configurations from C-ITS subsystems, ensuring that data can be restored quickly after a ransomware attack or system failure;
- Prioritize the restoration of OT systems that control essential infrastructure like traffic signals and communication networks;
- Regularly test restoration of the systems to ensure the ability to restore correctly lost data

Lessons learned and continuous improvement:

- Conduct post-incident reviews to document lessons learned from security incidents and improve response and recovery processes;
- Implement a continuous improvement process to enhance security controls and SOC processes based on incident findings.

4.9 SOC – Human factors

To implement, improve and use the previously stated SOC objectives, cybersecurity professionals are needed who can be responsible for monitoring the organization’s infrastructure at all times to detect cybersecurity events in real time and address them as quickly and effectively as possible. They should also be capable of developing the organization’s incident response plan, which defines activities, roles, and responsibilities in the event of a threat or incident.

However, it is not solely their technical expertise that ensures a successful SOC; effective communication and coordination among different teams within the SOC as well as with external stakeholders are essential for a cohesive response to security incidents. The SOC ensures that all relevant parties are informed promptly, enabling a swift and coordinated response.

Tab. 24 is a non-exhaustive list of potential SOC roles.

Tab. 24 *Different Human roles in the SOC Environment*

Role	*Summary*
SOC Manager	*Responsible for managing the SOC team and SOC operations*
Security Analyst	*Monitors the organization's networks and systems for signs of security threats, assists in triaging alerts based on severity, and handles simple alerts*
Incident Responder	*Reacts to security incidents by performing in-depth assessments, mitigating damage and restoring normal operations*
SOC Engineer	*Responsible for maintaining and updating tools and systems*
Threat Hunter	*Identifies potential security threats by proactively searching through network traffic data*
Forensic Analyst	*Performs root cause investigation of security incidents by analyzing digital evidence*

SOC Manager

The SOC Manager is responsible for managing the SOC and its teams, ensuring optimum performance. Managers oversee day-to-day operations, including effective monitoring and incident response. More specifically, their responsibilities include team leadership, such as hiring and training SOC personnel. In addition, managers are responsible for developing strategic approaches to enhance SOC capabilities, optimizing technologies by implementing the latest tools and systems, and continuously improving security measures. They communicate with all roles within the SOC and maintain communication with external stakeholders, such as the CISO, reporting on SOC performance and aligning security strategy.

Security Analyst

The Security Analyst monitors the organization's networks and systems for signs of security threats, assisting in triaging alerts to determine their authenticity and criticality. Analysts respond to simple security threats but escalates confirmed critical incidents to the incident response team. Their role also includes conducting vulnerability tests to identify system weaknesses and providing information to SOC engineers or relevant teams to address these issues and strengthen the organization's defenses. The Security Analyst communicates mostly with Incident Responders, Threat Hunters and SOC Engineers.

Incident Responder

The Incident responder investigates and mitigates security incidents escalated by Security Analysts. Responders perform in-depth assessment using threat intelligence and implements actionable strategies to minimize impact, prevent further compromises and restore normal operations. The Incident Responder communicates with Security Analysts, Forensic Analysts, SOC Engineers, and external stakeholders such as legal departments, communication services and law enforcement to ensure coordinated and comprehensive incident response.

Their responsibilities include:

- Incident Triage and Prioritization: Assessing the severity and potential impact of escalated incidents, prioritizing based on risk, and initiating appropriate response actions;
- Incident Response and Mitigation: Taking immediate action to contain, investigate, and mitigate the incident. They work swiftly to minimize the impact on systems, networks, and data. This may involve isolating affected systems, implementing countermeasures, and coordinating with relevant teams to resolve the incident effectively.

SOC Engineer

The SOC Engineer focuses on the infrastructure and tools that support the SOC. The engineer is responsible for configuring, maintaining and optimizing security tools, as well as developing various automated programs and processes to improve operational efficiency. The SOC Engineer also maintains and updates tools and systems, provides technical assistance to the SOC team in resolving tool-related issues, and monitors tool performance, making adjustments and configuration revisions to remain up to date. It also

addresses system vulnerabilities identified by Security Analysts. The SOC Engineer communicates with Security Analysts, Incident Responders, Forensic Analysts and the SOC manager.

Threat Hunter

The Threat Hunter proactively identifies and mitigates cybersecurity threats before they compromise an organization. This role is an extension of traditional cybersecurity functions, focusing on neutralizing advanced threats that may escape the SOC. The Threat Hunter constantly analyzes data to uncover hidden threats, tracks vulnerabilities and assesses risk, ensuring potential security gaps are closed before they can be exploited. Advanced threats can account for up to 10% of cyber threats, and not all advanced threats are detected by SOC solutions alone; this is where the Threat Hunter is invaluable. Threat Hunters gather intelligence from various sources such as the internet, forums and interest groups to get the latest information on emerging threats and attack techniques. Their communications are mostly with Security Analysts, SOC Engineers and the SOC Manager.

Forensic Analyst

The Forensic Analyst participates in the investigation of serious security incidents by analyzing digital evidence to extract useful information for mitigating system and network vulnerabilities. Forensic analysts perform in-depth forensic investigations to determine the root cause of incidents, assess the extent of the compromise, and identify the attacker's methods and motivations. The Forensic Analyst collaborates closely with incident response teams, sharing findings and insights to help resolve ongoing incidents. He is also responsible for handling digital evidence, ensuring its continuity and integrity for potential legal proceedings. After conducting the analysis, the Forensic Analyst provides a detailed report on the full scope of the breach and ways to mitigate its long-term impact. This report supports incident response efforts, provides formal records for the SOC Manager and helps inform future security strategies. Additionally, the Forensic Analyst may communicate with regulatory authorities to assist with any legal proceedings. External roles collaborating with the SOC are essential to support core functions of the NIST CSF. For the GOVERN function, there is generally no dedicated role within the SOC except the SOC manager; rather, the function is managed at the organizational level.

Chief Information Security Officer

The CISO is a senior-level executive who oversees an organization's cybersecurity strategy and operations. Beyond the SOC, the CISO is responsible for designing and developing the organization's cybersecurity governance framework, which includes setting standards for data protection, network security and incident response. The CISO ensures policies are in line with the organization's objectives and regulatory requirements. While not directly managing the SOC, the CISO provides strategic guidance, ensures compliance, and collaborates with internal and external stakeholders, such as the SOC Manager, other senior management, IT teams and regulatory authorities, aligning cybersecurity measures with business needs.

Risk Manager

The Risk Manager operates as an external entity to the SOC, typically within a broader governance role. This role maintains extensive interaction with the SOC and other organizational stakeholders, such as the CISO. The Risk Manager's primary responsibilities can be structured into three key areas: Risk Identification and Assessment, Risk Mitigation Strategies and Communication and Reporting. The Risk Manager continuously identifies and assesses risks and threats related to IT systems, networks and data within the organization, including those relevant to the SOC's functions. This involves evaluating the likelihood and potential severity of impact, with a focus on critical C-ITS assets that directly affect safety and transport operations. Based on this assessment, the Risk Manager develops targeted mitigation strategies, prioritizing risks according to their potential impact on C-ITS operations. Risk Managers communicate the result of the risk assessment and mitigation plans to the relevant stakeholders. They collaborate with the CISO to align risk management initiatives with overall security policies, ensuring a consistent approach. They also work closely with SOC members to integrate cybersecurity

insights like threat intelligence, asset inventories and vulnerability data into the risk assessment process. This two-way interaction also allows the SOC to act on the result of the risk assessment, while ensuring its outputs inform broader risk management decisions. Each role may contribute to multiple functions; however, *Tab. 25* highlights their primary responsibilities to emphasize their central contribution to achieving NIST's core functions.

***Tab. 25** Different Human roles in the SOC Environment*

NIST CSF core function	Role
IDENTIFY	SOC Manager, Threat Hunter, (Risk Manager)
DETECT	Security Analyst, Threat Hunter
RESPOND	Incident Responder, Forensic Analyst
GOVERN	(CISO), (Risk Manager), SOC Manager
PROTECT	SOC Engineer, Security Analyst
RECOVER	SOC Manager, SOC Engineer

4.10 Security Operation Center – Strategies

This section introduces key factors for defining the best strategies for SOC implementations and operations. The initial primitives below make it possible to compare the SOC strategies (In-house, Hybrid or MSSP) defined in *Tab. 26* and *Tab. 27*.

***Tab. 26** Key factors for SOC strategy definition*

Aspects	Descriptions
Governance structure	• Governance structure refers to the framework of policies, procedures, and decision-making processes that guide the operations of the SOC; • It defines the roles and responsibilities of various stakeholders, including senior management, SOC managers, analysts, and external service providers; • A clear governance structure ensures accountability, transparency, and compliance with regulations and organizational objectives.
Communications	• Communications encompass the channels and methods used for sharing information within the SOC team and with external stakeholders; • Effective communication is essential for timely detection and response to security incidents; • It includes both formal channels such as reports, meetings, and documentation, and informal channels like email, phone calls, and instant messaging.
Resources	• Resources refer to the people, skills, technology, and infrastructure required to operate the SOC effectively; • This includes cybersecurity professionals with expertise in threat detection, incident response, and forensics, as well as tools such as SIEM systems, threat intelligence platforms, and endpoint detection and response (EDR) solutions; • Adequate resource allocation is essential for maintaining SOC operations and responding to security incidents in a timely manner.
Accountability	• Accountability is the obligation of individuals or teams to accept responsibility for their actions, decisions, and performance; • In the context of a SOC, accountability ensures that stakeholders are held responsible for their roles in security monitoring, incident detection, analysis, and response; • Clear lines of accountability help prevent errors, improve transparency, and facilitate continuous improvement of SOC operations.
Data ownership	• Data ownership refers to the rights and responsibilities associated with the collection, storage, processing, and use of data within the SOC; • Organizations must clarify who owns the data collected and analyzed by the SOC, including log files, network traffic data, and security event information; • Data ownership issues can arise when working with external service providers, and it is essential to establish clear agreements regarding data access, use, and protection.

Scalability & flexibility	• Scalability refers to the ability of the SOC to handle increasing volumes of data, users, and security events without compromising performance or effectiveness; • Flexibility refers to the adaptability of the SOC to changes in technology, threats, regulations, and business requirements; • A scalable and flexible SOC can adjust its resources, processes, and technology to meet evolving security needs and organizational priorities.
Business objectives	• Business objectives are the strategic goals and priorities of the organization that the SOC supports; • These objectives may include protecting critical assets, ensuring regulatory compliance, minimizing operational disruptions, and safeguarding the organization's reputation; • A SOC strategy should align closely with the organization's business objectives to ensure that security efforts are focused on addressing key risks and achieving tangible business outcomes.

***Tab. 27** Key organizational structure strategy*

Strategy	***Descriptions***
In-House SOC	• In this approach, organizations establish their own SOC internally with dedicated staff and resources; • The SOC team is responsible for monitoring, detecting, analyzing, and responding to cybersecurity incidents; • This strategy provides complete control and customization over the SOC processes and technology stack. However, it requires significant investment in hiring, training, and maintaining skilled cybersecurity professionals and infrastructure; • **This strategy is the most conservative approach to data protection and cybersecurity ownerships (governance-level).**
Virtual SOC	• This approach is a variation of the In-house model where internal staff collaborate closely within a non-distributed organizational structure; • A virtual SOC operates remotely, with SOC analysts working from different locations; • Virtual SOC teams collaborate using remote communication and collaboration tools that must be used through secure communication protocol; • This approach allows organizations to tap into a global talent pool and overcome geographical constraints; • However, effective communication and coordination are essential to ensure the efficiency and efficacy of virtual SOC operations; • **This strategy might raise issues about data protection and cybersecurity ownerships (governance-level).**
Managed Security Services Provider (MSSP)	• Organizations can outsource their SOC capabilities to third-party MSSPs; • MSSPs offer a range of services including 24/7 monitoring, threat detection, incident response, and reporting; • This approach can be cost-effective for organizations that lack resources or expertise to build and maintain an in-house SOC; • MSSPs often have specialized tools, expertise, and experience in handling security incidents across various industries and sectors; • **This strategy might raise issues about data protection and cybersecurity ownerships (governance-level).**
Hybrid SOC	• A hybrid SOC model combines elements of both in-house and managed services; • Organizations may retain certain critical security functions in-house while outsourcing other functions to MSSPs; • For example, organizations may choose to handle incident response internally while outsourcing 24/7 monitoring and threat intelligence; • This approach allows organizations to leverage external expertise while maintaining control over core security functions; • **This strategy might potentially reduce issues raised from a completely MSSP-based approach, depending on activity distributions.**

Co-Managed SOC	• Co-Managed SOC is a variation of the hybrid model where organizations collaborate closely with MSSPs to manage their SOC operations; • In this model, the MSSP and the internal security team work together to monitor and respond to security threats, and internal team retains control over strategic decisions and high-level analysis, while the MSSP provides operational support and expertise; • **This approach can be beneficial for organizations that want to augment their internal capabilities without fully outsourcing their SOC functions.**
Cloud-Based SOC	• With the increasing adoption of cloud services, some organizations opt for cloud-based SOC solutions; • Cloud-based SOC platforms offer scalable, on-demand security monitoring and incident response capabilities; • These platforms leverage cloud infrastructure and analytics to provide real-time threat detection and response; • Cloud-based SOC solutions can be particularly suitable for organizations with distributed or cloud-native environments; • **This approach does not provide a full set of SOC capabilities and should therefore be considered as a potential add-on for enhancing other major strategies;**

For the purpose of establishing a SOC Roadmap, the alternatives listed above will be considered and benchmarked. The goal is to identify the most suitable setup for a governmental body capable of address cyber-risks in C-ITS.

4.11 Security Operation Center – Regulatory Context for SOC Implementation in C-ITS

This section will describe the regulatory frameworks —briefly introduced in section 2.3 – that will shape the development and operations of SOCs for C-ITS in Switzerland. Key national and European directives are also examined, as some of them help define SOC responsibilities in operational and cybersecurity contexts. The section will thus provide a detailed explanation of how this regulatory framework and key guidance will influence SOC operations in Switzerland. Specifically, it will outline:

- The impact of EU directives on SOCs in Switzerland;
- The SOC's responsibilities as defined by Swiss regulations and baseline guidance, highlighting specific actions and obligations for SOC teams;
- Relevant components from existing Swiss Directives, particularly those from FEDRO on OT security for EES, and how these shape SOC development and activities in the context of C-ITS.

4.11.1 European Union

"Revised ITS Directive" Directive (EU) 2023/2661 [12]

The revised ITS directive provides a comprehensive framework for managing ITS services. Key cybersecurity requirements from the directive and their implications for SOCs are described in *Tab. 28*.

***Tab. 28** Summary of the revised ITS directive*

Directive detail	SOC Tasks for Compliance
Cybersecurity requirements	**Swiss SOCs should**
The directive mandates secure communications and trust management for C-ITS, ensuring integrity and authenticity of message exchanges between vehicles and infrastructure. A C-ITS trust model based on PKI must be established, with the highest level of that PKI being the ECTL (European Certificate Trust List) [19], consisting of entries of all trusted root certification authorities in Europe.	• Implement a local PKI aligned with the ECTL to manage vehicle and infrastructure certificates. • Be able to validate certificates issued by other European CAs listed in the ECTL.

Interoperability & traffic data accessibility Traffic data must be interoperable, accessible in machine-readable formats, and compliant with EU standards (e.g., Delegated Regulation 2017/1926 [3]). There is no requirement to add new data or invest in additional roadside infrastructure, but the existing traffic data must be accessible in compliant digital formats.	• Swiss SOCs should ensure compatibility with the EU's ITS traffic data digital formats, to enable seamless cross-border interoperability.
Data availability and sharing Member States must operate National Access Points (NAPs) [18] to manage and share ITS-related data in machine-readable formats for interoperability.	• Switzerland could establish the equivalent of an NAP system or align its data-sharing framework with neighboring EU NAPs. SOCs will need the necessary access and capabilities to support the system in place.
Data protection and privacy requirements The directive enforces compliance with data protection standards, including the GDPR [1].	• SOCs must align their data handling processes with these legal requirements, ensuring anonymization and pseudonymization where applicable.
Emergency situations In emergency situations, the EU Commission can implement countermeasures to protect ITS services, such as suspending obligations or ensuring service continuity.	• Swiss SOCs should prepare incident response plans aligned with EU protocols for cross-border C-ITS incidents.
Artificial Intelligence Regulations For ITS services leveraging AI, the directive requires adherence to harmonized rules under the EU AI Act [10].	• Swiss SOCs should ensure that C-ITS AI systems align with Switzerland's upcoming, lighter sector-specific AI regulations (the EU AI Act doesn't apply), based on the Council of Europe's AI Convention and targeted legal adjustments in transport.
ITS Service Deployment Member States must deploy specific ITS services, such as time traffic information and road safety warnings, by certain deadlines.	• Swiss SOCs should prioritize deployment for these specific ITS services, ensuring compatibility with EU-deployed services.

For Swiss SOCs for C-ITS, the most important aspects of the revised EU ITS Directive are the implementation of an ECTL-compatible PKI system, the guarantee of data interoperability and accessibility in EU-compliant formats and the development of incident response plans aligned with EU protocols for cross-border C-ITS incidents.

4.11.2 United States

While the United States has implemented CIRCIA [8], Switzerland's FAISC [5] established a similar legal framework with comparable requirements. Although the previously mentioned CISA guideline could serve as useful reference for incident response practices, they are not mandatory in Switzerland, where existing regulations and standards already provide sufficient guidance on this topic. Therefore, U.S. regulations and guidelines will not be explored further at this stage.

4.11.3 Switzerland

ICT minimum standard – NCSC [24]

The ICT Minimum Standard, while not tailored to C-ITS, provides a comprehensive baseline for cybersecurity practices. Its alignment with the NIST CSF core functions simplifies the integration of its principles into C-ITS SOC operations. By detailing concrete tasks for achieving the objectives of each function, the standard bridges the gap between theoretical frameworks and practical implementation. Currently, this guidance is normative only in the energy sector, but it holds potential to become mandatory in other critical sectors, including public transport. Its practical approach makes it highly relevant for C-ITS

SOC planning and implementation, both for now and in anticipation of future regulatory developments. *Tab. 29* breaks down how each category corresponds to SOC responsibilities in a C-ITS context:

Tab. 29 *NIST Cyber Security Framework [23]*

NIST CSF Function	Category	SOC Responsibilities
Identify	**Asset management**	SOCs must maintain an **up-to-date inventory of C-ITS** components, including hardware, software and communication interfaces, to monitor and protect critical assets effectively
	Governance	Clear **policies** and **roles for SOC operations** must be defined to ensure alignment with organizational goals and requirements
	Risk assessment and risk management strategy	**Continuous assessment** of **cybersecurity risks** in **C-ITS systems** enable SOC to prioritize efforts and resource allocation. An external risk manager can have this responsibility
	Supply chain risk management	**Evaluating risks** associated with **third-party suppliers** and ensuring compliance with security standards is essential for maintaining the integrity of C-ITS infrastructure
Protect	**Access management**	**Role-based access controls** and **identity verification** mechanisms ensuring only authorized personnel can access SOC tools and C-ITS systems
	Awareness and training	Regular **training for SOC personnel** on threats specific to C-ITS systems enhances incident response capabilities
	Data Security	**Encryption**, **secure storage** and **access control** safeguard sensitive C-ITS data
	Protective technology	Deployment of protective technologies such as **firewalls**, **IPS** and **EDR tools**, which are the first line of defense in SOC operations
Detect	**Anomalies and events**	**SOCs** should **establish baselines for normal C-ITS operations** to be able to **detect** any **deviations** that may indicate security incidents
	Security continuous monitoring	**Real-time monitoring of C-ITS networks** and components enables rapid detection of potential threats
	Detection process	**Standardized procedures** for **identifying** and **categorizing incidents** ensures efficient threat analysis and escalation
Respond	**Response planning**	SOCs must have **documented playbooks** for **common C-ITS attack** scenarios
	Communication protocols	Clear **communication protocols** with **stakeholders** are essential for coordinated responses
	Analysis and mitigation	SOCs should conduct **detailed analysis of incident** to help identify root causes and implement targeted countermeasures
	Improvements	**Post-incident review** allows SOCs to refine response strategies
Recover	**Recovery planning**	SOCs must develop **recovery plans** to restore services after disruption
	Improvements	**Lessons learned** inform updates to policies and procedures
	Communication during recovery	**Transparent communication** to stakeholders during recovery phases facilitate coordinated efforts

The Swiss Federal Council has introduced a mandatory reporting requirement for cyberattacks targeting critical infrastructure, effective from April 1, 2025. The operators concerned include energy and water suppliers, transport companies, and cantonal and municipal administrations. They must inform the NCSC within 24 hours of detecting an attack. This measure will enable the NCSC to assist affected organizations and alert other critical infrastructure operators.

The reporting obligation applies when an attack threatens the operation of critical infrastructure, leads to data manipulation or leaks, or involves extortion, threats, or coercion. Organizations failing to comply with this requirement may face fines starting October 1, 2025, after a six-month preparation period for the new regulation.

This reporting requirement aligns with the functions of the NIST Cybersecurity Framework, which serves as the foundation for Switzerland's ICT Minimum Standard. This harmonization ensures that Swiss SOCs adopt best cybersecurity practices and implement comprehensive strategies to protect C-ITS. As a result, Swiss SOCs will be well-equipped with robust protection, detection, response, and recovery capabilities, positioning them effectively to address evolving cybersecurity challenges in C-ITS operations. To facilitate the process, a reporting form will be available on the NCSC's Cyber Security Hub platform, already used for information exchange with critical infrastructure operators. Organizations not yet registered on this platform will be able to submit reports via email.

FAISC: Federal Act on Information Security [5]

The FAISC is being amended with an obligation to report cyberattacks for operators of critical infrastructures to the BACS. The amended version ("revISA") will become law, entering into force in January 2025. Reports must be made within 24 hours following the discovery of the cyberattack and can be made anonymously. The list of cumulative criteria to decide whether an incident needs to be reported or not is described in in the act. Implications for SOCs on this new obligation include:

- Development of processes to meet the 24h reporting deadline;
- Implementation of systems to track and document incident meeting reporting criteria;
- Training for SOC personnel on new reporting obligations.

In addition to this new amendment, which leads to strict SOC requirements, the current version of the FAISC establishes several provisions that are important for SOC operations for C-ITS, as described in *Tab. 30*.

***Tab. 30** FAISC provisions linked to SOC Roles*

Category	FAISC Provisions	SOC Role
General principles	• **Information protection** (confidentiality, availability, integrity, traceability**)** • **Regular risk assessments** • Quick **detection** and **mitigation** of information security **violations** • **Action plans** for serious information security **breaches** and exercises for these scenarios • **Third-party agreements** in line with FAISC **requirements** and monitored for compliance	• Implement and maintain monitoring systems to ensure adherence to information security principles • Assist in risk assessments by providing threat intelligence and incident data • Develop and maintain incident detection and response capabilities • Create and maintain playbooks for major security incidents, conduct regular drills • Monitor third-party compliance with FAISC requirements
Information Classification and Handling	• **Information classification** based on potential harm • **Restricted access** to classified information	• Enforce classification policies for C-ITS data set by governance • Implement and manage access control systems for classified data • Monitor and audit access to classified C-ITS data

IT Security	• **Development of a security procedure for IT resources** • **Categorization of IT resources into security levels: basic protection, elevated protection, very high protection** • **Setting minimum security requirements for each security category. Periodic effectiveness checks for the "very high protection" category.**	• **Maintain security procedures for C-ITS IT resources in alignment with governance-defined policies** • **Enforce security controls based on C-ITS IT resource categorization defined by governance** • **Monitor compliance with security requirements for each category, especially focusing on the very high protection category**
Personnel Security	• Careful **selection**, **identification** and **training** of personnel accessing information and IT resources • **Restricted** issuance of **access** authorizations	• Provide regular security awareness training to SOC and C-ITS staff • Enforce access authorization policies through technical controls • Monitor access authorizations for C-ITS systems
Physical Security	• Adequate **physical protection** of information and IT resources • Establishment of **security zones**	• Monitor physical access to restricted zones for critical C-ITS components

The FAISC, particularly its upcoming amendment ("revISA"), establishes new obligations that directly impact SOCs. Beyond the new incident reporting requirements, the broader provisions of the FAISC also cover general security principles, information security and personnel security, and define essential practices that fall within the SOC for C-ITS's responsibilities.

FEDRO Directives

Instruction on OT Security governance - ASTRA 73006 v1.00 [13]**:**

This instruction addresses OT cybersecurity, particularly for operational and safety equipment. While the governance framework described focuses on OT systems, the SOC for C-ITS must address both OT and IT. However, OT security governance can be directly leveraged for C-ITS security management. Key elements of the instruction that can inform SOC governance for C-ITS are summarized in *Tab. 31*.

Tab. 31 *ASTRA 73006 linked to SOC relevance and actions*

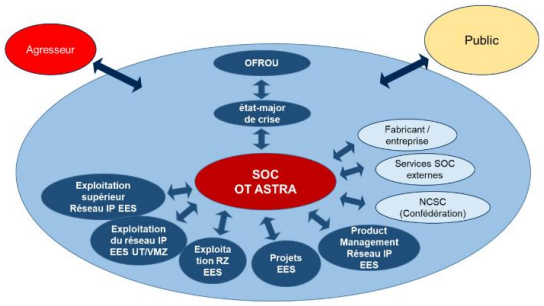
Category	Description	SOC Relevance and Actions
Organizational Structure	A **three-tiered approach**, with **Strategic** (Change Advisory Board), **Implementation** and **Operational** levels.	A similar tiered approach could be adopted to manage both IT and OT within SOC governance.
Three Pillars Approach	The instruction **focuses** on the three pillars: **Humans**, **Processes** and **Technologies.**	This approach aligns directly with the SOC framework described in this report and supports comprehensive security management.
Security Management Components	**Regulatory Compliance, Audit and Controlling, Risk Analysis**	Security Management Components are fully aligned with the SOC's GOVERN function described in this report.

The ASTRA 73006 Instruction offers a quite aligned framework with SOC governance in C-ITS. While it provides a strong foundation, full alignment and integration are to be carefully handled to manage overlaps at the IT-OT intersection, especially in roles, processes and technologies.

Directive on OT Security - ASTRA 13030 V2.0 [14]

The directive provides a comprehensive framework for securing operational and safety equipment. While primarily focused on OT systems, its core elements can be directly relevant for implementing an SOC for C-ITS. This relevance is described in *Tab. 32*.

***Tab. 32** ASTRA 13030 linked to SOC relevance and actions*

Category	Description	SOC Relevance and Actions
OT Security Management System	Ensures **uniform OT security level** and **architecture** with a focus on necessary security measures rather than maximum possible security	Adapt the OT security management system to handle hybrid IT-OT environments
Risk and Threat Analysis	Provides systematic **threat analysis for OT systems and processes**, using both quantitative and qualitative risk assessment Provides a **list of potential threats** and **risk scenarios** specific to EES infrastructure	Integrate risk and threat analysis methodologies into SOC processes Maintain an up-to-date threat intelligence repository
Organizational Structure	Defines clear **OT security roles** and **responsibilities** Introduces an **OT Security Operations Center** (SOC OT ASTRA), as a central point for monitoring, managing and defending EES infrastructure 	Use the SOC OT ASTRA model as a starting point for the SOC for C-ITS, expanding it to address both IT and OT aspects of C-ITS security Define human roles, technologies and processes for OT and IT
Personnel Development	Emphasizes **know-how**, **training** and **security awareness**	Develop security training programs to improve SOC team awareness and response capabilities
Technical Specifications	Promotes principles such as **defense-in-depth**, **least privilege**, **security by design/default**, and **traceability** Provides baseline protection measures for • Information (data); • OT systems; • OT base infrastructure; • Network/network zones; • Perimeter protection; • Physical infrastructure/access; • Mobile and third-party devices.	Implement defense-in-depth strategies, including network segmentation, least privilege access, encryption and audit controls

By encompassing risk analysis, personnel development and technical specifications for OT, this directive offers valuable insights for SOC implementation for C-ITS environments. While designed for OT, its components can be adapted to address both OT and IT aspects of C-ITS. The SOC OT ASTRA model can serve as a starting point for the proposed SOC for C-ITS, which will require adjustments to address the hybrid IT-OT nature of C-ITS

environments. The SOC for C-ITS will involve a broader range of personnel, technologies and processes.

Instruction on Roles and requirements for EES management - ASTRA 73001 [15]

This instruction outlines a management system for EES, focusing on standardized processes for identification, listing and management to ensure planning and maintenance. While not directly cybersecurity-related, this instruction still offers valuable elements for a SOC for C-ITS, as presented in *Tab. 33*.

***Tab. 33** ASTRA 73001 linked to SOC relevance and actions*

Element and Description	SOC Relevance and Actions
Structured Maintenance Framework covering routine maintenance, inspection and asset management	• The SOC could adapt this structured approach, applying it to security monitoring, incident response and risk-based prioritization of vulnerabilities

Swiss Equipment Management System (EMS-CH) ensuring planning, operation, maintenance and data management of EES	• The SOC could enhance security by:
	  • Integrating EMS-CH data into its security monitoring tools for real-time threat detection.
	  • Monitoring EMS-CH's data exchanges with third-party systems for data integrity and threat visibility

Asset Management with strict coding and hierarchical classification of EES elements	• The SOC must maintain a comprehensive asset inventory to track components and identify potential vulnerabilities or misconfigurations
Defined Roles and Responsibilities for EES maintenance, such as inspectors and quality controllers	• These roles could be mirrored or expanded within the SOC, where SOC analysts monitor cyber threats while EES personnel focus on physical threats
Interfaces and Integrations exist between EMS-CH and third-party systems, like MISTRA (Management Information System Roads and Traffic)	• The SOC should secure and monitor these data exchanges for threats, ensuring data flow protection and secure system interactions

The framework for managing EES provides a foundation for SOC operations by offering structured maintenance processes, standardized asset management and defined operational roles. The SOC can leverage these elements, integrating them into its security workflows for enhanced visibility, proactive threat detection and better cybersecurity measures.

Instruction on Management of operational and security equipment: roles, tasks, and requirements for user interfaces - ASTRA 73002 V1.01 [16]

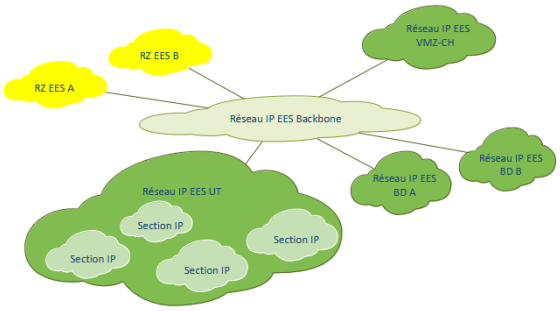
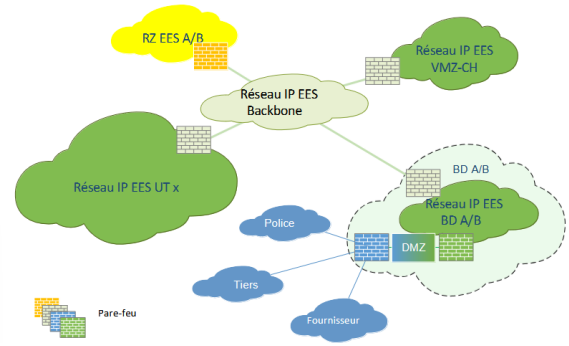
The instruction defines roles and tasks related to EES management. While it lacks cybersecurity roles, its framework could be expanded to include them. The instruction also describes a framework for creating and managing user interfaces for EES. The direct application to cybersecurity and specific SOC operations is limited in this instruction, therefore no additional details will be added here.

DIRECTIVE on IP EES Network ASTRA 13040 V1.3 [17]

The EES IP communication network provides a uniform communication infrastructure for EES throughout Switzerland, serving all FEDRO infrastructure sites, control centers and computing centers. It ensures uniform data flow for EES operations. The SOC will play a

key role in protecting this infrastructure, through monitoring, threat detection and enforcement of security controls. *Tab. 34* maps the directive to SOC relevance and actions.

***Tab. 34** ASTRA 13040 linked to SOC relevance and actions*

Category	Description	SOC Relevance and Actions
Network terminology and architecture	The IP EES network consists of: ▪ **IP EES UT Networks**: autonomous networks for EES systems within territorial units (UT), which are divided into independent IP sections (local subnets) for localized communication. ▪ **Connection rings**: interconnecting IP sections of UTs forming the core layer ▪ **IP EES Backbone network**: the core network linking UTs, data centers, and traffic management ▪ **IP EES VMZ-CH network**: Swiss traffic management center ▪ **IP EES BD A/B networks**: basic services ▪ **RZ EES A/B**: computing centers (RZ EES LAN does not belong to the EES IP network)  	Understanding IP EES network terminology and architecture is essential for effective SOC operations: • Maintain comprehensive visibility across all components enabling effective mapping and monitoring of critical assets and data flows • Apply targeted security controls and monitoring strategies based on architecture knowledge • Develop specific incident response playbooks for different network segments
Network security requirements	**High availability** and **security** for IP EES networks, which are central requirements, are ensured through: ▪ **Redundancy** design for equipment and fiber optic connections, avoiding single points of failure ▪ Network with high degree of **resilience** to failures ▪ **Firewall segmentation**: separation between EES UT IP network, EES Backbone IP network and federal networks ▪ **DMZ implementation for external connections**: all external connections between IP EES UT networks and third parties must pass through a DMZ.  IP EES network structure	The SOC should: • Set up monitoring systems to ensure that the redundant design is working, reporting any single points of failure • Test resilience to verify the network's ability to withstand failures • Manage firewall rules to ensure proper segmentation between networks and monitor firewall logs • Monitor all external connections and potential threats through the DMZ

Interfaces and integrations	The IP EES Backbone integrates various systems and networks, including territorial units, basic services, data centers, traffic management centers and partner networks. The federal administration network is completely separated from the IP EES Backbone	The SOC must ensure coverage across all connected systems and anticipate how network separation affects the monitoring scope and attack surfaces
Network equipment and services	Lists technologies and protocols used in the EES network, including MPLS, VLAN and IP/MPLS segmentation	The SOC should tailor monitoring strategies based on protocol use
IP Addressing and management	▪ Static IP addresses are used by all fixed equipment connected to the IP EES network ▪ Assigned IPv6 range: 2a07:2900:8000::/40 ▪ Centralized IP address management with the tool IPAM/DDI “Data Master”	The SOC should use IPAM/DDI data to identify and track all assets within the network, improving network visibility
DNS and DHCP configuration	DNS and DHCP configurations for IP addressing and device identification are managed via the IPAM/DDI tool	The SOC should use services configuration knowledge for misconfigurations and threats monitoring and detection
Network Management System	Manages network components using the FCAPS model (Fault, Configuration, Accounting, Performance, Security)	The SOC can leverage network management system data for performance, reliability and security insights
Operational Requirements	The infrastructure is set up centrally but used in a decentralized manner. Decentralized management: UTs manage local components: UT networks, DNS/DHCP servers, firewalls, DMZ Centralized management: IPAM/DDI tool, E2E-Service Monitoring tool, time and clock synchronization and inventory systems	The SOC would need to work closely with each UT team for local component monitoring The SOC would be responsible for the security of centralized managed tools and systems, which are critical targets for security monitoring as all UTs could be potentially impacted if compromised

The IP EES Network Directive defines a critical communication infrastructure for EES operations across Switzerland. The SOC can leverage the existing network architecture, operational practices, tools and systems already in place to further develop its capabilities. Building on this established foundation for OT systems will improve efficiency, ensure interoperability, and strengthen the overall cybersecurity posture.

4.11.4 Regulatory context summary

The regulatory landscape for SOC implementation for C-ITS is complex and encompasses both European and Swiss frameworks. The United States regulations are no longer considered, as a similar national framework with comparable requirements already exists. The revised EU ITS Directive lays the foundation for secure, interoperable C-ITS services across Europe, while Swiss regulations such as the FAISC and FEDRO directives provide a solid framework for information security management and OT security. The ICT Minimum Standard provides a comprehensive baseline for cybersecurity practices that can be adapted to C-ITS environments.

Integrating these diverse frameworks into a coherent SOC strategy that addresses both the IT and OT aspects of C-ITS, ensuring cross-border interoperability and maintaining the highest cybersecurity standards, is a challenge. For C-ITS SOCs in Switzerland, it is

essential to align with European C-ITS systems while taking advantage of existing frameworks and infrastructures, particularly for OT systems like EES.

An advantage of these regulations is their technology-agnostic nature, especially given the evolving cybersecurity threat landscape. This flexibility allows SOCs to develop tailored strategies and implement customized solutions without being constrained by rigid technology requirements. In addition to evolving threats, standards and regulations also undergo revisions, meaning that SOCs must stay flexible to accommodate emerging regulations and best practices. Adaptability remains a crucial factor for SOCs.

This need for adaptability is particularly important for SOCs for C-ITS, as C-ITS is considered part of a critical infrastructure in which security cannot rely on outdated systems unable to address current and future threats. While the regulations allow for flexibility in technology choices, other SOC operational requirements described in this chapter impose stricter guidelines. The standards outlined in chapter 4.2 and the directives discussed in the present chapter serve as valuable baselines for guiding SOC development, ensuring comprehensive incident management coverage.

Despite Switzerland's federal structure, SOC implementation and operations for C-ITS will not focus on individual cantonal levels to avoid unnecessary complexity. Instead, efforts could be based on the level of territorial units already established by FEDRO, which are consistently used for OT system management across the country. This geographical breakdown could serve as the foundation for SOC implementation in the C-ITS context.

This chapter detailed how these regulations and directives shape SOC responsibilities, including asset management, risk assessment, incident response, and security control implementation in C-ITS environments. The next chapter will translate these regulatory insights into a practical roadmap for SOC development, providing actionable steps drawn directly from the frameworks and guidelines explored here.

4.12 Security Operation Center for C-ITS– Challenges

SOCs around the world play a critical role in safeguarding our digital infrastructure against cyber threats. As cyberattacks are rising and becoming more sophisticated, the increasing challenges that SOC teams face limit their effectiveness. These challenges are described below.

OPERATIONAL CHALLENGES

- **Increasing volume of security alerts:** As the number of security alerts grows each year, analysts spend significant time investigating a deluge of warnings. Unfortunately, this often leads to missed alerts or delayed responses. To optimize their efficiency, SOC teams must find ways to reduce the time between breach detection and resolution. Of course, AI can help in some respects, but in the current state of maturity it is no substitute for SOC members. AI can assist, but not replace analysts or hunters.
- **Complex asset inventory and log gathering:** The C-ITS asset inventory is complex, due to its diverse sources, the mix of OT and IT assets, and its distribution across the country. Log collection is also a challenge, as SOCs must process logs from a variety of technologies, including both legacy and modern systems. Systems may generate logs in different formats, complicating centralized log management. Some legacy systems may not produce any logs at all. Collecting these logs in a readable format is essential for effective monitoring and incident response, requiring tools capable of normalizing data from diverse sources.
- **Complex incident response coordination:** When a security incident occurs, effective coordination among different teams (such as network, application, system administrators and operators of the C-ITS infrastructure) is crucial. SOC teams must ensure seamless communication and collaboration during incident response. And finally, the SOC team must continually improve and learn from incidents.

- **Balancing proactive and reactive approaches:** SOC teams must strike a balance between proactive threat hunting (identifying threats before they escalate) and reactive incident response (handling active incidents). Both are essential for effective security.

RESOURCE AND STAFFING CHALLENGES

- **Shortage of qualified personnel:** The demand for cybersecurity professionals with the necessary skills and practical experience exceeds the supply. Training programs and university curricula do not always match market needs, as they generally lack the practical experience required in real-world cybersecurity operations. Additionally, SOCs typically operate 24/7, requiring staff to work shift schedules. The working conditions to meet those needs may not be attractive.
- **Retaining skilled personnel:** Highly skilled SOC analysts are in demand and retaining them is a challenge. Burnout, stress, and the allure of better opportunities elsewhere contribute to turnover. Organizations must invest in professional development, create a positive work environment, and recognize the efforts of their security teams to retain talent. A "best place" mentality must be established, and the job must remain high-end and technically interesting.

TECHNICAL CHALLENGES

- **Managing a variety of tools:** SOCs rely on an array of security suites, making it challenging to monitor data from various sources effectively. With over 20 technologies in play, tracking and managing each one separately becomes cumbersome. A centralized platform is crucial for successful security operations and incident response. These challenges underscore the need for efficient processes, skilled personnel, and robust tools within SOC environments. By addressing these issues, organizations can enhance their cyber defense capabilities and protect critical assets.
- **Threat intelligence overload:** SOC analysts deal with an overwhelming amount of threat intelligence data from various sources. Filtering relevant information, distinguishing false positives from true threats, and staying up to date with emerging attack vectors can be daunting. In the area of C-ITS SOCs, there are also many niche solutions in use that the analyst does not deal with daily and therefore demand more time spent on investigations and analysis than commodity solutions.
- **Balancing automation and human expertise:** SOCs increasingly rely on automation to handle and speed up the treatment of routine tasks, allowing analysts to focus on complex investigations. However, striking the right balance between automation and human expertise is crucial. Over-automation can lead to false positives, while under-automation may miss critical threats. Finding the sweet spot ensures efficient operations, but requires a never-ending process of fine-tuning, which must also be adapted to possible changes in the entire company structure.

STRATEGIC AND COMPLIANCE CHALLENGES

- **Adapting to evolving threats:** Cyber threats constantly evolve, and attackers become more sophisticated. SOC analysts need to stay ahead by continuously learning about new attack techniques, vulnerabilities, and defense strategies.
- **Budget constraints and rising costs:** Budgets are a perpetual constraint for most businesses, regardless of size. Justifying spending on security operations and incident response can be difficult. Organizations must weigh the essential investment against potential benefits. Quantifying the impact of incidents such as data breaches on brand reputation and financial penalties is a complex task.
- **Compliance and regulatory challenges:** SOC operations must align with industry standards and regulations. Ensuring compliance while maintaining a security posture can be challenging, especially when regulations change frequently. Data protection (nFADP [4]) must also be considered and can make the work more complicated. Another challenge is ensuring compliance with regulations across multiple cantons, as the SOC must adhere to the specific requirements of each canton.

4.13 Demonstrator

In parallel to the current project's activities, the annexed report ***I.a Demonstrator*** describes a demonstrator with the goal of establishing a testing laboratory at ROSAS for analyzing the security of ITS-G5 systems used in V2X communications. The laboratory reproduces real-world V2X scenarios, enabling communication between an RSU, an OBU, and a dedicated hacking box designed to intercept, analyze, and potentially modify ITS-G5 transmissions. The setup utilizes Siemens and Cohda equipment, alongside a suite of software tools (VS-Code, Docker, Wireshark, Ethercap, etc.) to configure, monitor, modify, and analyze network exchanges. The architecture of this demonstrator is represented in *Fig. 26*.

For the purpose of illustrating the detection capabilities considered as key SOC components, a major feature has been developed on top of this demonstrator, integrating an Elastic SIEM solution. The ELK stack (Elasticsearch, Logstash, Kibana) was deployed to collect, centralize, and process logs from all laboratory components. This setup automates log collection and formatting, facilitates real-time threat detection, such as replay attacks and incorrect state transitions, and provides customizable dashboards and alerts for operators. The SIEM thus enhances the laboratory's ability to identify and respond to security incidents in ITS-G5 communications, supporting the development of more robust V2X security practices.

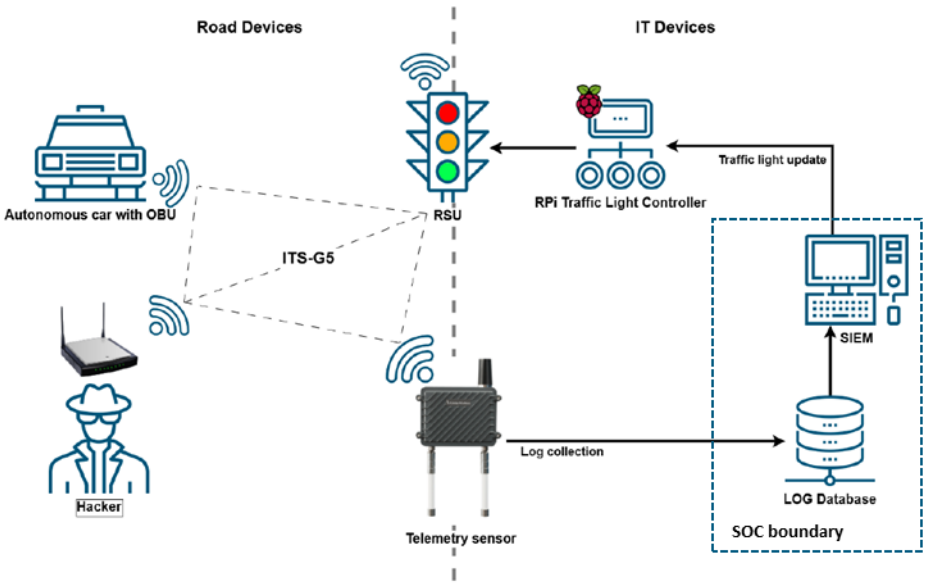


Fig. 26 *ITS-G5 demonstrator.*

5 Swiss SOC for C-ITS – Deployment Strategy

As part of the implementation of a SOC for Switzerland's road infrastructure, a structured approach has been adopted to evaluate different organizational models: an in-house SOC, an outsourced SOC via a MSSP or a hybrid model combining both as described in section 4.10 Security Operation Center – Strategies**.**

To guide this analysis, a multicriteria matrix was developed to assess each option based on key factors such as cost, governance, expertise, flexibility, and operational complexity. Using the MoSCoW prioritization method and weighting inspired by ISO 27005 [38] recommendations, this matrix provides an objective and detailed evaluation of the strengths and weaknesses of each organizational model.

5.1 Multicriteria matrix description

As part of this project's efforts to foresee the implementation of SOC capabilities for Switzerland's road infrastructure, a multi-criteria matrix was developed to evaluate the most suitable organizational structure: In-House, MSSP-based or Hybrid. This matrix considers various criteria:

- **Cost**: Financial implications and level of investment, taking into consideration CAPEX for initial setup and OPEX for ongoing operations;
- **Governance, control and compliance**: The degree of direct oversight, management, and ownership an organization has over its SOC operations, processes, technologies, and alignment with internal policies, procedures, compliance requirements, regulatory and industry-specific standards;
- **Expertise**: The availability and depth of specialized cybersecurity skills and knowledge, including the need for ongoing training and skill development;
- **Customization**: The ability to tailor SOC services and operations to meet specific organizational needs and requirements;
- **Scalability**: The SOC's ability to expand or contract its capabilities and resources in response to changing needs;
- **Time to implement**: How quickly the SOC can be set up and become fully operational;
- **Technology adoption**: The SOC's capacity to integrate and leverage new and advanced technologies;
- **Operational complexity**: The level of difficulty of managing and coordinating the various aspects of SOC operations;
- **Long-Term Flexibility**: The SOC's ability to adapt to evolving threats, organizational changes and technological advancements over time.

Each criterion has been assigned a specific weight to reflect its relative importance in the decision-making process. The detailed description of these weights, along with the rationale supporting their assignment, is provided below. This ensures a structured and objective evaluation of the different SOC implementation strategies.

MoSCoW prioritization and weighting

Each criterion in the multicriteria matrix is assigned to a MoSCoW prioritization level along with a corresponding weighting. The MoSCoW prioritization technique is a widely recognized method for managing requirements, categorizing them into four levels: must-have, should-have, could-have, and will-not-have. This approach allows for clear categorization of the criteria based on their importance and ensures that the SOC structure is chosen while considering the importance of each criterion, some being critical for decision-making, while others have a lower priority.

To incorporate these levels of importance into our multicriteria matrix, specific weights have been assigned to each MoSCoW category. The weighting process follows the scaling recommendations from ISO 27005, which suggest using between 3 and 10 levels to assess asset value based on selected criteria. For our matrix, we opted for a 4-step scale (0,3,7,10)

instead of a linear progression, allowing a more nuanced differentiation between levels of importance, thus providing more clarity in prioritization. The MoSCoW levels and their assigned weightings are presented in *Tab. 35*.

***Tab. 35** MoSCoW levels and weightings*

Weightings	Description
0	The criterion is not considered at all *(will not have)*
3	The criterion is considered as "*good-to-have*"
7	The criterion is a second priority and considered as "*should-have*"
10	The criterion is a first priority and considered as "*must-have*"

After defining each criterion's importance level and its corresponding weighting (0,3,7,10), a separate scoring system (1-4) was introduced to evaluate the extent to which each SOC implementation option (in-house, MSSP, hybrid) meets each criterion.

The four scoring rationales for each criterion were defined by the working group based on their expertise. According to the established scale, a score of 1 represents the lowest evaluation, indicating the least favorable outcome, while a score of 4 corresponds to the highest rating, indicating the most favorable outcome.

By applying this methodology, the working group can systematically assess the effectiveness of each SOC structure in fulfilling the defined criteria.

Tab. 36 provides a detailed summary of the rationale behind each criterion, ensuring transparency and consistency in the evaluation process.

***Tab. 36** Justification of Assigned Scores for Criteria*

Criteria	Rationale
Cost	1: Critical investment with very high costs. 2: Significant investment needed but feasible. 3: Moderate investment, manageable without major effort. 4: Little to no investment required.
Governance, control and compliance	1: Minimal or no control over operations and compliance, difficult to meet regulatory and industry standards 2: Limited control over certain operational aspects, partial compliance with internal or external requirements, or externally managed with potential misalignment 3: High control over most operations and governance, but not complete; compliance achievable with efforts for both internal (governance) and external (regulatory, industry-specific) requirements 4: Complete control and full ownership over all processes, technologies, and governance, full compliance guaranteed with internal policies and regulatory, industry standards
Expertise	1: Critical reliance on advanced expertise and frequent training. 2: Continuous training and skilled personnel regularly required. 3: Occasional training or expertise required. 4: Little to no need for expertise or training.
Customization	1: Customization impossible or negligible. 2: Limited or partial customization. 3: Significant customization possible but with some restrictions. 4: Complete and unrestricted customization.
Scalability	1: Critical resources and major transformation needed. 2: Significant resources required to scale. 3: Moderate resources needed for limited scalability. 4: No additional resources required for scaling.
Time to Implement	1: Critically prolonged time to become operational. 2: Long implementation time but acceptable.

	3: Implementation requires moderate time. 4: Immediate or very fast implementation.
Technology Adoption	1: Critical investment in cutting-edge technologies. 2: Notable investment in advanced tools required. 3: Limited investment or basic tools suffice. 4: No investment or integration needed.
Operational Complexity	1: Involves managing extremely complex and interdependent processes, requiring substantial expertise and effort. 2: Requires regular management of multiple complex processes and technologies. 3: Limited complexity with occasional management of a few processes. 4: No significant complexity to manage, straightforward operations.
Long-Term Flexibility	1: Critical adjustments requiring very high resources. 2: Regular adjustments demanding significant resources. 3: Occasional adjustments requiring minimal resources. 4: No adjustments required.

The final scores of the multicriteria matrix are calculated by combining the selected rationale score (1-4) with the MoSCoW weight of the criterion (0,3,7,10), resulting in a value representing both the importance of each criterion and the effectiveness of each SOC option in meeting the criterion.

The objective of this approach is to identify the SOC structure with the highest overall score to ensure the best strategic choice.

5.2 Multicriteria matrix results

The multicriteria matrix was filled out individually by the members of the working group to obtain diverse scores along with explanations of the scoring from various perspectives. To enhance the robustness of our evaluation, each member considered specific factors and nuances relevant to their expertise, ensuring a well-rounded and comprehensive assessment.

Tab. 37, *Tab. 38* and *Tab. 39* summarize the different results obtained for each SOC structure. The analyses conducted by each member are provided in appendix I.c Multicriteria matrix.

***Tab. 37** In-House SOC multicriteria matrix results*

Criteria	Average score	Explanation of results
Cost	1	The working group's assessment indicates that the In-House SOC structure demands critical investment and very high costs. The key aspects highlighted in the descriptions include: • High CAPEX and OPEX requirements, with continuous cost burdens over time. • Significant investment in infrastructure, tools, and skilled personnel. • Internal staffing and training needs leading to increased expenses. • Long-term operational costs making the SOC a continuous financial commitment.
Governance, control and compliance	3.8	The assessment highlights a strong capability for control and compliance within an In-House SOC. Key takeaways include: • The organization has complete control over all SOC processes, policies, procedures, and technologies, allowing for full alignment with internal governance frameworks and industry regulations. • Direct control over data and processes allows for quick decision-making. However, integrating compliance requirements within the organization can be a long and complex process. • The ability to build a tailored SOC from the start ensures seamless integration with governance frameworks, security policies, and industry compliance standards.

		• Critical data stays in-house.
Expertise	1	The evaluation suggests that the in-house SOC heavily relies on advanced expertise and frequent training to maintain effective operations. Key insights from the descriptions include: • A significant baseline of knowledge is required for all activities, with internal resources driving all efforts. • As an in-house operation, the expertise should primarily be internal, though consulting may be considered as a starting point. • Skilled cybersecurity professionals are essential, along with regular training to keep up with evolving threats. • Continuous training is vital in a rapidly changing cybersecurity landscape to maintain a high level and up-to-date competence. • The in-house SOC model demands skilled professionals who must be continually trained to stay ahead of emerging risks.
Customization	4	The evaluation suggests that the in-house SOC provides complete and unrestricted customization, offering significant flexibility. Key insights from the descriptions include: • Full control over all processes, including policies, procedures, playbooks, tooling, and implementation strategy, enabling the SOC to be tailored to the organization's specific needs. • Complete autonomy in decision-making and adjustments, allowing for rapid responses to evolving requirements. • High flexibility in aligning security operations with organizational goals, ensuring that every aspect of the SOC is customized to meet internal demands.
Scalability	2	The evaluation suggests that scaling the in-house SOC requires significant resources, particularly in terms of staffing and infrastructure. Key insights from the descriptions include: • Technical scaling is possible but limited by the capacity of existing personnel, requiring additional staff to handle increased workloads. • Expanding the SOC's capabilities demands substantial investments in both human resources and infrastructure. • Scaling human resources is particularly challenging, as it involves hiring and training additional staff to meet increased demand.
Time to Implement	1.2	The evaluation suggests that implementing the in-house SOC will take a prolonged amount of time. Key insights from the descriptions include: • Full implementation is the organization's responsibility, with the need to establish every aspect, leading to a prolonged setup time. • The implementation is complex, requiring extensive internal resources, which results in a slow process to become fully operational. • Although the overall implementation takes considerable time, initial use cases can be productive within a shorter timeframe.
Technology Adoption	1.8	The evaluation suggests that adopting advanced technologies for an in-house SOC requires significant investment. Key insights from the descriptions include: • Investment is needed for technology benchmarking, pilot deployment, and pushing to production to ensure effective integration of cutting-edge tools. • While the possibilities for technology adoption are vast, significant investment in advanced tools is required to maximize efficiency and meet critical infrastructure needs. • To be fully effective, the SOC must invest in and integrate advanced cybersecurity tools, making it a key aspect of its operational strategy.
Operational Complexity	1.2	The evaluation suggests that managing an in-house SOC involves significant complexity and requires substantial expertise. Key insights from the descriptions include: • Full control over end-to-end processes, including policies, procedures, playbooks, tooling, and implementation strategy, increases the complexity of operations. • The need for internal knowledge and expertise requires substantial investment and makes the management of operations more intricate.
Long-Term Flexibility	2.4	The evaluation suggests that while long-term flexibility is achievable, it requires regular adjustments and significant resources. Key insights from the descriptions include: • Full control over end-to-end processes allows for continuous improvement and standard maintenance, which supports flexibility but requires ongoing effort.

	• The SOC owner is responsible for continuous improvement, providing a clear roadmap for the future, meaning flexibility is manageable with normal resources. • Regular adjustments are necessary to stay current with evolving threats, but these adjustments are time-consuming and staff-intensive since all modifications are handled in-house. • While flexibility is generally good, "vendor lock-in" with certain products can limit adaptability, and adjusting strategies or technologies can be resource-intensive.

***Tab. 38** MSSP SOC multicriteria matrix results*

Criteria	Average score	Explanation of results
Cost	2.4	The evaluation suggests that while costs are still a factor, they are more manageable compared to an in-house SOC. Key insights from the descriptions include: • Moderate to major initial investment (CAPEX), followed by moderate to major ongoing operational costs (OPEX). • Lower employee costs, making it a more viable option for government entities. • Service fees as the primary cost driver, reducing the burden of hiring and maintaining an in-house team. • Cost-effectiveness, as outsourcing security operations is generally more affordable than developing and running an internal SOC.
Governance, control and compliance	2	The assessment highlights significant limitations in governance and compliance when relying on a Managed Security Services Provider. Key insights include: • Organizations must rely heavily on the MSSP's compliance capabilities, which can introduce risks related to non-conformities, lack of visibility, and reduced control over outsourced activities. Strong supplier management and audit practices are essential. • Compliance with Swiss legislation or other regulatory frameworks depends entirely on selecting an MSSP that meets these requirements. If a compliant provider is found, compliance can be ensured; otherwise, major risks arise. • Governance synchronization between the customer and MSSP can be complex, and while compliance is typically managed by the provider, ensuring alignment with internal policies and specific regulatory frameworks remains a challenge. • Some data may have to be anonymized before being handed out to the MSSP, due to different laws or privacy concerns.
Expertise	3.6	The evaluation suggests that while expertise is still required, it is largely managed externally by the MSSP. Key insights from the descriptions include: • The responsibility for expertise is transferred to the MSSP, with the internal team relying on the Service Level Agreement (SLA) to ensure the required skills are delivered. • The MSSP provides its own dedicated team of professionals, bringing specialized expertise and experience, minimizing the need for internal training or development. • While some minimal knowledge is required internally to communicate effectively with the MSSP, the heavy reliance on the provider means less focus on ongoing internal training. • The MSSP leverages external experts with industry-wide experience, ensuring the organization benefits from the latest cybersecurity expertise.
Customization	2	The evaluation suggests that while some customization is possible, it is limited by the capabilities and offerings of the MSSP. Key insights from the descriptions include: • The level of customization is largely dependent on the MSSP's capabilities, and while almost everything can be customized under certain conditions, cost constraints may limit this flexibility. • There is negligible control over the customization process as the MSSP typically offers its own standardized solutions, and customization is primarily dependent on the provider’s willingness. • While some customization is possible, it is still limited in comparison to the flexibility offered by an in-house SOC.
Scalability	3.6	The evaluation suggests that the MSSP SOC provides good scalability with moderate resource requirements. Key insights from the descriptions include:

		• MSSPs typically offer cloud-based solutions that support a wide range of products, allowing for on-demand increases in capacity and scalability, although costs may be a factor. • The scalability of the SOC is managed by the MSSP, meaning that the responsibility for expanding or contracting resources lies with the service provider. • Since the MSSP handles all SOC capabilities, scalability is seamless and does not significantly impact internal resources or operations. • The service provider can easily scale up or down to accommodate organizational growth or changes, offering flexibility without major challenges.
Time to Implement	3.2	The evaluation suggests that the implementation time for an MSSP SOC is moderate and achievable within a reasonable timeframe. Key insights from the descriptions include: • The implementation time for an MSSP SOC is generally moderate, with pilot projects achievable in a reasonable timeframe, influenced by the existing infrastructure knowledge. • Utilizing pre-configured solutions, expert teams, and operational services, the MSSP model enables a quicker setup compared to building an in-house SOC from scratch.
Technology Adoption	3	The evaluation suggests that while some investment in advanced technologies is needed, much of the technology adoption is handled by the MSSP. Key insights from the descriptions include: • The MSSP has already implemented the necessary technologies, and the investment required for technology adoption is focused on benchmarks, pilot deployments, and pushing to production. • The service provider possesses specialized tools and technologies, which are continually evolving, reducing the need for client-side investments in cutting-edge technologies. • Technology adoption is primarily managed by the MSSP, with minimal client-side involvement, though minor adjustments may be required for alignment with the organization's processes. • The MSSP offers access to advanced cybersecurity technologies, ensuring that the SOC benefits from the latest tools without requiring significant internal investment. • MSSPs are well established in the IT ecosystem. However, OT MSSPs are not common yet.
Operational Complexity	3.2	The evaluation suggests that the operational complexity is relatively low, as the MSSP takes on most of the tasks. Key insights include: • The MSSP handles the majority of operational tasks, with the client's involvement limited to alignment and risk management, significantly reducing operational complexity. • The service provider manages most complexities, leaving the client with only minimal management responsibilities. • Outsourcing the SOC to the MSSP reduces the operational burden on internal teams, simplifying coordination and day-to-day operations.
Long-Term Flexibility	3.2	The evaluation suggests that while some flexibility is available, adjustments to the MSSP SOC are generally manageable with minimal resources. Key insights include: • MSSPs often provide cloud-based solutions that can support diverse product fleets and scale on demand, offering flexibility under cost conditions. • Adjustments to keep up with evolving threats are managed by the MSSP, with minimal effort required from the client side, though changes in contracts or switching providers may involve complexity. • While the service provider manages flexibility, vendor lock-in and contract modifications can limit long-term adaptability, making significant changes more challenging.

***Tab. 39** Hybrid SOC multicriteria matrix results*

Criteria	Average score	Explanation of results
Cost	2	The analysis suggests that while the costs are significant, they remain feasible compared to a fully in-house model. Key insights from the evaluation include: • A hybrid approach requires investment in both internal staff and MSSP services, leading to costs on both fronts but offering flexibility in resource allocation over time.

		• The balance between in-house infrastructure and outsourced functions results in a mix of CAPEX and OPEX, making cost distribution more complex yet more manageable than a fully in-house SOC. • While initial investments are lower than an in-house SOC, ongoing service costs remain a primary financial consideration, requiring strategic cost management.
Governance, control and compliance	3	The assessment highlights that while a Hybrid SOC provides a high degree of control, it does not guarantee full ownership due to outsourcing. Key insights include: • Governance and compliance are dictated by service-level agreements (SLAs) with MSSPs. Control handover requires effort but is manageable with well-structured contracts. However, misalignment between customer and provider governance requirements can introduce challenges. • The in-house portion allows for adaptable governance, but compliance for outsourced functions requires additional coordination and effort. Aligning external compliance with internal governance baselines can be complex. • The Hybrid SOC model reduces concerns related to data protection and ownership compared to a fully outsourced SOC, as critical security functions remain under internal control while leveraging external compliance support.
Expertise	2.4	The evaluation highlights that maintaining expertise is a key challenge, as it requires both internal capabilities and reliance on external specialists. Key insights from the assessment include: • Hybrid SOCs require continuous training for internal staff to manage in-house operations effectively while leveraging external expertise for outsourced functions. • A balance must be maintained between in-house knowledge and external support, ensuring a shared understanding between internal teams and MSSP partners. • Organizations must invest in building critical cybersecurity expertise internally while also relying on service providers for specialized capabilities.
Customization	3	The evaluation indicates that while significant customization is possible, some limitations arise due to the coexistence of in-house and outsourced services. Key insights include: • Hybrid SOCs offer flexibility, allowing organizations to define customization thresholds when selecting an MSSP, ensuring alignment with internal needs. • Partial customization is achievable, but maintaining compatibility between in-house operations and managed services may introduce constraints. The involvement of multiple stakeholders requires well-structured agreements with external partners.
Scalability	2.8	The evaluation suggests moderate scalability capabilities, with the flexibility to adjust both in-house and outsourced functions. Key insights include: • Scalability is shared between internal teams and MSSP partners, allowing for adaptability but requiring additional resource planning. • While MSSPs can scale their services easily, scaling internal human resources may pose challenges and require strategic workforce adjustments.
Time to Implement	2.4	The assessment suggests a moderate to long implementation time due to the need to integrate both in-house and outsourced components. Key insights include: • Initial reliance on MSSP partners can accelerate short-term setup, but long-term internal capability building will require time. • The process of aligning internal expertise with external service providers adds complexity, extending the overall implementation timeline. • While outsourcing reduces some implementation burdens, effective integration of both in-house and MSSP functions remains a time-consuming process.
Technology Adoption	2.6	The assessment highlights a notable but manageable investment in technology adoption. Key insights include: • Initial reliance on MSSP partners ensures a solid technological foundation, with an iterative shift toward internal adoption over time. • To maintain scalability and efficiency, continuous investment in advanced tools is necessary to avoid technological bottlenecks. • While MSSP providers handle a portion of technology adoption, internal teams must stay aligned to ensure seamless integration, which may impact operational processes. • The hybrid model allows organizations to leverage both in-house and MSSP-provided technologies, ensuring access to advanced cybersecurity solutions.

Operational Complexity	2.6	The assessment highlights moderate complexity due to shared responsibilities between internal teams and MSSP providers. Key insights include: • The initial reliance on MSSP for foundational processes reduces complexity, but transitioning activities in-house over time introduces additional coordination challenges. • The critical aspect of complexity stems from the need to establish and maintain seamless integration between in-house operations and the MSSP, ensuring effective and precise communication, as well as proper process alignment. • Managing interdependencies between internal teams and the MSSP adds a layer of operational difficulty, particularly for critical security functions handled in-house. • Overall, while the hybrid model reduces some operational burdens, it introduces new challenges in governance, coordination, and role delineation between both stakeholders.
Long-Term Flexibility	3.2	The evaluation highlights a relatively high degree of adaptability, though some constraints exist. Key insights include: • The Hybrid SOC benefits from flexible contractual agreements with MSSP partners, preventing major technological or procedural lock-ins and allowing for adjustments when needed. • The main limitation to flexibility lies in modifying the MSSP scope, which may introduce contractual complexities or delays in implementing changes. • Adaptation to evolving threats is a continuous process, but leveraging both internal expertise and external MSSP resources reduces complexity while maintaining responsiveness. • The model provides strong flexibility by allowing organizations to adjust the balance between in-house and outsourced functions as requirements evolve, ensuring long-term adaptability.

In summary, this analysis compares three SOC models, In-House, MSSP, and Hybrid, by evaluating their strengths and weaknesses across key criteria such as cost, governance, expertise, scalability, customization, and operational complexity. Each model presents specific trade-offs between control, flexibility, and investment, allowing organizations to choose the most suitable solution for their cybersecurity needs.

- The **In-House SOC** provides maximum control (3.8) over governance, compliance, and customization (4.0), allowing for full alignment with internal security frameworks and regulatory requirements. However, it comes with extremely high costs (1.0) due to significant CAPEX and OPEX investments in infrastructure, staffing, and continuous training. Expertise is a major challenge (1.0), requiring a highly skilled internal team with ongoing education to maintain operational effectiveness. Scalability (2.0) is resource-intensive, as expanding the SOC demands hiring and training additional personnel. Technology adoption (1.8) and operational complexity (1.2) are also major challenges, requiring substantial investment and expertise. Implementation time (1.2) is long due to the need to build everything from scratch, while long-term flexibility (2.4) is achievable but requires continuous adaptation efforts. Despite its resource demands, the in-house model is the best option for organizations prioritizing full control, customization, and governance adherence.
- The **MSSP SOC** offers cost-effective security operations with strong expertise (3.6) and high scalability (3.6) due to its reliance on external providers, but it presents challenges in governance and compliance (2.0) as organizations must depend on the MSSP's regulatory adherence. Customization (2.0) is limited due to standardized solutions, while long-term flexibility (3.2) is constrained by contractual obligations. Technology adoption (3.0) and operational complexity (3.2) are manageable, as MSSPs handle most tasks. Implementation is moderate in complexity (3.2) but offers a quicker setup than in-house solutions.
- The **Hybrid SOC** balances internal control (3.0) with outsourced efficiencies, ensuring some governance and compliance (3.0) while maintaining long-term flexibility (3.2) through adaptable contracts. Cost (2.0) remains a factor due to dual investments in internal teams and external services. Customization (3.0) and technology adoption (2.6) are feasible but require coordination between in-house and outsourced components. Operational complexity (2.6) and implementation time (2.4) are moderate due to integration efforts, while scalability (2.8) is achievable with proper planning. Expertise remains a challenge (2.4) as organizations must develop internal knowledge while relying on external specialists.

By multiplying the weight assigned to each criterion by the scores given by each member of the working group (WG) who completed the multicriteria matrix, the results (summarized in *Tab. 40*) indicate that the "In-House SOC" is the least favorable option and can be eliminated from consideration. The results for the "MSSP SOC" and "Hybrid SOC" are very close, suggesting that the best approach would be to outsource as many activities as possible to the MSSP while maintaining internal expertise to make informed decisions on critical security events. This balance ensures cost efficiency, scalability, and access to specialized expertise while retaining strategic control over key cybersecurity operations.

Tab. 40 *Multicriteria matrix results comparison*

SOC Structure	WG Person #1	WG Person #2	WG Person #3	WG Person #4	WG Person #5	Average
In-House	122	122	118	115	115	**118,4**
MSSP	162	190	183	193	179	**181,4**
Hybrid	179	129	146	176	183	**162,6**

In conclusion, based on the results of the multicriteria matrix, the working group believes that implementing a national in-house SOC presents several major challenges that make this approach less suitable compared to an outsourced or shared solution. The key limitations and constraints are summarized below:

- **Budgetary constraints and human resources**: An in-house SOC requires significant investments in infrastructure, monitoring software, and skilled personnel. Recruiting and retaining cybersecurity experts is a major challenge in Switzerland, where the demand for these skills exceeds the available workforce. A federal office may struggle to maintain a 24/7 team capable of responding effectively to security incidents;
- **Technological complexity and operational maintenance**: Cyber threats evolve rapidly, requiring constant updates to detection technologies and methodologies. Managing an in-house SOC means handling advanced security tools (SIEM, EDR, SOAR, threat intelligence, etc.), which demands continuous expertise and a substantial budget to ensure effective and up-to-date protection;
- **Information sharing and threat intelligence**: A federal SOC must have a comprehensive view of threats targeting various public administrations. Operating in isolation, an in-house SOC would limit its ability to share and receive threat intelligence with other entities, such as the NCSC other federal offices, or international partners. A shared approach would enhance coordination and responsiveness to cyberattacks;
- **Resilience and scalability**: An in-house SOC may face limitations in resilience against sophisticated attacks (DDoS, targeted ransomware, etc.). In the event of a major crisis, a federal office might lack the capacity to handle the increased load and respond effectively. An outsourced or shared SOC solution would provide greater flexibility and scalability, allowing for rapid adjustments based on evolving threats.

The most suitable solution is therefore a hybrid approach with extensive support from an MSSP. For example, a federal office could implement a hybrid SOC in which sensitive incident management is handled by an internal team, while global threat detection and monitoring are entrusted to an external provider.

Below are some examples of MSSPs:

- **Swisscom** [70]: As the leading telecommunications service provider in Switzerland, Swisscom offers Security Analytics and Security Operations Center (SOC) as a service. These solutions enable businesses to outsource security incident analysis and management, providing continuous monitoring and specialized expertise to safeguard their infrastructures;
- **ELCA Security – Senthorus** [71]: Senthorus, operated by ELCA Security, is a next-generation SOC based in Geneva. It provides 24/7 threat detection and response services, leveraging advanced technologies and local expertise to protect businesses' digital perimeters;

- **terreActive** [72]: Based in Switzerland, terreActive offers a Security Operations Center dedicated to protecting its clients' IT infrastructures. Their SOC provides continuous monitoring and preventive measures against cyber threats, ensuring the availability and security of critical business networks and applications;
- **Kudelski** [73]: Kudelski Security provides managed security services with continuous monitoring, threat intelligence, and incident response. With its international headquarters in Geneva and an office in Adliswil, Switzerland, Kudelski offers tailored solutions and expert support to help businesses mitigate cyber threats and enhance their security posture in real time.

5.3 Deployment description

Implementing an SOC requires careful planning and strategic deployment to ensure efficiency and effectiveness. Several approaches can be adopted to implement an SOC, depending on the organization's priorities and requirements. Three primary deployment methods have been identified: geographical, technological, and capability-based.

5.3.1 Geographic deployment

Geographic deployment focuses on identifying key physical locations where the SOC should initially concentrate its efforts. This approach is particularly useful for organizations with multiple sites, global operations, or varying levels of cybersecurity risk across regions. The deployment may begin in high-risk areas, critical infrastructure locations, or specific operational hubs before expanding to other locations. Geographic deployment allows for a phased approach, ensuring that security operations are efficiently distributed according to the most pressing needs. Additionally, having a BOM listing the necessary hardware and equipment is crucial to ensure a smooth and efficient deployment process.

An SOC can be deployed in a geographic approach, progressively expanding its coverage from urban areas to national road networks. *Fig. 27* is a visual example of a geographic deployment:

- 1st Phase – City road infrastructure
    - The SOC is initially deployed at the urban level, securing critical road infrastructure such as intersections, connected traffic lights, and RSU sensors;
    - The focus is on real-time monitoring to prevent local cyber threats, such as intrusions, DoS attacks on traffic management systems, and sensor data tampering.
- 2nd Phase – Cantonal road infrastructure
    - Once urban security is stabilized, the deployment expands to canton-level roads, incorporating a broader network of sensors and V2X communication stations;
    - At this stage, the SOC enhances threat intelligence, aggregates traffic data, and correlates incidents across multiple cities to detect coordinated cyberattacks.
- 3rd Phase – Swiss road infrastructure
    - Finally, the security monitoring infrastructure extends to the national road network, integrating advanced security systems on a country-wide scale;
    - At this level, the SOC manages large-scale cybersecurity operations, leveraging AI-driven threat analysis, automated response mechanisms, and national-level collaboration to ensure road network resilience.

***Fig. 27** Geographic deployment example.*

Other examples of geographic deployment:

- **Crossing with traffic lights:** Sensors and connected systems in a city center, especially those involved in traffic management;
- **Connected infrastructure of a motorway tunnel:** Monitoring of critical systems, such as cameras, smoke detectors, air sensors, or connected digital signs;
- **Smart Cities:** Deployment of SOC operations to oversee public infrastructure, IoT networks, and emergency response systems.

5.3.2 Technology deployment

Technology deployment involves selecting a specific type of sensor or monitoring device and implementing all the necessary SOC components to support it. This method ensures a structured approach, integrating security tools, data processing capabilities, and incident response workflows around a well-defined technology. The deployment includes sensor integration, data collection, correlation analysis, and incident response mechanisms.

An SOC can be deployed using a technological approach, gradually integrating various road infrastructure components and sensors. *Fig. 28* is a visual example of a technological deployment:

- 1st Phase – Traffic light RSU
    - The initial phase focuses on deploying and securing RSUs integrated into traffic lights, which enable V2I communication and real-time traffic data exchange;
    - The SOC monitors for cyber threats such as unauthorized access attempts, data interception, jamming attacks, and communication disruptions targeting RSUs.
- 2nd Phase – Surveillance camera
    - In the second phase, surveillance cameras are introduced to enhance visual monitoring of road infrastructure;
    - The SOC tracks cyber threats such as unauthorized camera access, tampering attempts, video feed hijacking, and malware injection that could compromise surveillance integrity.
- 3rd Phase – Smoke detector
    - The final phase integrates smoke detectors, expanding the SOC's monitoring capabilities to include environmental and safety-related threats;
    - The SOC detects cyber threats such as sensor spoofing, false alarm generation, and system disablement, ensuring that smoke detectors remain operational and reliable in emergency situations.

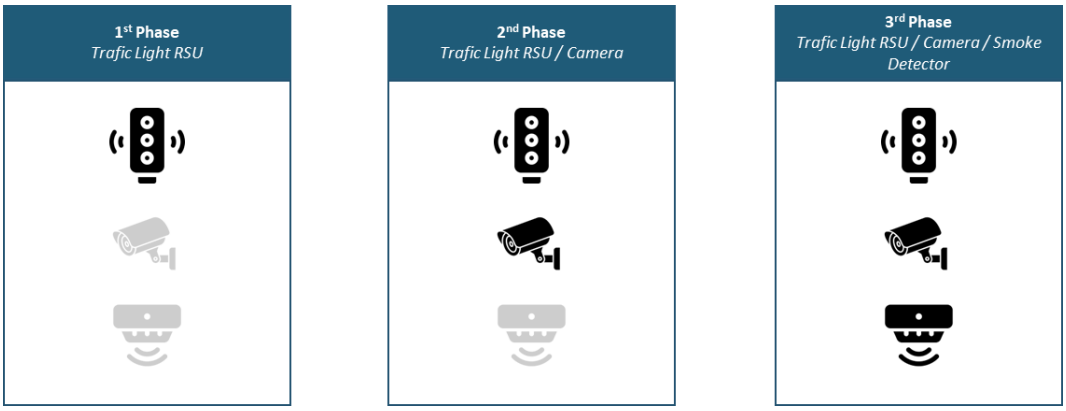


Fig. 28 *Technological deployment example.*

Examples of RSU technology deployment:

1. **Selection and installation:** Deploy RSU sensors at strategic locations to monitor vehicle and traffic data;
2. **Data collection & transmission:** Ensure real-time transmission of collected data to a central processing system;
3. **Integration with SIEM:** Connect RSU data to a SIEM system for analysis;
4. **Anomaly detection:** Use (AI-driven) analytics to identify unusual patterns, such as unauthorized access or potential cyber threats;
5. **Incident response mechanism:** Establish automated alerting and escalation processes for rapid mitigation of detected security events;
6. **Lessons learned and continuous improvement:** Regularly assess security incidents and system performance to identify gaps, refine detection mechanisms, and enhance SOC efficiency based on real-world insights.

5.3.3 Capability deployment

Capability deployment is structured around the gradual implementation of SOC functionalities based on priority needs. This method involves rolling out SOC services in phases, starting with critical functions such as threat monitoring, incident detection, or response coordination. By prioritizing capabilities, organizations can establish a foundational security posture before expanding to more advanced functions such as threat intelligence, forensic analysis, or automated response mechanisms. This deployment strategy allows for flexibility and scalability, adapting to evolving security threats and business needs.

Examples of capability deployment:

- **Real-time incident monitoring:** Implementation of SIEM tools to monitor threats 24/7, providing immediate detection and alerts;
- **Vulnerability management:** Proactive analysis of systems and networks to detect security flaws, ensuring timely remediation before exploitation;
- **Incident response:** Establishing a dedicated incident response team to prioritize the mitigation of cyber-attacks on critical areas or technologies, ensuring rapid containment and recovery.

An SOC can be deployed using a phased capability-based approach, gradually enhancing its ability to collect data, detect anomalies, and respond to incidents. *Fig. 29* is a visual example of a capability deployment:

- 1st Phase – IDENTIFY
    - The first phase establishes basic data collection capabilities, enabling the SOC to gather and centralize information from various sensors and infrastructure components;
    - At this stage, anomaly detection and incident response are not fully integrated, but initial data insights help lay the foundation for future cybersecurity monitoring.

- 2nd Phase – DETECT
  - In the second phase, anomaly detection mechanisms are activated, allowing the SOC to analyze collected data and identify potential cybersecurity threats such as unauthorized access, unusual traffic patterns, or system anomalies;
  - Incident response capabilities remain limited, with a primary focus on monitoring and threat identification.
- 3rd Phase – RESPOND
  - The final phase introduces full incident response capabilities, enabling the SOC to proactively mitigate detected threats and react to security incidents in real time;
  - At this stage, the SOC operates as a fully functional cybersecurity defense system, leveraging data collection, anomaly detection, and automated response mechanisms to ensure infrastructure resilience.

***Fig. 29** Capability deployment example.*

5.4 Deployment results

The chosen deployment strategy combines technology and geographic deployment methods, with a focus on covering all capability phases from the start. This hybrid approach ensures quick initial operating capability while providing comprehensive SOC activities from the start and a manageable scope.

Technology deployment

The initial deployment will focus on a single technology (Phase 1). By concentrating on a specific technology – such as traffic light RSU, surveillance cameras, or smoke detectors – the SOC can optimize data integration, collection, processing, monitoring, and incident response processes. Future phases will integrate additional technologies.

This aligns with recent attacks on individual C-ITS technologies. Focusing initially on a single technology enables the SOC to deal with relevant real-world threats and to quickly optimize its security processes for the most immediate risks.

Geographic deployment

The initial deployment will be set in an urban area (Phase 1). Expansion to broader geographic areas (canton-level in Phase 2 and national-level in Phase 3) will occur in the next phases. Local deployment enables easier management in the beginning.

This phased approach matches typical C-ITS rollouts, where systems are deployed in limited defined contexts.

Capability deployment

Unlike the phased approach in technology and geographic deployments, all three capability phases – Identify, Detect, Respond - will be covered from the start. This comprehensive

capability approach ensures a strong foundational security posture and immediate operational value.

Benefits of the chosen strategy

The chosen strategy, shown in *Fig. 30*, allows for quick initial operating capability. It also enables easy scalability in both technology integration and geographic coverage, as the SOC matures. The comprehensive capability approach ensures that critical security functions are in place from the beginning, reducing the risk of undetected or unaddressed security threats during the next deployment phases. The focused initial deployment allows for easier adjustments and refinements to the SOC solution as it starts “small” and not on a wide scale. Furthermore, as the SOC will provide full capability coverage in the first operating phase, it can quickly demonstrate its value and generate insights for future expansions.

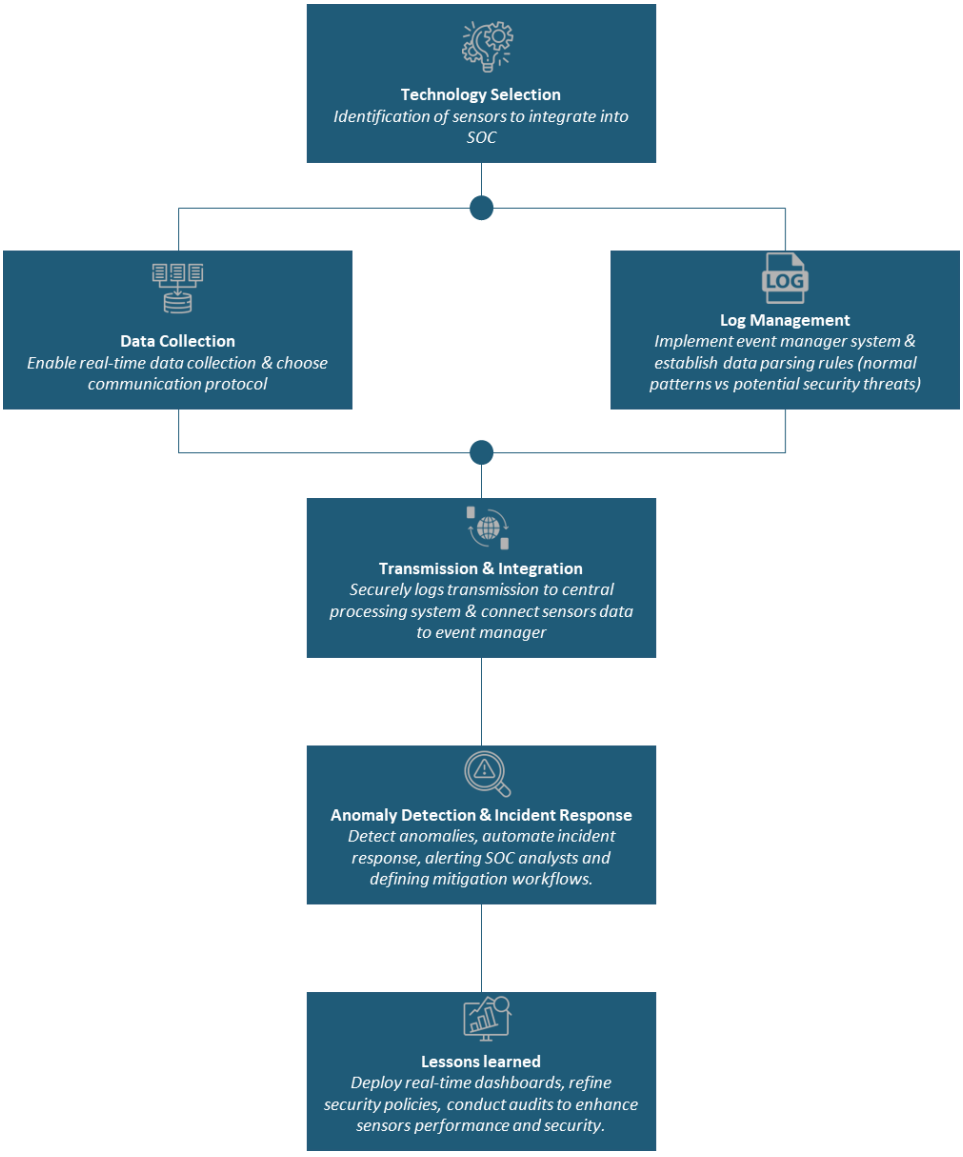


Fig. 30 *Deployment strategy example.*

6 Swiss SOC for C-ITS – Roadmap phases

Setting up an SOC is a complex task. The roadmap phases provide a structured approach to ensure effective implementation. Two key references were used in the development of this roadmap: ENISA's report "How to Setup CSIRT and SOC" [43], which provides results-oriented guidance for setting up a CSIRT or SOC by analyzing existing literature, conducting field research and drawing on real-world implementation experience, and "11 Strategies of a World-Class Cybersecurity Operations Center" [65], which offers valuable insights into the foundational steps of building an SOC.

The Swiss SOC roadmap follows five phases, with initial operating capabilities estimated after 18 months of development, as shown in *Fig. 31* below.

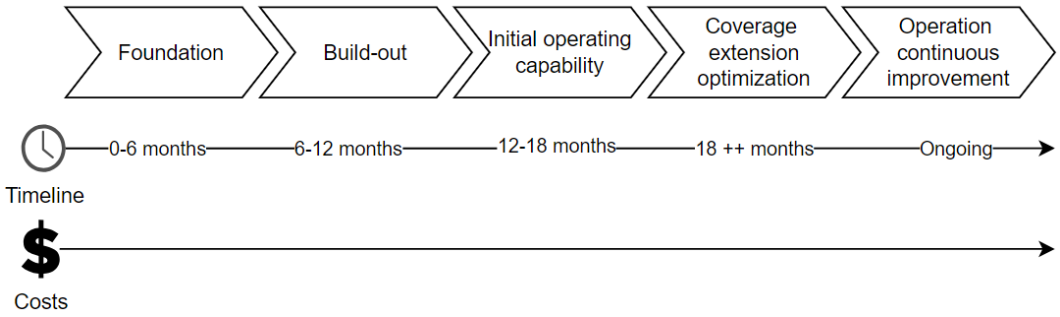


***Fig. 31** SOC five phase roadmap.*

Foundation

This phase lays the base for the SOC. The focus is on ensuring foundational elements are in place by addressing strategic, governance and resource-based aspects. It involves defining the mission, objectives and key stakeholders, conducting a needs assessment and securing initial funding and resources. In addition, high-level requirements and policies are defined.

Build-out

During this phase, the physical and technical infrastructure of the SOC is set up. This includes setting up the SOC facility, acquiring and deploying the necessary tools, defining operational processes, deploying the chosen initial technology and establishing basic capabilities. Another important part of this phase is the creation and management of the C-ITS asset inventory. The process of identifying and cataloguing assets begins here and continues as the SOC is developed in subsequent phases.

Initial operating capability

During this phase, the SOC reaches its initial operating capability and delivers SOC services. It completes phase 1 technology deployment (focused on a single technology), phase 1 geographic deployment (urban area) and full capabilities for capability deployment (Identify, Detect, Respond). At the end of this phase, the SOC is operational and capable of managing security incidents prior to large-scale deployment. Mandatory reporting capabilities are also implemented in this place.

Coverage extension optimization

During this phase, the SOC's coverage is extended to broader geographic areas and integrates additional technologies. It also focuses on optimizing SOC operations (processes), as well as inter-organizational collaboration and information sharing, e.g., for threat intelligence.

Operation continuous improvement

The final phase focuses on continuous improvement of SOC operations. It involves regular reviews, updates, and enhancements to ensure the SOC remains effective and adapts to evolving security threats.

6.1 Phase 1 – Swiss SOC for C-ITS foundations

This initial phase lays the base for the SOC. It focuses on ensuring foundational elements are in place by addressing the strategic direction, governance framework, risk management approach, resource planning and financial considerations required to build an SOC. It also ensures that all key stakeholders are identified and onboarded. Initial processes are developed, tool requirements are identified, and key human roles are filled during this phase.

6.1.1 Objectives & outcomes

Fig. 32 summarizes the key objectives and expected outcomes of this phase. Detailed explanations of the processes involved are provided in the sections below.

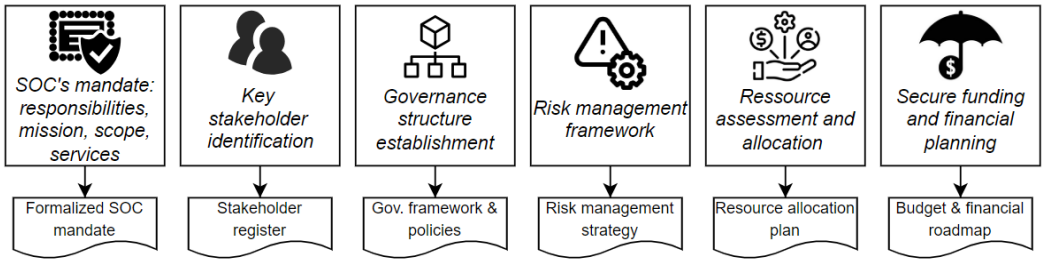


***Fig. 32** Roadmap phase 1 objectives and outcomes.*

Phase duration: approx. 6 months

Total phase cost: approx. 234’000 CHF

6.1.2 Detailed processes

SOC’s mandate: responsibilities, mission, scope and services

What: Establish a formal mandate of the Swiss SOC, detailing its mission, scope, main responsible parties and service offerings.

Resources: [4.1 SOC organization] [5.4 Deployment results]

Who: The hosting organization, MSSP, key stakeholders, legal counsel

How:
1. Conduct collaborative stakeholder workshops;
2. Draft the mandate document, containing:
    a. Justification for the SOC: Define the need for an SOC. Outline the expected benefits;
    b. Responsibility assignment: Define roles and responsibilities for the hosting organization and the MSSP, using a RACI matrix;
    c. Mission and operational scope: Define the SOC’s high-level objectives, identify the operational scope. Document key SOC activities and services.
3. Implement formal approval processes.

Expected outcome: A well-defined SOC mandate encompassing its mission, responsibilities (RACI matrix: Responsible – execution, Accountable – final authority, Consulted – provides input, Informed – kept updated), operational scope, and key activities and services.

Key stakeholder identification

What: Identification of key stakeholders influencing SOC operations, along with the establishment, maintenance, and facilitation of communication and collaboration throughout its development/operation.

Resources: [4.4 Core function - IDENTIFY]

Who: Representatives from the hosting organization, government agencies, industry partners, MSSP

How:
1. Identification and mapping of all relevant stakeholders, including government, private sector, other SOCs and industry partners. The list will probably include NCSC teams and the 11 UTs from cantons;
2. Conduct workshops with stakeholders to gather input on their role and define their interactions with the SOC;
3. Establish communication channels and contact points to facilitate information sharing.

Expected outcome: A comprehensive stakeholder register with defined roles, interaction types with the SOC and established communication channels.

Governance structure establishment

What: Definition of the organizational structure, policies and procedures that govern the SOC's operations, focusing on the GOVERN function as described by the NIST.

Resources: [4.3 Core function - GOVERN] [4.9 SOC – Human factors]

Who: SOC leadership, hosting organization representatives

How:
1. Establish the SOC leadership roles (e.g., SOC manager, CISO, Risk Manager);
2. Develop a governance framework outlining the SOC's organizational structure, roles, responsibilities, reporting lines;
3. Develop core governance processes and cybersecurity policies;
4. Develop/Improve an OT and information security management plan adhering to industry good practices, e.g., ISO 27001 [36], ISA/IEC 62443-2-1 [25]

Expected outcome: An established governance structure, with defined roles, responsibilities, governance processes and cybersecurity policies.

Risk management

What: Develop a risk management framework aligned with the SOC's objectives and operational priorities in the C-ITS environment.

Resources: [MB4_20_02C_01 – Cyber Threat Intelligence Framework and Recommendations for C-ITS [41]] [3.3 Approaching C-ITS with the MITRE ATT&CK framework [44]] [4.3 Core function - GOVERN] [4.4 Core function - IDENTIFY]

Who: Risk manager, SOC leadership

How:
1. Define risk appetite and acceptance criteria: identify acceptable risk levels for different SOC functions;
2. Develop risk management framework: define risk identification, assessment and mitigation technologies, establish a risk register to track risks and mitigation measures;
3. Establish communication between the SOC and risk management for integration of SOC insights into risk assessment at a later point.

Expected outcome: A comprehensive risk management framework, defined risk appetite, and established processes for integrating SOC insights into risk assessments.

Resource assessment and allocation

What: Evaluate existing capabilities and determine resource needs for the SOC. Ensure adequate allocation of personnel, technology, and financial resources to support SOC operations.

Resources: [4.9 SOC – Human factors] [4.3.1 Core function - GOVERN – Technologies] [4.4.1 Core function - IDENTIFY – Technologies] [4.5.1 Core function - DETECT – Technologies] [4.6.1 Core function - RESPOND – Technologies] [4.7.1 Core function - PROTECT – Technologies] [4.8.1 Core function - RECOVER – Technologies]

Who: SOC leadership, HR representatives, MSSP

How:
1. Evaluation of the existing capabilities, tools, personnel and budget that can be integrated into the SOC;
2. Identification of resources available from the MSSP (for hybrid organizational structure);
3. Determine staffing and tooling needs based on a resource assessment and create a resource allocation plan. *Tab. 41* shows an estimation baseline for internal staffing in the Swiss market:
4. Establish a hiring strategy, including internal recruitment and MSSP engagement, and initiate the hiring process.

Tab. 41 *Staffing costs*

Role	Estimated salary per year [CHF]	Additional estimated costs for employer (~20%) [CHF]	Total Cost [CHF]
SOC manager	140,000	28,000	168,000
Security analyst	90,000	18,000	108,000
Incident responder	110,000	22,000	132,000
SOC engineer	110,000	22,000	132,000
Threat hunter	85,000	17,000	102,000
Forensic analyst	110,000	22,000	132,000

Note 1: The estimates reflect Swiss market rates, which are generally higher than EU averages. The staffing plan includes positions, which falls within the range of a small to medium-sized organizations.

Note 2: CISO and Risk manager roles are considered as external to SOC in-house organization and would be reflected as costs for consultancy or MSSP services bought on-demand.

Expected outcome: A resource allocation plan, including staffing requirements, technology needs, and integration of existing resources.

Secure funding and financial planning

What: Develop a comprehensive budget and financial plan for the SOC, taking into account the resource allocation plan, to support both initial setup and ongoing operations.

Resources: [4 Security Operation Center overview]

Who: SOC leadership, MSSP, government entities and funding bodies

How:
1. Develop a high-level budget roadmap taking into account the resource allocation and projected needs across all phases of the SOC's development;
2. Create a detailed capital (CAPEX) and operational (OPEX) breakdown, by phase:
    - Foundation: Minimal costs focused on strategic planning, governance, and securing initial resources;
    - Build-out: Significant investments in infrastructure, technology, and staffing to set up the SOC;
    - Initial operating capability: Costs primarily for staffing, MSSP services, and initial technology deployment;

- Coverage extension and optimization: Investments for expanding geographic and technological coverage, optimizing SOC operations;
- Continuous improvement: Ongoing maintenance, reviews, updates and enhancements of SOC operations.

3. Identify and secure funding: government and public sector funding, MSSP co-funding model, internal budget allocation and revenue generation potential

Expected outcome: An approved budget and financial plan

An example of the cost breakdown is represented in *Fig. 33* and *Fig. 34*. All detailed budget items are available in appendix ***I.b*** Detailed budget***.***

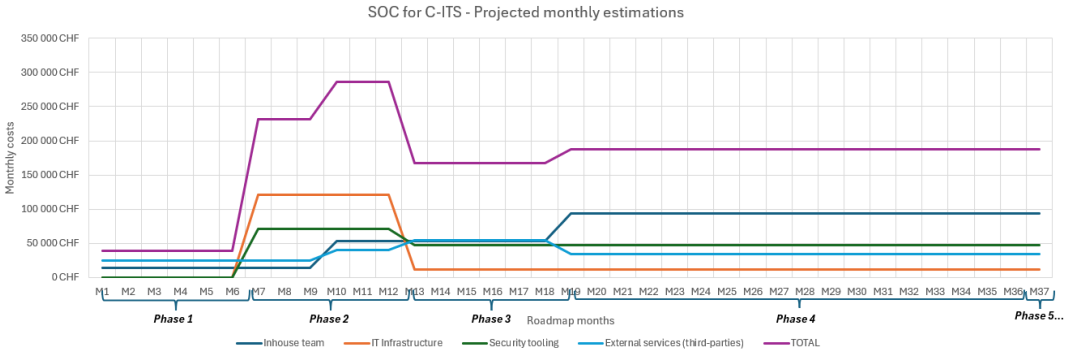


Fig. 33 *SOC Roadmap – projected monthly cost estimations.*

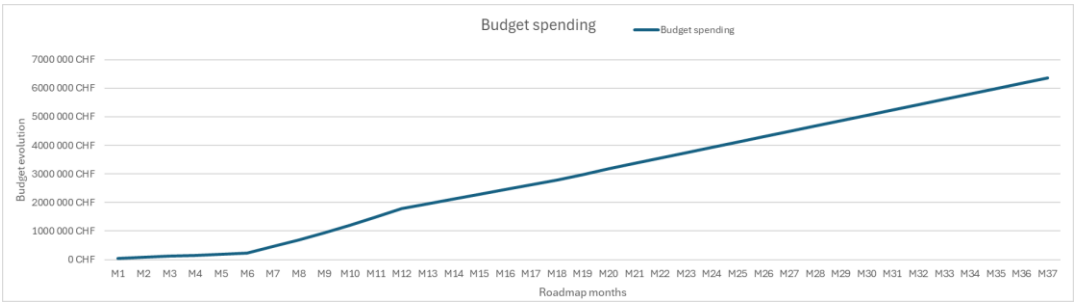


Fig. 34 *SOC Roadmap – projected monthly budget spending estimations.*

Fig. 33 above shows the evolution of costs per month and cost center, for the in-house team (incl. salaries and related costs), IT infrastructure (incl. backend infrastructure), security tooling (incl. SIEM and any other related tools supporting specific SOC operations), and external services (incl. MSSP, consultancy, training, etc.). By considering integration of new tools within newly instantiated backend infrastructure as part of <Phase 2>, this part of the roadmap represents the most costly timespan.

This trend is also visible in *Fig. 34* above, which illustrates the evolution of budget spending month-by-month as an absolute amount. The steeper the curve is, the higher the monthly costs. This confirms <Phase 2> as the biggest challenge financially. Subsequent phases are dedicated to the initial and continuous operations, representing stabilized costs.

In a nutshell:

- Phase 1 costs mostly include initial staffing and consultancy services for establishing the SOC's organization;
- Phase 2 costs cover technical implementation of the infrastructure and tooling needed to operate the SOC (= biggest CAPEX), as well as possibly increasing internal staffing;
- Phase 3 costs include the initiation of extended MSSP collaboration, on top of continuous licensing and internal costs;
- Phase 4 costs include the completion of in-house staff with additional roles and workforce, by reducing extended involvement of the MSSP in daily activities.

6.1.3 Outcome

By the end of this phase, a hybrid SOC organization should be established, with clear responsibilities for the hosting organization and the MSSP, a clear SOC governance organization, knowledge of the resources available and needed, core processes created, and a budget plan.

Key deliverables

- SOC mandate;
- Stakeholder register;
- Governance framework with RACI matrix;
- Core governance processes, information security policies;
- Risk management framework;
- Resource allocation plan with staffing process underway;
- Approved budget and financial roadmap.

Key Performance Indicators

- Percentage of staff roles filled: Target 25%
- Foundational deliverables completion rate
    - Percentage of planned core deliverables (mandate, governance, stakeholder register, risk framework, budget) finalized and approved by the end of Phase 1: Target: ≥ 90%
- Stakeholder engagement coverage
    - Proportion of identified key stakeholders (e.g., government, MSSP, cantons) formally onboarded and involved in SOC development: Target: ≥ 85%
- Adherence to phase timeline
    - Percentage of milestone activities completed within the scheduled 6-month timeframe: Target: ≥ 95% of activities on schedule
- Overall phase quality and satisfaction score
    - Average satisfaction score (from stakeholders or steering committee) regarding the quality, clarity, and relevance of SOC foundations established during Phase 1: Target: ≥ 8/10

6.2 Phase 2 – Swiss SOC for C-ITS build out

This phase relies on key processes to ensure effective deployment. This includes selecting and integrating C-ITS infrastructure, implementing SOC technologies like SIEM and automation tools, and establishing staffing and training plans for skilled personnel. Additionally, a structured asset inventory and management system ensures visibility and compliance, while operational workflows streamline incident monitoring and response.

6.2.1 Objectives and outcomes

Fig. 35 summarizes the key objectives and expected outcomes of this phase. Detailed explanations of the processes involved are provided in the sections below.

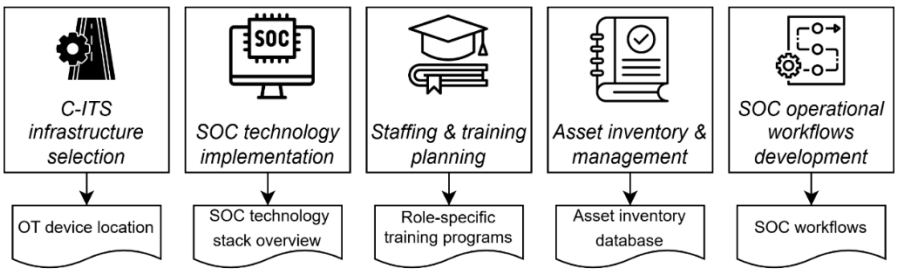


***Fig. 35** Roadmap phase 2 objectives and outcomes.*

Phase duration: approx. 6 months
Total phase cost: approx. 1’552’500 CHF

The primary objective is to define an effective deployment strategy. Chapter 5 “Swiss SOC for C-ITS – Deployment Strategy” explores different organizational structures (In-House, MSSP, Hybrid) and deployment options for a C-ITS SOC (geographic, technological, and capability-based).

The hybrid approach with MSSP support was chosen to combine internal management of critical incidents with outsourced global threat monitoring. This ensures direct control over sensitive incidents while leveraging the expertise to an external provider.

The deployment will follow a phased approach:
- Technological: Initial focus on a single technology (RSU, cameras, detectors, adjustable speed limit sign) to optimize data integration and refine monitoring and response processes. Subsequent phases will expand the technological scope;
- Geographic: Launch in an urban area for easier management, followed by gradual expansion to the cantonal and national levels;
- Capability-based: Unlike the other two approaches, core capabilities (Identification, Detection, Response) will be implemented from the start to ensure comprehensive security coverage.

This strategy enables a rapid operational launch, controlled scalability, and immediate demonstration of the SOC’s value.

6.2.2 Detailed processes

C-ITS infrastructure selection

What: The C-ITS infrastructure selection focuses on identifying OT devices, such as RSUs, cameras and adjustable speed limit signs, to support SOC monitoring and incident detection. The initial deployment prioritizes a single technology, ensuring optimized data integration and refined monitoring processes. Geographic deployment begins in urban areas, where managing infrastructure is more controlled, before expanding to cantonal and national levels in subsequent phases. This approach ensures a scalable and secure integration of OT devices, aligning with SOC capabilities from the outset while progressively extending technological scope and geographic coverage.

Resources:
- 6.1.3 Outcome: Governance framework, stakeholder register, risk management approach;
- Technical references: Swiss road infrastructure data, C-ITS architecture guidelines (ETSI [39], ISO 21177 [40]);
- Stakeholder input: ASTRA, cantonal transport agencies, MSSP, infrastructure operators;
- Technology specifications: Vendor documentation for connected OT devices.

Who: SOC leadership, ASTRA & Cantonal agencies, MSSP, Technology providers, external cybersecurity experts

How:
1. Infrastructure mapping: Involves identifying existing C-ITS assets such as RSUs and cameras in urban areas, conducting site assessments to evaluate placement feasibility and network connectivity, and identifying gaps requiring new installations for effective SOC monitoring;
2. Device selection and placement strategy: Prioritizes one type of asset in urban zones for early threat detection, defines selection criteria based on interoperability, security features, and data relevance, and establishes a phased deployment roadmap from urban areas to cantonal and national levels in subsequent phases;
3. Integration planning: Ensures selected asset connectivity with SOC infrastructure through secure communication protocols like ITS-G5 and 5G, develops a data flow

architecture to optimize incident detection, and implements security controls such as encryption, access management, and logging policies;
4. Regulatory and compliance considerations: Focus on aligning deployments with Swiss regulations on data privacy and cybersecurity, adhering to ETSI C-ITS, ISO/IEC 27001 [36] and ISA/IEC 62443-2-1 [25] frameworks for secure integration, and addressing potential cyber-physical threats, including device tampering and unauthorized access.

Expected outcome: The expected outcome is a structured and scalable deployment of C-ITS infrastructure, starting with the identification and mapping of existing OT devices, such as RSUs and cameras, in urban areas. A well-defined selection and placement strategy will ensure optimal integration of these devices based on interoperability, security features, and data relevance, enabling effective SOC monitoring. Secure connectivity and data flow architecture will be established, incorporating encryption, access management, and logging policies to protect communications between OT devices and the SOC. Compliance with Swiss regulations and international cybersecurity standards will be ensured, mitigating cyber-physical risks and reinforcing the security of C-ITS infrastructure. This phase will result in a comprehensive asset inventory, validated placement strategy, and a roadmap for phased technological and geographic expansion.

SOC technology implementation

What: The implementation of SOC technology focuses on deploying and configuring essential tools for real-time monitoring, detection, and response to cyber threats within the C-ITS environment. This includes log collection, SIEM integration, threat intelligence platforms, and anomaly detection systems. The goal is to establish a secure and scalable architecture that enables efficient data processing, correlation, and incident response.

Resources:

[4.1.2 SOC functions] [4.4.1 Core function - IDENTIFY – Technologies] [4.5.1Core function - DETECT – Technologies] [4.6.1 Core function - RESPOND – Technologies] [4.7.1Core function - PROTECT – Technologies] [4.8.1 Core function - RECOVER – Technologies]

In addition, the implementation of SOC technology requires a robust infrastructure, including servers, storage, and networking components to support log collection and analysis. Security tools such as SIEM, log management systems, threat intelligence platforms, and intrusion detection/prevention systems are essential for effective threat monitoring and response. Communication protocols like ITS-G5, 5G, and secured APIs must be integrated to ensure seamless data exchange between C-ITS components and the SOC. Compliance with cybersecurity frameworks, including ISO/IEC 27001 [36], ISA/IEC 62443-2-1 [25], ETSI C-ITS [39], and Swiss regulations, is critical to maintaining security and regulatory alignment. Additionally, comprehensive documentation, standard operating procedures, and integration guidelines, will support the implementation and future optimization of the SOC's technological capabilities.

Who: SOC engineer, MSSP, FEDRO OT specialists

How:
1. Log collection and aggregation: Identify relevant data sources (RSUs, traffic sensors, surveillance cameras, etc.), configure log forwarding mechanisms, and implement a centralized log management system;
2. SIEM deployment and configuration: Install and configure the SIEM platform, define log parsing rules, set up correlation rules for detecting anomalies, and integrate with external threat intelligence feeds;
3. Threat intelligence and anomaly detection: Implement a threat intelligence platform, integrate it with SIEM, and deploy AI-driven anomaly detection systems for proactive monitoring;
4. Secure communication and data flow architecture: Establish encrypted channels for data transmission, enforce strict access controls, and ensure compliance with cybersecurity standards;
5. Automated incident response and workflow implementation: Define alerting mechanisms, automate incident escalation workflows, and integrate playbooks for rapid mitigation;

6. Testing and optimization: Conduct system validation tests, fine-tune detection rules to reduce false positives, and optimize system performance for scalability.

Expected outcome: A fully operational SOC technology stack capable of securely collecting, processing, and analyzing security events within the C-ITS ecosystem. The SOC will have a centralized log management system, a configured SIEM platform with automated threat detection, and secure communication channels. Incident response workflows will be established, ensuring quick detection and mitigation of cybersecurity threats. Compliance with Swiss regulations and international standards will be maintained, supporting future scalability and technological expansion.

Staffing and training planning

What: Build on the staffing requirements defined in phase 1 by establishing a structured training plan to ensure the SOC has the necessary expertise to operate effectively. This includes hiring qualified personnel, developing competency frameworks, and implementing training programs to enhance technical and operational capabilities.

Resources: [4.9 SOC – Human factors] [6.1.2 Detailed processes (Resource assessment and allocation – Outcome)]

A successful staffing and training plan requires a combination of human and financial resources, along with structured learning programs. HR and recruitment teams will work alongside SOC leadership to define job roles, assess market availability, and establish competitive compensation plans. Financial resources must be allocated for hiring, certifications, and continuous training. Training resources include cybersecurity frameworks (e.g., NIST [23], MITRE ATT&CK [44], ISO/IEC 27001 [36], ISA/IEC 62443-2-1 [25]), vendor-specific technical training for SIEM and security tools, and tabletop exercises for incident response. Additionally, partnerships with academic institutions, cybersecurity training providers, and MSSP support will be leveraged to enhance staff competencies.

Who: SOC leadership, CISO, HR representatives

SOC Engineers, Security Analysts and Incident Responders will participate in training programs.

External training providers, industry experts and MSSP partners will deliver training sessions.

How:
1. Competency framework and training plan: Define required skills for each SOC role, identify training needs, and develop a structured learning path, including certifications and on-the-job training;
2. Implementation of training programs: Provide foundational training on cybersecurity principles, hands-on technical training for SOC tools, and advanced courses on threat detection, forensic analysis, and incident response;
3. Simulations and continuous learning: Conduct real-world simulations (e.g., red teaming, blue teaming, tabletop exercises), integrate ongoing training sessions, and ensure staff remains updated on emerging threats and technologies.

Expected outcome: By the end of this process, a structured training framework will be in place, ensuring that all SOC members possess the necessary skills to manage cybersecurity threats effectively. Continuous learning and hands-on simulations will enhance operational readiness, enabling the SOC to detect, analyze, and respond to incidents efficiently within the C-ITS environment.

Asset inventory and management

What: The asset inventory and management process establishes a structured approach to identifying, classifying, and maintaining an up-to-date registry of all C-ITS-related assets within the SOC's operational scope. This includes physical devices (RSUs, cameras, sensors), network components, software, and data sources. The goal is to ensure visibility,

accountability, and security of all assets while enabling efficient risk assessment and incident response.

Resources: [4.4 Core function - IDENTIFY], existing asset databases from authorities (e.g., ASTRA) and private-sector partners, network discovery tools, BOM and SBOM

Who: SOC Engineer, Security Analysts, C-ITS infrastructure providers, MSSP supporting automated asset discovery and classification

How:
1. Data collection and consolidation: Gather existing asset information from authorities, operators, and internal SOC records, merging various databases into a unified asset inventory;
2. Automated discovery and classification: Deploy asset management tools to scan networks, detect connected devices, and categorize them by type, function, and ownership;
3. Asset tagging and risk profiling: Label assets with unique identifiers, define their criticality to SOC operations, and assess potential vulnerabilities;
4. Integration into SOC processes: Link asset data to security monitoring, incident response workflows, and risk management processes;
5. Ongoing updates and compliance checks: Establish governance rules for regular inventory reviews, audits, and alignment with cybersecurity regulations.

Expected outcome: A comprehensive and continuously updated asset inventory that enhances SOC visibility, threat detection, and incident response. The inventory will be integrated into security processes, ensuring asset lifecycle tracking, risk-based prioritization, and regulatory compliance for C-ITS infrastructure.

SOC operational workflow development

What: The development of SOC operational workflows establishes standardized processes for threat detection, incident response, log management, escalation procedures, and continuous monitoring. These workflows ensure that SOC operations run efficiently, incidents are managed effectively, and security events are properly documented and addressed. The goal is to create structured, repeatable, and adaptable processes that align with best practices (e.g., NIST [23], ITIL [74], ISO/IEC 27001 [36], ISA/IEC 62443-2-1 [25]) while being tailored to the specific needs of the C-ITS environment.

Fig. 36 shows an example of a high-level incident management process workflow diagram integrating NIST core functions.

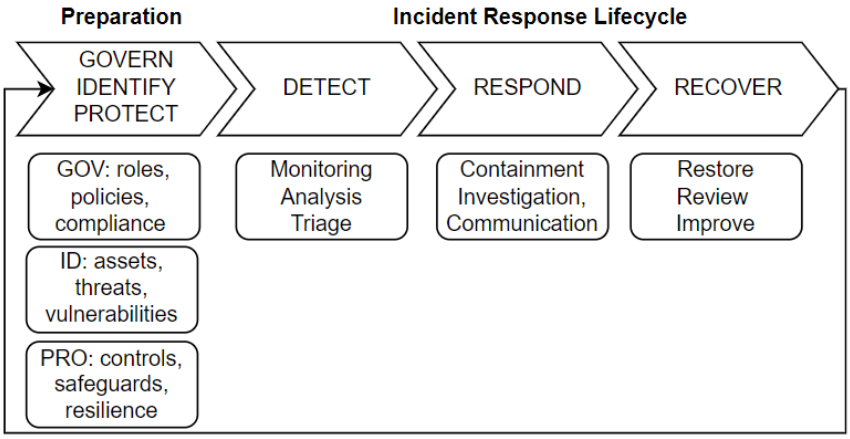


***Fig. 36** NIST process workflow diagram example.*

Resources: [3Approaching C-ITS security concerns],[4.6.1 Core function - RESPOND – Technologies] existing procedures from MSSP partners or industry benchmarks

Who: SOC leadership, MSSP provider

How:

1. Define SOC core functions: Identify essential SOC processes, including event monitoring, threat detection, alert triage, incident response, forensics, and post-incident reporting;
2. Develop process maps and escalation matrices: Structure workflows by defining roles, responsibilities, decision points, and escalation paths within the SOC;
3. Integrate workflows with SOC tooling: Implement automation where possible (e.g., SOAR for response orchestration, SIEM for event correlation) and connect workflows with asset inventory and incident management platforms;
4. Validation and testing: Conduct tabletop exercises and incident simulations to refine and validate workflow effectiveness;
5. Documentation & training: Create standard operating procedures (SOPs) and provide training to SOC analysts and response teams.

Expected outcome: A documented set of SOC workflows and procedures that ensures efficient incident detection and management within the C-ITS environment. These workflows will be integrated with SOC tools, aligned with industry best practices, and continuously improved based on operational feedback and evolving threat landscapes.

6.2.3 Outcome

By the end of this phase, the SOC will have its basic infrastructure in place, with the facility being set up, the deployment of essential tools, technologies, the definition of core processes and a training framework in place.

Key deliverables

- Chosen OT device and location;
- SOC technology stack overview;
- SOC operational workflows;
- Preliminary asset inventory database;
- Role-specific training programs;
- Threat intelligence platforms.

Key Performance Indicators

- Technological deployment progress rate
    - Percentage of SOC technologies (SIEM, log management, IT platform, etc.) deployed and operational compared to the initial plan: Target: ≥ 90%
- SOC personnel readiness index
    - Percentage of critical SOC positions filled and personnel completing initial training (technical skills, simulations, certifications): Target: ≥ 85%
- Asset inventory accuracy rate
    - Percentage of C-ITS assets correctly identified, classified, and integrated into the asset inventory database: Target: ≥ 95%
- Operational workflow maturity score
    - Level of completion and validation of SOC workflows (detection, response, escalation), measured through tests and simulations: Target: 80%

6.3 Phase 3 – Swiss SOC for C-ITS initial operating capability

The main goal of this phase is to fully deploy the SOC's capabilities, with the definition and implementation of playbooks that support NIST core functions (Identify-Detect-Respond) and integrate the chosen technology from a given site. This phase builds on the workflows developed in Phase 2 and implements specific playbooks on top. Additionally, this phase focuses on establishing stakeholder agreements, developing information exchange frameworks, extending asset inventories and refining processes through test runs. It also involves compliance adjustments, including meeting NCSC mandatory reporting requirements. This phase represents the first fully operational SOC and precedes large-scale deployment.

6.3.1 Objectives and outcomes

Fig. 37 summarizes the key objectives and expected outcomes of this phase. Detailed explanations of the processes involved are provided in the sections below.

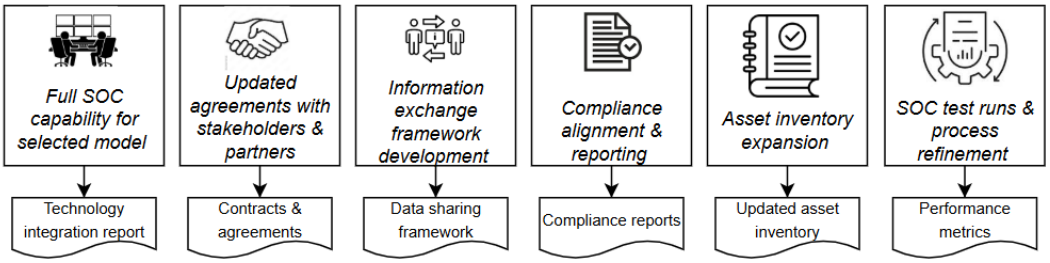


***Fig. 37** Roadmap phase 3 objectives and outcomes.*

Phase duration: approx. 6 months
Total phase cost: approx. 1’008’000 CHF

6.3.2 Detailed processes

Full SOC capability for selected technology and location

What: Achieve full operational capability of the SOC for the chosen C-ITS technology at the selected location. This involves completing the integration of all SOC tools and technologies and NIST core functions (identify, detect, respond) to enable comprehensive monitoring, detection and response capabilities. This also involves getting the SOC staffed close to full capacity, ensuring almost all roles are filled.

Resources: [6.2.3 Outcome], [4.4 Core function - IDENTIFY], [4.5 Core function - DETECT], [4.6 Core function - RESPOND]

Who: SOC team (analysts, engineers, incident responders), MSSP provider

How:
1. Get close to full staffing capacity: Ensure that almost all roles are filled (SOC Manager, CISO, Risk Manager, Incident Responder, SOC Engineer, Threat Hunter, Forensic Analyst, and Security Analyst (partially)). Initially, one to two security analysts will be sufficient to handle the current volume of events. As the SOC scales up, technologies are added, and geographical coverage expands, additional security analysts will be onboarded to achieve full staffing capacity;
2. Finalize C-ITS technology integration in the SOC’s monitoring and security tools, which are represented in *Fig. 38*.
3. Implement Identify-Detect-Respond functions as described in *Tab. 42*.

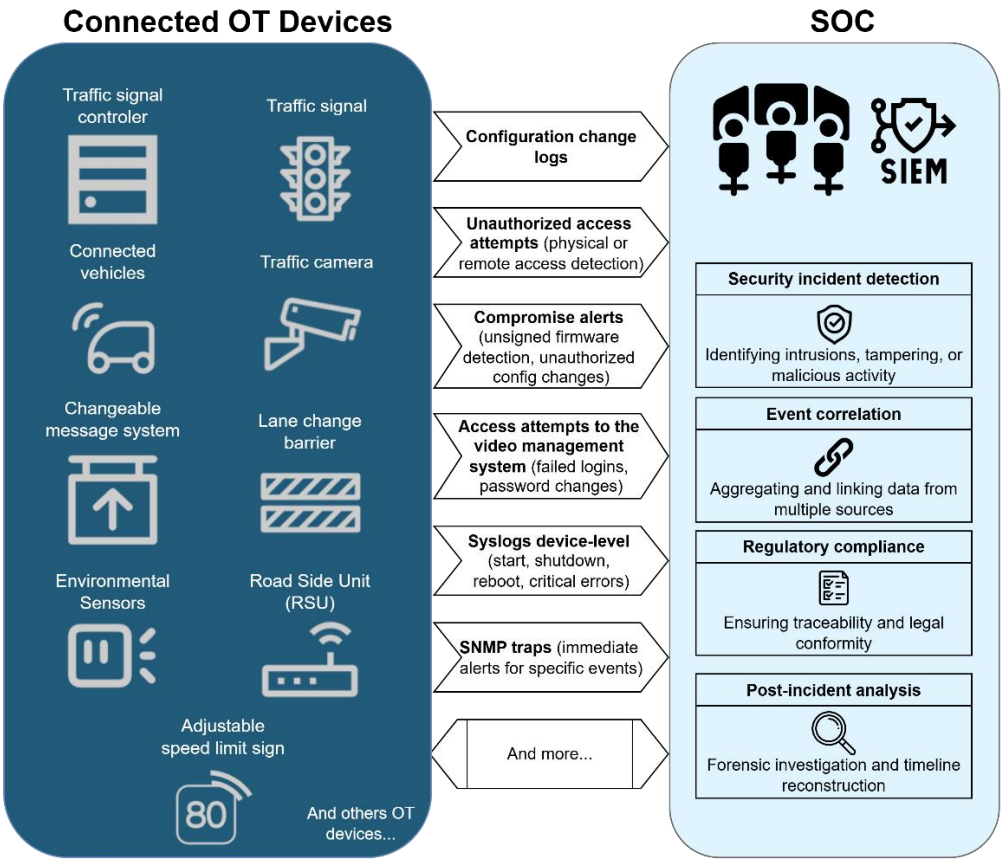


Fig. 38 *Example of communication data exchange from OT Devices to SOC.*

Tab. 42 *NIST core functions*

IDENTIFY	Asset discovery and inventory, Asset inventory expansion	Continue asset identification to fill the asset inventory. Implement automated processes to identify all instances of the chosen C-ITS technology within the selected location.
	Vulnerability management	Conduct regular scans of C-ITS assets. Implement vulnerability management processes to track, prioritize and remediate vulnerabilities.
	Threat intelligence and risk assessment support	Ensure processes for gathering threat intelligence are in place. Establish communication channels with the risk manager to share asset inventory, vulnerability data, threat intelligence.
DETECT	Security monitoring and log management	Continuously monitor logs generated by the C-ITS technology for security-related events. Establish baseline behavior.
	Threat detection and alerting	Integrate threat intelligence to identify known IOCs, develop custom detection rules tailored to specific C-ITS threats.
	Network traffic analysis	Implement packet capture and analysis capabilities using anomaly-based detection.
	Alert management	Implement an alert triage and prioritization process to focus on the most critical incidents. Establish clear escalation paths for different types of alerts.

RESPOND	Incident response plan	Develop specific playbooks for common attack scenarios. Include incident response steps: detection & analysis, containment, eradication, recovery, post-incident activity and relevant parties responsible.
	Post-incident forensics	Define processes for conducting forensic investigation after an incident.

Expected outcome: a fully operational, almost fully staffed SOC with defined playbooks tailored to a C-ITS environment, ensuring effective monitoring, incident detection and response.

Agreements with stakeholders and partners

What: Establish new agreements and update existing ones with stakeholders and partners to define roles, responsibilities and collaboration mechanisms for SOC operation.

Resources: [6.1.3 Outcome Key deliverables (stakeholder register)], Documentation of stakeholder inputs and requirements

Who: SOC management team**,** key stakeholders**,** MSSP**,** new stakeholders and partners

How:
- Review and gap analysis: Assess current agreements and identify areas needing updates or new contracts based on evolving SOC operational needs;
- Identify additional partnerships/stakeholders based on evolving SOC functions;
- Conduct workshops with those new stakeholders to gather input on their role and define their interactions with the SOC;
- Establish communication channels and contact points to facilitate information sharing.

Expected outcome: Updated stakeholder register, contracts and agreements

Information exchange framework development

What: At this stage, communication channels between stakeholders should be established. The next step in terms of data gathering is to integrate the SOC into information exchange frameworks to enhance situational awareness and incident response. This includes the NCSC threat intelligence information exchange platform and other platforms such as Information Sharing and Analysis Centers (ISACs) and the Malware Information Sharing Platform (MISP), which provide access to critical threat data.

Resources: [4.4 Core function - IDENTIFY(Threat Intelligence Integration)], NCSC report platform [Incident] [Vulnerability]

Who: NCSC, other information sharing platform holders, SOC Analysts and Threat Intelligence Managers, MSSP

How:
- Identify relevant frameworks:
  - NCSC threat intelligence platform;
  - ISACs;
  - MISP;
  - Other industry-specific platforms.
- Create workflows for information intake and utilization;
- Establish secure integration;
- Educate SOC personnel on new information sharing processes;

Expected outcome: SOC integrated into relevant information exchange platforms, improving threat detection, situational awareness, and incident response capabilities.

Compliance alignment and mandatory reporting

What: Compliance adjustment to follow Swiss regulations and align with EU regulations. Establishment of mandatory reporting to NCSC.

Resources:
- [4.11 Security Operation Center – Regulatory Context for SOC Implementation in C-ITS];
- ICT minimum standard & reporting guidelines – NCSC [24];
- Swiss Federal Act on Information Security (FAISC) [5];
- FEDRO Directives;
- EU ITS Directive (EU) 2023/2661 [12].

Who: SOC management team, MSSP

How:
1. Mandatory reporting to NCSC:
    a. Get the list of criteria and rules that trigger mandatory reporting:
        i. Source document: amended version “revISA” (2025) [5];
        ii. The report must be made to the BACS;
        iii. Reports can be made anonymously and are required within 24 hours of discovering a cyberattack.
    b. Create automated processes with rules to make reporting efficient and consistent:
        i. Use SIEM tools for automated incident detection based on pre-defined criteria;
        ii. Automate reporting forms with incident data.
2. Other compliance adjustments:
    a. For detailed SOC roles and actions for compliance, see section 4.11 Security Operation Center – Regulatory Context for SOC Implementation in C-ITS. *Tab. 43* summarizes the compliance adjustments to be made according to European and Swiss standards/guidelines;
    b. Ensuring compliance involves a four-step process:
        i. Conducting a gap analysis;
        ii. Developing and executing a remediation plan;
        iii. Updating policy and procedure;
        iv. Comprehensive documentation in a final report.

Expected outcome: Compliance document demonstrating alignment with Swiss and EU regulations.

Tab. 43 *Compliance adjustments regarding regulations and directives*

Regulation/Directive	Compliance adjustments
EU ITS Directive (EU) 2023/2661 [12]	Implement an ECTL-compatible PKI system.
	Ensure compliance with EU ITS data formats. Align with EU data-sharing frameworks.
	Develop incident response plans aligned with EU protocols for cross-border C-ITS incidents
	Ensure AI systems within C-ITS comply with EU AI regulations
GDPR [1]	Ensure data handling aligns with legal requirements, ensure anonymization and pseudonymization where applicable.
FAISC [5]	Ensure compliance with the general principles, information classification and handling, IT security, personnel security, and physical security provisions.

ICT Minimum Standard (NCSC) [24]	Align SOC operations with the NIST core functions (Identify, Protect, Detect, Respond, Recover). Practical implementation examples are given in the ICT Minimum Standard.
FEDRO Directives	Align SOC where relevant, leveraging directives regarding OT security governance and OT security.

SOC service test runs and process refinement

What: Conduct test runs of SOC services and capabilities to adjust processes, workflows, and technology implementation as appropriate.

Resources: [4.6.2 Core function - RESPOND – Processes (Incident response playbooks and workflows)], [6.2.2 Detailed processes (SOC technology implementation)], test scenarios and simulated attack patterns.

Who: SOC Analysts, SOC Engineers, MSSP, Incident Responders

How:
1. Develop test plan considering key SOC capabilities to test and realistic attack scenarios;
2. Conduct tabletop exercises, walking through scenarios, validating communication workflows and identifying potential gaps;
3. Perform simulated attacks and test SOC alerting and escalation procedures;
4. Evaluate tool effectiveness, identifying false positives/negatives, bottlenecks;
5. Collect feedback from SOC personnel, identify areas needing training or process adjustments;
6. Refine processes and workflows based on findings;
7. Update documentation.

Expected outcome: Updated incident response playbooks, tool performance reports, process refinements records

6.3.3 Outcome

At the end of this phase, the SOC will have reached its initial operating capability, fully implementing the Identify-Detect-Respond functions and integrating the chosen C-ITS technology at the selected site. Incident response playbooks and with other key operational documents will be written. In addition, final contracts and agreements will be formalized, and sharing frameworks or liaisons will be functional. The SOC will be fully compliant with Swiss and EU regulations, including mandatory reporting requirements. Finally, SOC processes and tools will be validated and refined through testing, ensuring readiness for full-scale deployment.

Key deliverables
- Contracts and agreements;
- Data sharing framework;
- Compliance reports;
- Technology integration report;
- Updated asset inventory;
- Incident response playbooks;
- Security monitoring and threat detection reports;
- Post-incident analysis reports;
- SOC service tests and process refinement report.

Key Performance Indicators

- SOC service availability
  - Percentage of time the SOC systems (SIEM, ticketing, dashboards, etc.) and staff are operational and accessible: Target ≥ 99.5% uptime
- Compliance alignment score
  - Degree to which SOC processes, tools, and documentation comply with Swiss (NCSC, FAISC) and EU (GDPR, ITS Directive) standards and mandates: Target ≥ 90% based on gap analysis and remediation tracking
- Asset inventory coverage
  - Proportion of in-scope C-ITS assets (RSUs, cameras, signs, etc.) successfully identified and integrated into the asset inventory and monitoring tools: Target ≥ 95% of planned assets
- SOC test run success rate
  - Ratio of successfully executed test runs (e.g., tabletop, simulated attack, alert triage) that meet the predefined objectives without critical gaps: Target ≥ 85%
- Staffing completion
  - Percentage of required SOC roles that are staffed (full-time or interim), including internal and MSSP personnel: Target ≥ 90%
- Detection speed
  - Average time from threat occurrence to detection by the SOC (via SIEM, alerts, sensors, etc.): Target to be baselined during test runs (e.g., target < 10 min for high severity)
- Detection breadth
  - Variety and number of threat scenarios that can be detected based on current playbooks and detection rules (malware, anomalies, misconfigurations, etc.): Target to be defined in detection rule coverage matrix
- Monitoring coverage
  - Percentage of traffic/logs/systems in the C-ITS scope that are actively monitored by the SOC (data sources mapped to SIEM): Target aim for > 90% log coverage of critical systems
- False positive rate
  - Proportion of alerts classified as false positives during test runs or live operations: Target < 10–15% depending on alert category

6.4 Phase 4 – Swiss SOC for C-ITS coverage extension and optimization

In this phase, the focus is on scaling the initial operating capability of the SOC to encompass a larger geographic area and integrate a wider array of C-ITS technologies. By the end of this phase, the SOC will operate at full staffing capacity, integrating all in-scope C-ITS assets. A comprehensive asset inventory will be maintained, and further test runs will be implemented to validate the SOC's ability to effectively handle high-volume security events. This phase is anticipated to be the most extensive in the roadmap as the integration of all C-ITS assets is a time-intensive task.

6.4.1 Objectives and outcomes

Fig. 39 summarizes the key objectives and expected outcomes of this phase. Detailed explanations of the processes involved are provided in the sections below.

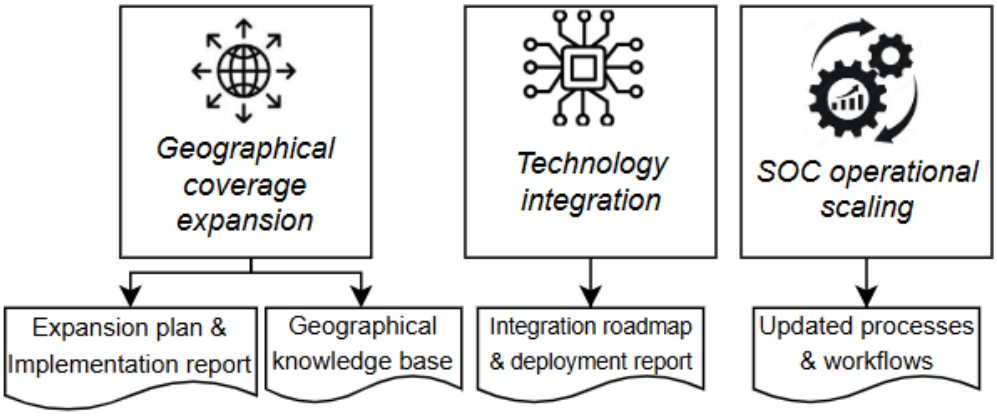


Fig. 39 *Roadmap phase 4 objectives and outcomes.*

Phase duration: approx. 18 months (depending on the size of the geographical area, the various extension phases, and the range of technologies linked to the SOC).

Total phase cost: approx. 3'384'000 CHF

6.4.2 Detailed processes

Geographical coverage expansion and technology integration

What: Geographical coverage expansion and technology integration are closely linked. Following the successful integration of a technology in a limited location in phase 3, coverage will be extended to other geographical areas. Simultaneously, the integration of additional technologies at the initial test site will start, and upon successful validation, will be systematically rolled out to other geographical areas.

Resources: [4.4 Core function - IDENTIFY(asset inventory)], [6.3.3 Outcome (technology integration report)], [5.4 Deployment results]

Who: SOC team (management, analysts, engineers, incident responders), MSSP, technology providers, local authorities

How:

1. Asset inventory assessment
    a. Review existing C-ITS assets per geographical area;
    b. Identify the type of technologies (e.g., RSUs, cameras, sensors) and locations of available assets;
    c. Develop a dynamic asset inventory system that automatically updates as new C-ITS are deployed or existing ones are modified.
2. Establish a geographic expansion roadmap (see *Tab. 44* and *Fig. 40*)
    a. A hybrid prioritization will be used to determine the expansion order, balancing risk-based criteria with practical implementation feasibility;
    b. While a purely risk-based approach ensures the most vulnerable and impactful areas are covered first, it can be complex to implement and potentially slow down deployment. Instead, to ensure an efficient expansion plan, risk criteria (e.g., traffic volume, accident rates, presence of critical infrastructure, C-ITS asset density) will be assessed alongside the practical implementation feasibility (logistical simplicity) of integrating C-ITS into the SOC. The hybrid approach will therefore consist in combining the risk ratings with deployment practicability, optimizing the order in which areas are integrated into the SOC's coverage.
3. Parallel technology expansion (see *Fig. 40*)
    a. Introduce new technologies at an initial test site;
    b. Upon successful validation, roll out the integration of validated technologies following the roadmap.

4. Parallel standardization process (see *Fig. 40*)
    a. Standardize the integration process of new C-ITS technologies;
    b. Develop automated scripts, reports and pre-built security configurations.

Tab. 44 *Likely progress of the roadmap*

Step 1	Urban and high-traffic areas, critical intersections in major urban centers (e.g., Zurich, Geneva, Basel), integrating the validated C-ITS technology from phase 3.
Step 2	Major highways and inter-city routes connecting urban centers, expanding into surrounding cantonal areas.
Step 3	Rural areas and smaller towns, gradually integrating remaining C-ITS assets.

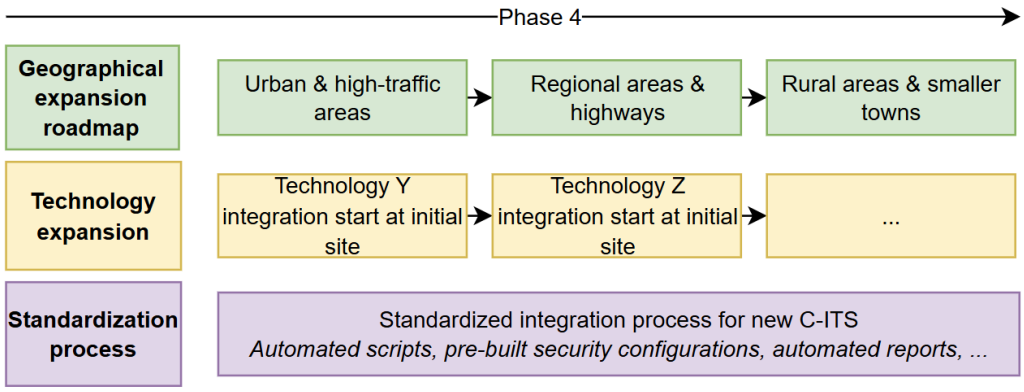


Fig. 40 *Phase 4 rollout.*

Expected outcome: A structured and prioritized SOC geographic expansion plan, technology coverage expansion across locations and automated asset inventory management.

SOC operational scaling

What: Refine and extend SOC workflows to accommodate expanded geographical coverage and newly integrated technologies. Enhance automation and AI capabilities to improve efficiency.

Resources: [6.2.3 Outcome (SOC operational workflows, threat intelligence platforms)], [6.3.3 Outcome (Incident response playbooks)], [4.4 Core function - IDENTIFY(asset inventory)], AI and automation tools

Who: SOC team (management, analysts, engineers, incident responders, Threat Hunter), MSSP

How:
1. Workflow refinement for expanded coverage:
    a. Develop a knowledge base that includes information about local contacts, procedures, resources and escalation paths for each geographical area;
    b. Adapt SOC workflows to incorporate geographical context and account for the specific characteristics and challenges of different geographical areas (urban, regional, rural).

2. Workflow refinement for new technologies:
    a. Optimize SOC incident handling workflows to effectively detect potential security incidents by developing specific correlation rules and pre-defined playbooks tailored to incidents involving newly integrated technologies.
3. Automation and AI integration - scaling efficiencies
    a. Automate the process of enriching alerts with contextual information, integrating for example:
        i. Threat intelligence feeds;
        ii. Asset databases;
        iii. Geolocation data.
    b. Implement AI algorithms to identify anomalous behavior patterns in C-ITS environment;
    c. Develop SOAR playbooks to automate incident response tasks;
    d. Automate the generation of reports based on key SOC metrics and performance indicators. Examples include incident detection metrics, incident response metrics, threat intelligence and trends metrics, system health metrics, and SOC operational efficiency metrics.

Expected outcome: More efficient and scalable SOC operations, improved incident response speed and accuracy through automation and AI enhancements, and adjusted workflows and playbooks for geographic and technology expansion.

6.4.3 Outcome

By the end of this phase, the SOC will have expanded its operational scope both geographically and technologically. All in-scope C-ITS assets will be linked to the SOC, with comprehensive information flow feeding back into the SOC. SOC processes will be optimized, with a higher level of automation, and more resilient, ready to handle large-scale incidents and large amounts of security events.

Key deliverables

- Expanded geographic coverage plan and implementation report;
- Knowledge base for geographical coverage;
- Technology integration roadmap and deployment status;
- Updated SOC processes, workflows and playbooks after optimization.

Key Performance Indicators

- Asset inventory coverage
    - Percentage of known C-ITS assets that are registered and actively maintained in the SOC's dynamic inventory system: Target ≥ 98% of known assets should be included and automatically updated
- Geographic coverage expansion
    - Percentage of the planned geographic areas that are actively monitored by the SOC (i.e., visibility and alerting are operational): Target: gradual increase based on expansion roadmap; e.g., 30% by mid-phase, 100% by end
- Technology integration success rate
    - Success rate of integrating new C-ITS technologies into the SOC (SIEM visibility, alert generation, playbook readiness): Target ≥ 90% of planned technologies should be fully integrated and validated
- Mean Time to Detect (MTTD)
    - Average time between the occurrence of an incident and its detection by the SOC: Target < 15 minutes for critical events
- Mean Time to Respond (MTTR)
    - Average time between incident detection and the initiation of a response or containment action: Target < 30 minutes for high-priority incidents
- Automated incident resolution rate
    - Percentage of incidents resolved automatically via SOAR (automated playbooks, contextual enrichment, scripted actions): Target ≥ 50% of low to medium-severity incidents resolved through automation by end of phase

6.5 Phase 5 – Swiss SOC for C-ITS operation and continuous improvement

This last phase of deployment ensures the SOC's long-term effectiveness, adaptability and sustainability through continuous maintenance and improvement. This involves anticipating emerging threats, enhancing personnel expertise, integrating new technologies and tools, optimizing procedures and automation, and strengthening compliance through new certifications and labels.

6.5.1 Objectives and outcomes

Fig. 41 summarizes the key objectives and expected outcomes of this phase. Detailed explanations of the processes involved are provided in the sections below.

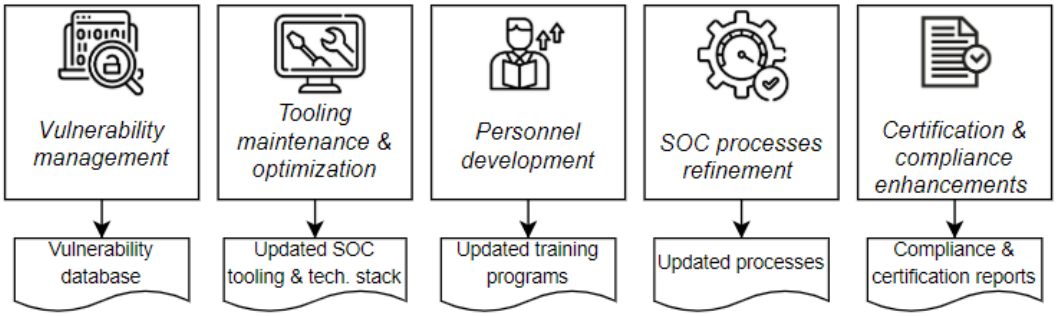


***Fig. 41** Roadmap phase 5 objectives and outcomes.*

Phase duration: Long-term / continuous

Total phase cost: approx. 188'000 CHF/per month

6.5.2 Detailed processes

Vulnerability management

What: Automate vulnerability scanning and integrate results into the incident response process. Maintain a vulnerability knowledge database.

Resources: [4.4.1 Core function - IDENTIFY – Technologies (vulnerability management)], [6.1 Phase 1 – Swiss SOC for C-ITS foundations], [4.5.1Core function - DETECT – Technologies (threat intelligence feeds)], [6.2 Phase 2 – Swiss SOC for C-ITS build out], [4.6 Core function - RESPOND (relevant workflows and playbooks)], [6.3.3 Outcome]

Who: SOC Engineer, Threat Hunter, Risk Manager

How: The vulnerability management process, shown in *Fig. 42*, begins with automated vulnerability scanning, which is scheduled regularly to ensure consistent monitoring and detection of risks across the infrastructure. The results from these scans are then integrated into incident response workflows, enabling incident responders to respond effectively to the identified vulnerabilities. Existing playbooks are refined based on insights gained from scanning activities, ensuring they remain relevant and actionable. Regular risk assessments are conducted to prioritize mitigation efforts. Finally, all discovered vulnerabilities, along with their mitigation and remediation plans, are maintained in a vulnerability knowledge database, ensuring central storage of information for tracking and reporting.

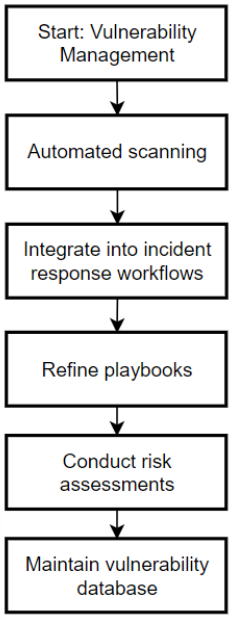


Fig. 42 *Vulnerability management process.*

SOC tooling and infrastructure maintenance and optimization

What: Ensure all SOC tools and infrastructure remain fully operational, up-to-date, and optimized for performance.

Resources: [4.4 Core function - IDENTIFY(asset discovery & management tools)], [4.5 Core function - DETECT (Threat detection)], [6.3.3 Outcome], [4.6 Core function - RESPOND (response tools i.e. SIEM, xDR, IDS/IPS), (automation & orchestration tools i.e. SOAR)], [4.7 Core function - PROTECT (access and security management i.e. IAM, encryption tools)], [4.8 Core function - RECOVER (resilience and backup tools)]

Who: SOC Engineer

How:
- Perform regular maintenance, updates, patching SOC tools and infrastructure;
- Maintain asset inventory with automated updates;
- Implement automated license and BOM management;
- Implement lifecycle management plan for hardware/software, ensuring timely replacement and upgrades of outdated components;
- Perform regular penetration testing to identify and mitigate vulnerabilities;
- Perform regular backups of critical systems to ensure data availability and recovery capabilities;
- Continuously monitor and evaluate new technologies for potential integration into the SOC.

Personnel expertise strengthening

What: Improve SOC personnel expertise through ongoing training and adaptation to evolving threats

Resources: [4.7.2 Core function - PROTECT – Processes], [6.2.3 Outcome (external cybersecurity certification programs)], [4.5.1Core function - DETECT – Technologies (threat intelligence)]

Who: SOC personnel

How:
1. Enhance training programs with threat intelligence inputs and evolving threat landscape insights;
2. Ensure all personnel complete role-specific programs.

SOC operations and process optimization

What: Continuously refine and optimize SOC operations to improve efficiency and reduce errors.

Resources: [6.2.2 Detailed processes (SOPs and playbooks)], Performance monitoring tools, Process automation tools

Who: SOC Engineer, security analysts, incident responders, CISO

How:
- Develop and refine SOP to minimize errors and improve operational efficiency and consistency;
- Continue automating SOC processes;
- Conduct regular KPI reviews (e.g., MTTD/MTTR) to identify inefficiencies and optimize processes;
- Optimize resource allocation for efficient use of SOC resources and capabilities.

Certification and compliance

What: Obtain and maintain relevant certifications and security trust labels.

Resources: [4.3 Core function - GOVERN (compliance frameworks)], [4.3.2 Core function - GOVERN – Processes (policy documentation)]

Who: CISO, MSSP, external auditors

How:
- Obtain and maintain relevant certifications (e.g., ISO 27001 [36]);
- Obtain security and trust labels (e.g., Digital Trust Label);
- Maintain updated documentation on policies, procedures, and configurations;
- Align certifications and compliance with evolving regulatory requirements.

Conduct internal and annual reviews

What: Review SOC performance, identify improvement areas and prioritize enhancement initiatives

Resources: [2.6.3 Purdue model: L4 to L5 – C-ITS systems (incident reports)], [6.3.2 Detailed processes (SOC service test runs and process refinement – SOC performance reports)], Stakeholders feedbacks, [6.3.3 Outcome (post-incident analysis reports)]

Who: SOC leadership, SOC personnel, MSSP, stakeholders

How:
- Set up an annual workshop/meeting with SOC stakeholders to highlight priorities for improvement;
- Conduct an annual internal review where all SOC personnel provide input for improvements;
- Review of all priorities and plan improvement initiatives, assigning teams and processes to implement them.

6.5.3 Outcome

This phase ensures the SOC has all processes and activities required for a continuous improvement cycle. Long-term sustainability and adaptability are secured by the processes in this phase.

Key deliverables

- Annual SOC performance and stakeholder needs review;
- Approved annual budget for SOC operations and improvements;
- Identified and prioritized initiatives for enhancement;
- Updated SOC tooling and technology stack;
- Compliance and certification reports;
- Updated training programs.

Key performance indicators

- MTTD, as indicators maintained all along SOC operation
- MTTR, as indicators maintained all along SOC operation
- Incident response rate
    - Percentage of detected security incidents that receive a documented and appropriate response within SLA timeframes: Target ≥ 98% of incidents responded to within agreed response time (SLA-defined)
- False positive rate
    - Percentage of alerts flagged as incidents by the SOC that are later determined to be benign or non-threatening: Target ≤ 10% (should decrease over time with better tuning and automation)
- Security incident volume
    - Number of security incidents detected and handled by the SOC during a given period: Tracked monthly/quarterly; used to identify trends, attack patterns, and evaluate tooling effectiveness
- Compliance rate
    - Percentage of compliance requirements (internal policies, ISO 27001, regulatory mandates, Digital Trust Label, etc.) that are met: Target ≥ 95% compliance with defined frameworks; measured via internal audits and external certifications
- Patch management efficiency
    - Percentage of identified critical vulnerabilities patched within the defined time window (e.g., 7 days for high-risk, 30 days for medium): Target ≥ 90% of critical vulnerabilities patched within policy-defined timeframe
- SOC personnel training completion rate
    - Percentage of SOC staff who complete mandatory, role-specific training and certifications annually: Target ≥ 90% of personnel complete assigned modules and certifications per year

6.6 Phases summary

Fig. 43 presents a structured, five-phase roadmap for building and operating a Security Operations Center (SOC). It covers the entire lifecycle, from foundational steps like mandate definition and risk management, through technology implementation, stakeholder engagement, and compliance, to the extension of coverage and continuous improvement. Each phase includes key activities and deliverables, ensuring a comprehensive and scalable approach to SOC development and operation.

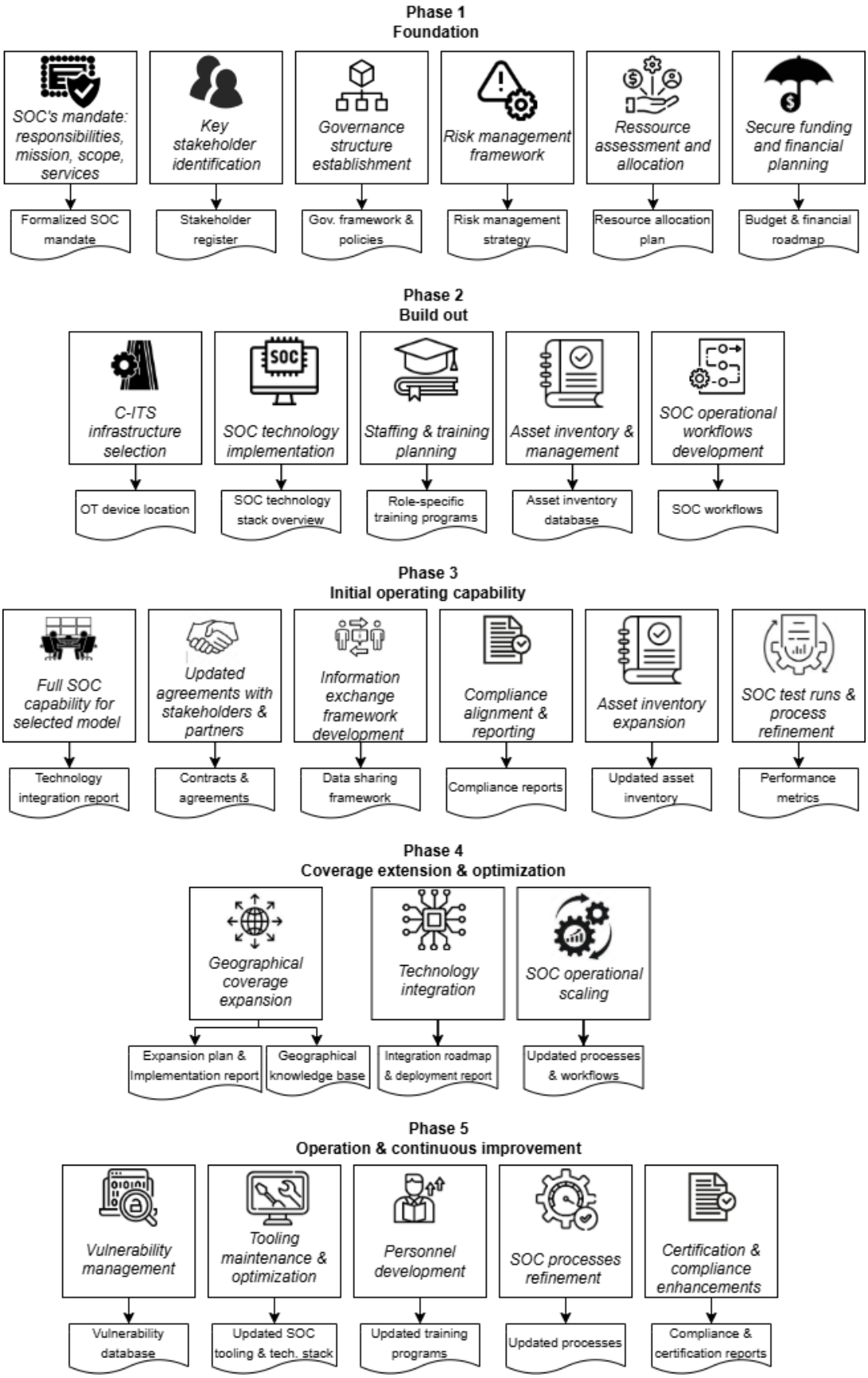


Fig. 43 *Roadmap summary.*

7 Swiss SOC for C-ITS – Roadmap challenges and perspective

This chapter outlines implementation considerations, key challenges encountered during the development of the SOC roadmap and challenges expected during practical implementation. It also highlights research opportunities to support and guide the future development of the SOC.

7.1 Roadmap implementation

While the roadmap provides a structured phased approach to SOC deployment, practical implementation will inevitably require a degree of flexibility. Some parallelization of phases is likely to occur, with activities planned for later phases – such as asset inventory or stakeholder communication – beginning earlier to accelerate readiness.

Key implementation considerations will therefore include making strategic adjustments to sequencing, setting early priorities and maintaining flexibility of execution to adapt to real-world constraints and interdependencies.

7.2 Roadmap challenges

Several challenges were encountered during the development of this report and its proposed roadmap. Some stemmed from complex strategic decisions made during the design phase, such as defining the most effective SOC implementation model, while others were anticipated during the practical execution of the roadmap.

One of the earliest challenges was selecting the appropriate level of implementation for the SOC, being at Canton, UT or National level. Each option presented its own advantages and drawbacks, and no single answer proved ideal. Ultimately, a centralized SOC model was selected, combined with a phased deployment strategy: starting with a limited but comprehensive capability focused locally on one technology, then gradually expanding both in the geographical implementation and range of technologies covered. This approach helps to avoid the organizational complexity associated with SOC management directly at UT-level and Canton-level.

Another challenge that we expect to encounter in implementing the roadmap relates to the skills and commitment of the people responsible for establishing the SOC. The success of the SOC initiative will depend heavily on the commitment and expertise of the project leaders and managers, particularly in the early phases. As highlighted in ISO/IEC 62443-2-1 [25], policy and leadership commitment is very important. Without adequate active support from top management, any cybersecurity program will lack authority, funding and enforcement and the deployment of the SOC is likely to fail. Accordingly, Phase 1 of the roadmap prioritizes the identification and engagement of key stakeholders.

Technological integration also presents technical challenges, especially given the dual IT/OT nature of C-ITS assets and the presence of legacy systems. Integrating a diverse mix of new and legacy assets, many of which were not designed with cybersecurity in mind, adds complexity in creating a unified monitoring environment. Additionally, establishing a comprehensive asset inventory (BOM) is also expected to be a challenge, due to the variety, number, and connectivity capacity of these assets; automatic asset discovery may not always be an option, further increasing complexity.

The implementation of the SOC roadmap is also likely to be complicated by the need to manage multiple activities and phases in parallel. Although the roadmap provides a logical sequence of steps, in practice, several tracks such as technical setup, asset inventory, and stakeholder coordination are likely to run simultaneously. Appropriate prioritization and

sequencing of these activities is essential to maintain consistency and momentum throughout the project.

As the SOC expands its coverage, another challenge will be to determine the order of geographic and technological rollout. This requires achieving the right balance between practical implementation feasibility and a risk-based approach, prioritizing the most vulnerable and impactful areas for early coverage.

Additional operational challenges are expected in areas such as budgeting, timelines, financing and communication. Maintaining alignment among the leadership and all stakeholders throughout the implementation process will be critical, especially as this is where major decisions will be made. The initial phase of the roadmap is designed to address these issues by clarifying the SOC's mandate, mission, scope, service offering and responsible parties.

Being aware and proactively addressing these challenges, many of which are addressed in the roadmap, will be key to ensuring the successful deployment of the SOC.

7.3 Research opportunities

Several key research opportunities can support the development of the SOC roadmap. Firstly, the development of an asset management system tailored to C-ITS operational technology, which is essential for maintaining accurate inventory, tracking device lifecycles and assessing security levels effectively would be an impactful contribution to a critical and resource-intensive task in the roadmap.

Simulating SOC operations is another important area of research. This includes defining incident scenarios and conducting controlled incident response exercises. These simulations can be useful for testing SOC processes, tools, and coordination mechanisms without the need to fully integrate them into the existing C-ITS infrastructure, thereby gaining valuable operational experience and helping to detect and correct weaknesses at an early stage in the process.

Another research opportunity would be to conduct a pilot experiment in a restricted urban area, which would allow the practical challenges of deploying the SOC in a real-world context to be assessed. Insights from the pilot can inform the broader implementation strategy.

Finally, a specific research project could focus on the geographical and technological expansion of the SOC following Phase 1. This project would focus on developing a framework for tailored deployments in cantons or regions, considering factors such as governance structures, technological maturity, resource availability, risk profiles and specific operational needs. Such a framework would ensure a coherent and effective deployment strategy tailored to more local contexts.

Pursuing these research directions will provide valuable information to optimize SOC functionality, reduce implementation risks and support the implementation of a scalable and secure SOC across Switzerland.

7.4 Open questions

Chapter "7. Expected Results, Benefits, and Beneficiaries of the Research" of the project application "MB4_20_02G_01-ProjectDescription-CertX-ROSAS," raised significant open questions categorized by beneficiary. Partial or complete answers to these questions are presented below:

National authorities who define and enforce minimal rules and practices for Swiss C-ITS and road infrastructure

- Do we need cybersecurity monitoring and reacting capabilities on national / cantonal levels?

Yes. Given that C-ITS is classified as critical infrastructure, continuous cybersecurity monitoring and incident response capabilities are necessary at both national and cantonal levels to ensure the security and resilience of Swiss mobility systems.

- Who are the most relevant / capable stakeholders to handle such activities for the Swiss mobility environment? Should it happen at the national level with the support of NCSC? Or at the cantonal level using support from the cyber departments in police agencies? Or any other setup?

The NCSC is the primary national authority, supported by sectoral bodies like FEDRO for road infrastructure. Cantonal police cyber departments may support at the local level. A hybrid model is recommended: national-level leadership with cantonal/local implementation and coordination.

- Are we ready / sufficiently trained and equipped for applying such capabilities to C-ITS environments? If not, how to provide such capabilities in the short- / mid- / long-term?

Switzerland has foundational frameworks (e.g., ICT minimum standard, FAISC), but full readiness for C-ITS-specific SOC operations is still developing. Short-term: leverage existing SOCs and train staff. Mid-term: build dedicated C-ITS SOC capabilities, harmonize processes, and invest in training. Long-term: continuous improvement, integration of advanced technologies, and regular exercises.

- Do we know any potential supporting services in that context? If so, do we have to collaborate with them?

Yes. There are existing SOC service providers (Swisscom, ELCA Security, terreActive, Kudelski, and others), as well as academic centers with relevant expertise. Collaboration is recommended to share knowledge, resources, and best practices. As mentioned in the results presented in this report, the deployment of a hybrid SOC is the most suitable solution. For example, a federal office could implement a hybrid SOC where sensitive incident management is handled by an internal team, while global threat detection and monitoring are entrusted to an external provider.

- Do we have the right skills in-house to run such an SOC? If not, how can the skillset be setup and found?

There is a recognized skills gap. Upskilling current staff, recruiting specialists, and partnering with academic institutions for training and research are recommended. Outsourcing some SOC functions to specialized providers can also bridge immediate gaps.

Operators of C-ITS subsystems (e.g., public transportation providers) representing key stakeholders and actors

- Where are the boundaries related to responsibility sharing and information disclosure for incident detection, reaction and notification between operators and authorities?

Operators are responsible for incident detection and initial response on their own systems, with mandatory reporting and escalation to national authorities (NCSC, FEDRO) for significant incidents. The legal framework (FAISC, directives) defines these boundaries, with clear escalation and notification protocols.

- With whom should we collaborate?

Operators should collaborate with national authorities (NCSC, FEDRO), cantonal cyber units, other mobility operators, and SOC service providers.

Product suppliers providing infrastructure components to be integrated as C-ITS devices

- What is the information we should share, and with whom, to ensure continuous cybersecurity maintenance at the C-ITS level?

Share security advisories, vulnerability disclosures, and update/patch information with C-ITS operators, SOCs, and relevant authorities. Maintain open channels for incident reporting and threat intelligence sharing.

- With whom should we collaborate?

C-ITS operators, national/cantonal authorities, and SOCs.

Service suppliers supporting the establishment and/or operation of secure C-ITS by providing advanced capabilities

- What are the specificities of C-ITS to be considered for adjusting our services?

Services must address the convergence of IT/OT, real-time requirements, heterogeneous protocols, and regulatory compliance. Solutions should be tailored to both legacy and modern C-ITS environments.

- With whom should we collaborate?

Authorities, C-ITS operators, product suppliers, and academic partners.

Academic entities developing their competences and capabilities in this area interested in further development and research

- What are the main capabilities to be developed in support of Security Operation Centers?

Key capabilities include advanced threat detection (using AI/ML), forensics for IT/OT environments, automation/orchestration (SOAR), and specialized training for SOC analysts in C-ITS contexts. These capabilities need to ensure SOC core functions: GOVERN – IDENTIFY – DETECT – RESPOND – PROTECT – RECOVER.

- What are the current needs and future research opportunities in this field?

Needs: improved detection of C-ITS-specific threats, risk assessment methodologies, and incident response strategies for hybrid IT/OT systems. Opportunities: research in automated threat hunting, resilience of interconnected mobility systems, and secure-by-design approaches for future C-ITS deployments.

8 SOC for C-ITS – Conclusions

The mobility ecosystem is increasingly defined by interconnected vehicles and infrastructure through C-ITS. While these systems enhance mobility, they are also attractive targets for threat agents, requiring both proactive and reactive measures.

Necessity of a national SOC for C-ITS

C-ITS is considered as an essential component of modern transport systems, and, as such, forms part of Switzerland's critical infrastructure. C-ITS is therefore subject to cybersecurity regulations that govern critical infrastructure. Swiss and international regulations impose obligations on critical infrastructure operators and general cybersecurity measures, including incident reporting and risk management. The diversity of the C-ITS ecosystem requires coordinated responses between government agencies, transportation authorities, technology operators and other stakeholders, and the SOC is an effective structure to enable efficient operations between multiple entities. Moreover, Swiss Federal Railways (SBB) have demonstrated the benefits of centralized monitoring capabilities, merging control sites at major operating centers, enabling further automation and having a positive impact on efficiency.

Establishing and operating a national SOC for C-ITS

Setting up a national SOC for C-ITS in Switzerland requires a structured definition of requirements, encompassing several aspects:

- Regulatory alignment with the Swiss and European frameworks for critical infrastructure, data privacy, incident reporting and related obligations;
- The functional scope, covering both IT and OT assets and reflecting the dual nature of C-ITS;
- The technical requirements, considering the necessary tools and technologies needed to support the SOC's functions, as well as the integration with existing infrastructure;
- The organizational structure, defining roles, responsibilities, and governance.

The implementation follows a phased roadmap starting with a foundational setup, leading into build-out, development of initial operating capability, extension of coverage to full operation, and continuous improvement activities. The deployment strategy follows a hybrid model, combining geographic and technological scaling. It starts with a limited-scale deployment covering all core SOC capabilities, enabling rapid initial operating capacity.

SOC operations are structured around the core functions of the NIST cybersecurity framework (identify, protect, detect, respond, and recover), with specific tools, technologies, and human resources identified for each function.

Implementation time frame and cost estimates

The proposed roadmap anticipates the completion of phase 4, covering deployment at national level, within approximately 36 months. Phase 5 represents a long-term phase of continuous operation and improvement.

The estimated costs and implementation times are as follows:

- Phase 1 (Foundation): ~CHF 234'000 over 6 months;
- Phase 2 (Build-out): ~CHF 1'552'500 over 6 months;
- Phase 3 (Initial operations): ~CHF 1'008'000 over 6 months;
- Phase 4 (Coverage extension & optimization): ~CHF 3'384'000 over 18 months;
- Phase 5 (Continuous operations): ~CHF 188'000 per month.

Monthly costs peak during phase 2 due to significant CAPEX for IT infrastructure and integration, security tools and team integration. Monthly costs stabilize in subsequent phases. Phase 4 remains costly overall because of its extended duration covering the expansion of the SOC. The monthly operating costs for phase 5 reflect the ongoing effort to maintain, adapt and improve SOC capabilities over time.

Assessment of SOC models

The analysis shows that an SOC model for C-ITS at the cantonal level or based on territorial units in Switzerland is not achievable. Initial consideration of a territorial unit-based model, similar to the SA-CH framework for OT, was set aside after discussions with ASTRA, who highlighted, based on their knowledge of the infrastructure, that such an approach would be unrealistic due to the excessive complexity of the current framework for OT, distributed across UTs. Similarly, ASTRA indicated that even a fully centralized SOC alternative would be difficult to implement given the current organizational landscape.

Despite these challenges, no alternative emerged in the implementation of the SOC that could be effective. The strategy considered was therefore a centralized SOC managed at a national level, with a deployment strategy starting with a limited but comprehensive capability and expanding coverage over time. This approach offers a more manageable solution than a hierarchy of smaller UT-based SOCs and allows for rapid initial operating capacity. Geographical expansion follows a prioritization model that balances risk-based factors (such as accident rates and critical infrastructures) with practical implementation feasibility, ensuring an efficient allocation of resources while minimizing deployment friction.

In terms of ownership, the optimal model is a hybrid configuration featuring extensive involvement of an MSSP, seen as a key driver for SOC operations, combined with an internally managed governance team involving stakeholders from Swiss authorities. This balances efficiency with the necessary oversight and good management of resources.

The establishment of a national SOC for C-ITS is both necessary and feasible, provided it follows a phased implementation strategy and a hybrid governance model. This approach enables centralized coordination while allowing for gradual and scalable deployment, ensuring that all requirements, whether regulatory or operational, are met along the way.

This roadmap offers Swiss authorities a pragmatic route to securing connected mobility in the future.

Annexes

I. External annexes

All external annexes listed below can be requested to the following contact address:

- info@certx.com

a. Demonstrator

The detailed report on demonstrator deployments is available in “MB4_20_02G_01-AnnexA-Demonstrator.pdf”.

b. Detailed budget

The detailed estimations of budget per phase is available in “MB4_20_02G_01-AnnexB-Financials_v2.xlsx”

c. Multicriteria matrix

The detailed multicriteria matrix is available in “MB4_20_02G_01-AnnexC-Multicriteria_Matrix.xlsx”

Acronyms

Acronym	Meaning
ABAC	Attribute-Based Access Control (ABAC)
BACS	Federal Office for Cybersecurity (BACS)
BC/DR	Business Continuity / Disaster Recovery (BC/DR)
BCP	Business Continuity Planning (BCP)
BOM	Bill of Materials (BOM)
CIRCIA	Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA)
CISA	Cybersecurity and Infrastructure Security Agency (CISA)
CISO	Chief Information Security Officer (CISO)
C-ITS	Cooperative Intelligent Transport Systems and Services (C-ITS)
CRA	Cyber Resilience Act (CRA)
CSF	Cyber Security Framework (CSF)
CSIRT	Computer Security Incident Response Teams (CSIRT)
CTI	Cyber Threat Intelligence (CTI)
C-V2X	Cellular Vehicle-to-Everything (C-V2X)
DDoS	Distributed Denial of Service (DDoS)
DETEC	Federal Department of the Environment, Transport, Energy and Communications (DETEC)
DHCP	Dynamic Host Configuration Protocol (DHCP)
DMZ	Demilitarized Zone (DMZ)
DNS	Domain Name System (DNS)
DoS	Denial-of-Service (DoS)
DRP	Disaster Recovery Planning (DRP)
DSRC	Dedicated Short-Range Communications (DSRC)
ECTL	European Certificate Trust List (ECTL)
EDR	Endpoint Detection and Response (EDR)
EES/BSA	Equipment d'Exploitation et de Sécurité / Betriebs- und Sicherheitsausrüstungen (Operating and Safety Equipment) (EES/BSA)
ESS	Equipment de Sécurité et de Signalisation (Safety and Signaling Equipment) (ESS)
EWS	Engineering Workstation (EWS)
FAISC	Federal Act on Information Security in the Confederation (FAISC)
FISMA	Federal Information Security Modernization Act (FISMA)
GDPR	General Data Protection Regulation (GDPR)
GRC	Governance, Risk, and Compliance (GRC)
H2M	Human to Machine (H2M)
HBOM	Hardware Bill of Materials (HBOM)
IAM	Identity and Access Management (IAM)
ICT	Information and Communications Technology (ICT)
IDS	Intrusion Detection System (IDS)
IEC	International Electrotechnical Commission (IEC)

IOC	Initial Operating Capability (IOC)
IoT	Internet of Things (IoT)
IPAM/DDI	IP Address Management (IPAM) / DNS, DHCP, IPAM (DDI)
IPS	Intrusion Prevention System (IPS)
ISA	International Society of Automation (ISA)
ISAC	Information Sharing and Analysis Center (ISAC)
IT	Information Technology (IT)
ITIL	Information Technology Infrastructure Library (ITIL)
ITS -S -SU -G5	Intelligent Transport Systems and Services (ITS) -Station (-S) -Station Unit (-SU) -5 GHz (-G5)
KAR	Korte Afstands Radio (Short Range Radio, NL/BE traffic light comms) (KAR)
LED	Light-Emitting Diode (LED)
M2M	Machine to Machine (M2M)
MFA	Multi-Factor Authentication (MFA)
MISP	Malware Information Sharing Platform (MISP)
MOSCOW	Must-have, Should-have, Could-have, and Won't-have (MOSCOW)
MSSP	Managed Security Service Provider (MSSP)
MTTD	Mean Time To Detect (MTTD)
MTTR	Mean Time To Respond (MTTR)
NAP	National Access Point (NAP)
NCSC	National Cyber Security Centre (NCSC)
NDR	Network Detection and Response (NDR)
nFADP	New Federal Act on Data Protection (nFADP)
NGFW	Next-Generation Firewall (NGFW)
NIDS	Network Intrusion Detection System (NIDS)
NIST	National Institute of Standards and Technology (NIST)
NTA	Network Traffic Analysis (NTA)
OBU	On Board Unit (OBU)
OEM	Original Equipment Manufacturer (OEM)
OT	Operational technology (OT)
PCAP	Packet Capture (PCAP)
PCI	Payment Card Industry (Data Security Standard) (PCI)
PERA	Purdue Enterprise Reference Architecture (PERA)
PKI	Public Key Infrastructure (PKI)
PLC	Programmable Logic Controller (PLC)
RACI	Responsible, Accountable, Consulted, Informed (RACI)
RAS	Remote Access Servers (RAS)
RBAC	Role-Based Access Control (RBAC)
RCS	Rail Control System (RCS)
RSA	Rivest–Shamir–Adleman (cryptographic algorithm) (RSA)
RSU	Road-Side Unit (RSU)

RTU	Remote Terminal Unit (RTU)
SBB	Swiss Federal Railways (SBB)
SBOM	Software Bill of Materials (SBOM)
SCADA	Supervisory Control and Data Acquisition (SCADA)
SDR	Software Defined Radio (SDR)
SEM	Security Event Management (SEM)
SIEM	Security Information and Event Management (SIEM)
SIM	Security Information Management (SIM)
SIS	Safety Instrumented System (SIS)
SLA	Service Level Agreement (SLA)
SN	Swiss Norm (SN)
SOAR	Security Orchestration, Automation, and Response (SOAR)
SOC	Security Operations Center (SOC)
SOX	Sarbanes-Oxley Act (SOX)
SuC	System under Considerations (SuC)
TARA	Threat Analyses and Risk Assessment (TARA)
TCP	Transmission Control Protocol (TCP)
TII	Transport Infrastructure Ireland (TII)
TIP	Threat Intelligence Platform (TIP)
TLP	Traffic Light Protocol (TLP)
TMC	Transportation Management Center (TMC)
TMS	Traffic Management Systems (TMS)
TSC	Traffic Signal Controller (TSC)
TTP	Tactics, Techniques, and Procedures (TTP)
UT	Unité Territoriale (UT)
V2C	Vehicle-to-Cloud (V2C)
V2I	Vehicle-to-Infrastructure (V2I)
V2P	Vehicle-to-Pedestrian (V2P)
V2V	Vehicle-to-Vehicle (V2V)
V2X	Vehicle-to-Everything (V2X)
VIN	Vehicle Identification Number (VIN)
VMS	Variable Message Sign (VMS)
XDR	Extended Detection and Response (XDR)

Bibliography

Regulations

[1] Regulation European Union (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).
https://data.europa.eu/eli/reg/2016/679/oj

[2] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA relevance). Official Journal of the European Union, L 2024/2847, 20 November 2024.
http://data.europa.eu/eli/reg/2024/2847/oj

[3] European Commission. (2017). Commission Delegated Regulation (EU) 2017/1926 of 31 May 2017 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU-wide multimodal travel information services (as amended).
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32017R1926

[4] Swiss Confederation. (2022). Federal Act on Data Protection (nFADP) of 25 September 2020 (Status as of 1 September 2023). https://www.fedlex.admin.ch/eli/cc/2022/491/en

[5] Swiss Confederation. (2022). Federal Act on Information Security in the Confederation (FAISC) of 18 March 2022 (Status as of 1 January 2024). https://www.fedlex.admin.ch/eli/cc/2022/492/en

[6] United Nations (UN) Economic Commission for Europe. (2021). UN Regulation No. 155: Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system (ECE/TRANS/WP.29/2020/79, as amended).
https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security

[7] United Nations Economic Commission for Europe. (2021). UN Regulation No. 156: Uniform provisions concerning the approval of vehicles with regards to software update and software update management system (ECE/TRANS/WP.29/2020/80, as amended).
https://unece.org/transport/documents/2021/03/standards/un-regulation-no-156-software-update-and-software-update

[8] Cybersecurity and Infrastructure Security Agency. (2024). Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).
https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia

[9] Cybersecurity and Infrastructure Security Agency. (2024). Water and Wastewater Sector: Incident Response Guide.
https://www.cisa.gov/resources-tools/resources/water-and-wastewater-sector-incident-response-guide-0

[10] European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending certain Union legislative acts (Artificial Intelligence Act). Official Journal of the European Union, L, 12 July 2024.
https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

Directives

[11] 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).
https://data.europa.eu/eli/dir/2022/2555/oj

[12] 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. https://data.europa.eu/eli/dir/2023/2661/oj

[13] Federal Roads Office (FEDRO). (2022). Instruction 73006: Operational Technology (OT) Security Governance (V1.00).
https://www.astra.admin.ch/dam/astra/fr/dokumente/standards_fuer_nationalstrassen/astra_73006_ot_security_governance.pdf.download.pdf/73006f.pdf

[14] Federal Roads Office (FEDRO). (2024). Directive 13030: OT Security (V2.0).
https://www.astra.admin.ch/dam/astra/fr/dokumente/standards_fuer_nationalstrassen/astra_13030_it-sicherheitleit-undsteuersystemederbetriebs-undsic.pdf.download.pdf/astra_13030f.pdf

[15] Federal Roads Office (FEDRO). (2011). Instructions 73001: Roles and requirements for EES (Équipements d'exploitation et de sécurité) management.
https://www.astra.admin.ch/dam/astra/fr/dokumente/standards_fuer_nationalstrassen/astra_73001_rollenundanforderungenfuerdasmanagementderbetriebs-u.pdf.download.pdf/astra_73001_rolesetexigencespourlagestiondesequipementsdexploitationetdesecuriteees.pdf

[16] Federal Roads Office (FEDRO). (2013). Instructions 73002: Management of operational and security equipment – roles, tasks, and requirements for user interfaces (V1.01).
https://www.astra.admin.ch/dam/astra/fr/dokumente/standards_fuer_nationalstrassen/astra_73002_steuerungderbsarollenaufgabenundanforderungenfuerben.pdf.download.pdf/astra_73002_pilotagedeseesrolestachesetexigencespourlesinterface.pdf

[17] Federal Roads Office (FEDRO). (2017). Directive 13040: IP EES Network (V1.3).
https://www.astra.admin.ch/dam/astra/fr/dokumente/standards_fuer_nationalstrassen/astra%2013040%20ipnetzbsa.pdf.download.pdf/astra%2013040%20reseauipees.pdf

[18] European Commission. (2024). National Access Points (NAPs) for transport data in the EU. Retrieved May 2025, from https://transport.ec.europa.eu/transport-themes/smart-mobility/road/its-directive-and-action-plan/national-access-points_en

Standards

[19] Keyfactor. (n.d.). C-ITS Enrollment Certification Authority (ECA) Overview: European Certificate Trust List (ECTL) [Web page].
https://docs.keyfactor.com/ejbca/latest/c-its-eca-overview

[20] International Organization for Standardization & SAE International. (2021). ISO/SAE 21434:2021 Road vehicles – Cybersecurity engineering.

[21] International Organization for Standardization. (2018). ISO 26262:2018 Road vehicles – Functional safety.

[22] International Organization for Standardization. (2023). ISO 24089:2023 Road vehicles – Software update engineering.

[23] Nelson, A., Rekhi, S., Souppaya, M., & Scarfone, K. (2025). Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A Cybersecurity Framework (CSF) 2.0 Community Profile (NIST Special Publication 800-61 Revision 3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r3

[24] National Cyber Security Centre (NCSC). (2024). Information and Communication Technology (ICT) minimum standard.
https://www.ncsc.admin.ch/ncsc/en/home/infos-fuer/infos-it-spezialisten/themen/ikt-minimalstandards.html

[25] International Electrotechnical Commission & International Society of Automation. (2018–2024). ISA/IEC 62443: Industrial communication networks – Network and system security

[26] International Organization for Standardization. (2014). Intelligent transport systems – Communications access for land mobiles (CALM) – Architecture (ISO Standard No. 21217:2020).

[27] SAE International. (2024). Vehicle-to-Everything (V2X) Communications Message Set Dictionary (SAE Standard J2735).

[28] Swiss Association of Road and Transportation Experts (VSS). (1992). SN 640 832: Traffic light installations; basic standard

[29] Swiss Association of Road and Transportation Experts (VSS). (2001). SN 640 844-3: Traffic signal controllers – Functional safety requirements

[30] European Committee for Standardization. (2014). Road vertical signs – Variable message traffic signs (EN Standard No. 12966:2014).

[31] Swiss Association of Road and Transportation Experts (VSS). (2001). SN 671 510: Level crossings road–rail; signalling and operation

[32] Swiss Association of Road and Transportation Experts (VSS). (2004). SN 671 971: Automatic road traffic control systems based on digital imaging; architecture and requirements

[33] Swiss Association of Road and Transportation Experts (VSS). (2005). SN 671 972: Automatic road traffic state monitoring by digital imaging; architecture and requirements

[34] Swiss Association of Road and Transportation Experts (VSS). (2010). SN 671 973: Automatic road traffic state monitoring by digital imaging; quality requirements

[35] International Society of Automation. (2023). ISA-112: SCADA Systems Management.

[36] International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements

[37] International Organization for Standardization & International Electrotechnical Commission. (2023). ISO/IEC 27035-1:2023 – Information technology – Information security incident management – Part 1: Principles and process. https://standards.iteh.ai/catalog/standards/sist/072431a8-239f-498d-bf1d-c86027603a52/iso-iec-27035-1-2023

[38] International Organization for Standardization & International Electrotechnical Commission. (2022). ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks (4th ed.).

[39] European Telecommunications Standards Institute (ETSI). (n.d.). [Title of specific ETSI standard or deliverable]. https://www.etsi.org/

[40] International Organization for Standardization. (2024). ISO 21177:2024 Intelligent transport systems — ITS station security services for secure session establishment and authentication between trusted devices. https://www.iso.org/standard/81067.html

Documentation

[41] Federal Office of Road (FEDRO). (2024). “Cyber Threat Intelligence Framework and recommendation for C-ITS”. ARAMIS. *https://www.aramis.admin.ch/Grunddaten/?ProjectID=49812&Sprache=en-US*

[42] National Cyber Security Centre (NCSC). (2024). Strategy of the NCSC.
https://www.ncsc.admin.ch/ncsc/en/home/ueber-ncsc/strategie-bacs.html

[43] European Union Agency for Cybersecurity (ENISA). (2024). ENISA Threat Landscape 2024 (ISBN: 978-92-9204-675-0; DOI: 10.2824/0710888).
https://securitydelta.nl/media/com_hsd/report/690/document/ENISA-Threat-Landscape-2024.pdf

[44] MITRE Corporation. (2024). MITRE ATT&CK®: A knowledge base of adversary tactics and techniques. https://attack.mitre.org/

[45] Lockheed Martin. (2011). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

[46] Obaid, M., & Szalay, Z. (2020). A novel model representation framework for cooperative intelligent transport systems. Periodica Polytechnica Transportation Engineering, 48(1).
https://doi.org/10.3311/PPtr.13759

[47] Be-Mobile. (n.d.). Cooperative Intelligent Transport Systems (C-ITS) [Image].
https://be-mobile.com/solutions/traveler-information/cooperative-intelligent-transport-systems-c-its

[48] Williams, T. J. (1994). The Purdue enterprise reference architecture. Computers in Industry
https://www.pera.net/Pera/Report_160_Handbook/PERA_Handbook.pdf

[49] EBP. (n.d.). Swiss Traffic Management (Swiss TM). Retrieved October 2024, from https://www.ebp.ch/en/projects/swiss-traffic-management-swiss-tm

[50] Cegelec Mobility. (2016). Supervision systems, Neuchâtel, Switzerland. Retrieved October 2024, from https://www.mobility-way.com/en/references/supervision-systems-neuchatel-switzerland/

[51] United Nations Economic and Social Council. (2001). Recommendations of the group of experts on safety in road tunnels. Retrieved October 2024, from
https://unece.org/DAM/trans/doc/2002/ac7/TRANS-AC7-09e.pdf

[52] Swiss Federal Railways SBB. (n.d.). Rail Control System (RCS) – the future of traffic management. Retrieved October 2024, from
https://bahninfrastruktur.sbb.ch/fr/produits-prestations/systemes-informatiques/gestion-du-trafic/rcs.html

[53] Swiss Federal Railways SBB. (n.d.). Cybersecurity to protect SBB. Retrieved October 2024, from
https://company.sbb.ch/en/the-company/responsibility-society-environment/safety/information-security/cyber-security.html

[54] Audi of America. (n.d.). Tech talk: Audi, Traffic Light Information and the future of what—and how—to drive. Retrieved October 2024, from https://media.audiusa.com/en-us/releases/412

[55] 5G Open Road. (2023). La 5G pour une mobilité automatisée et connectée sur route ouverte. Retrieved October 2024, from http://5gopenroad.com/

[56] Transport Infrastructure Ireland. (n.d.). EU Connected Vehicle Pilot Study. Retrieved October 2024, from https://www.tii.ie/news/press-releases/eu-connected-vehicle-pilo/

[57] NLTimes. (2024, October 7). Tens of thousands of Dutch traffic lights vulnerable to hackers: report. NLTimes. https://nltimes.nl/2024/10/07/tens-thousands-dutch-traffic-lights-vulnerable-hackers-report

[58] Ruetir. (2024, October 7). Hacker can turn Dutch traffic lights green or red remotely. Ruetir. https://www.ruetir.com/2024/10/07/hacker-can-turn-dutch-traffic-lights-green-or-red-remotely/

[59] University of Applied Sciences and Arts Western Switzerland Fribourg (HEIA-FR). (2023). SecV2IComm: Validation of secure and reliable Vehicle-to-Infrastructure (V2I) communication. Retrieved May 2025, from https://www.heia-fr.ch/fr/recherche-appliquee/instituts/isis/projets-de-recherche/secv2icomm/

[60] Pajic, M., & Duke University. (2024, February 8). MadRadar hack can make self-driving cars 'hallucinate' imaginary vehicles and veer dangerously off-course. Live Science. https://www.livescience.com/technology/electric-vehicles/madradar-hack-can-make-self-driving-cars-hallucinate-imaginary-vehicles-and-veer-dangerously-off-course

[61] Toronto Transit Commission (TTC). (2021, November 1). TTC provides update on cyber security incident. TTC. https://www.ttc.ca/news/2021/November/TTC-provides-update-on-cyber-security-incident

[62] Zolder. (2020, September 18). Hacking the traffic light of the future. Zolder. https://zolder.io/blog/hacking-the-traffic-light-of-the-future/

[63] Railway-News. (2020, December 7). Global cyber attack hits Deutsche Bahn. Railway-News. https://railway-news.com/global-cyber-attack-hits-deutsche-bahn/

[64] British Broadcasting Corporation (BBC) News. (2016, November 28). Hackers hit San Francisco transport systems. BBC News. https://www.bbc.com/news/technology-38127096

[65] Knerler, K., Parker, I., & Zimmerman, C. (2022, March). 11 Strategies of a World-Class Cybersecurity Operations Center: Highlights. MITRE Corporation. https://qualias.net/11-strategies-of-a-world-class-cybersecurity-operations-center-highlights/

[66] Forum of Incident Response and Security Teams (FIRST). (2025). The Computer Security Incident Response Team (CSIRT) Services Framework Version 2.1. https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2-1

[67] Payment Card Industry Security Standards Council. (2024). Payment Card Industry Data Security Standard (PCI DSS) v4.0.1. https://www.pcisecuritystandards.org/pdfs/pci_ssc_quick_guide.pdf

[68] Sarbanes–Oxley Act of 2002, Pub. L. No. 107–204, 116 Stat. 745. https://www.sarbanes-oxley-act.com

[69] Federal Information Security Modernization Act of 2014, 44 U.S.C. § 3551 et seq. (2014). https://www.cisa.gov/topics/cyber-threats-and-advisories/federal-information-security-modernization-act

[70] Swisscom. (n.d.). Security Analytics and Security Operations Center (SOC). Retrieved May 2025, from https://www.swisscom.ch/en/business/enterprise/offer/security/threat-detection-and-response/security-analytics-and-soc.html

[71] ELCA Security. (n.d.). Senthorus: Swiss Next Generation SOC. Retrieved May 2025, from https://www.elcasecurity.ch/en/senthorus-mssp/about-senthorus-swiss-next-generation-soc

[72] terreActive. (n.d.). Security Operations Center. Retrieved May 2025, from https://www.terreactive.ch/en/security_operations_center

[73] Kudelski Security. (n.d.). Managed Security Services. Retrieved May 2025, from https://kudelskisecurity.com/services/managed-security/

[74] AXELOS. (2019). ITIL® Foundation: Information Technology Infrastructure Library (ITIL) 4 Edition. TSO (The Stationery Office). https://www.axelos.com/resource-hub/itil

Project conclusion

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'environnement, des transports, de l'énergie et de la communication DETEC
Office fédéral des routes OFROU

RECHERCHE DANS LE DOMAINE ROUTIER DU DETEC

Version du 09.10.2013

Formulaire N° 3 : Clôture du projet

établi / modifié le : 31.07.2025

Données de base

Projet N° : MB4_20_02G_01

Titre du projet : Roadmap for Swiss C-ITS Security Operation Center

Echéance effective : 31.08.2025

Textes :

Résumé des résultats du projet :

Cooperative Intelligent Transport Systems (C-ITS) and Vehicle-to-everything (V2X) technologies are reshaping mobility by allowing real-time data exchange between vehicles, infrastructure, and road users. As these interconnected systems become increasingly vital and exposed, their cybersecurity is a critical priority, especially given their classification as part of Switzerland's critical national infrastructure.

Following earlier research on proactive risk management, this report focuses on reactive cybersecurity, and more specifically the creation of a national Security Operations Center (SOC) for C-ITS. The objectives are to assess the need for such a SOC, examine possible models for its establishment, and provide a tailored roadmap for its implementation in Switzerland.

C-ITS introduces new cybersecurity challenges due to expanded communication between diverse stakeholders, including government, industry, and technology providers. The regulatory framework is complex, involving international standards, European directives, and new Swiss laws such as mandatory cyber incident reporting and minimum ICT standards aligned with global best practices.

A SOC is proposed as the central mechanism for monitoring, detecting, and responding to cyber threats across C-ITS assets, which include both information technology (IT) and operational technology (OT) elements. Adhering to the NIST Cybersecurity Framework, the SOC would be built on the core functions of governance, risk identification, threat detection, incident response, protection, and recovery, all supported by dedicated processes, technology, and skilled personnel.

Several organizational models were considered:

- In-house SOC: Full internal operation, offering maximum control but high costs.

- Outsourced (MSSP) SOC: Use of a Managed Service Provider, more cost-effective but with data sovereignty concerns.

- Hybrid SOC: Sensitive functions remain internal while certain tasks are outsourced, balancing control, flexibility, compliance, and cost.

A multi-criteria analysis identified the hybrid SOC as the optimal model. Deployment will follow a combined technological and geographical approach, starting with specific systems (e.g., traffic light RSUs) in a focused area, then scaling out across regions and technologies for broader coverage and maturity.

The roadmap to implementation includes six phases: foundation, build-out, initial operating capability, expansion/optimization, operation, and continuous improvement. Full national rollout is estimated within 36 months at a cost of CHF 6.2 million, with ongoing operational costs thereafter.

Key challenges include integrating diverse IT/OT environments, managing legacy systems, building a comprehensive asset inventory, balancing rollout priorities, and ensuring stakeholder engagement. Strong governance and specialized expertise, particularly during initial phases, are crucial for project success.

In conclusion, a centralized hybrid-model SOC is recommended for securing Switzerland's C-ITS infrastructure. Phased implementation will facilitate rapid readiness, compliance with regulatory requirements, and effective long-term resilience.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'environnement, des transports, de l'énergie et de la communication DETEC
Office fédéral des routes OFROU

Atteinte des objectifs :

The project successfully addressed its key aims by offering a well-grounded and context-aware analysis of the necessity, organizational options, and operating models for a national Security Operations Center tailored to C-ITS in Swiss road traffic. It considered both strategic and operational dimensions, balancing regulatory, technological, and practical aspects relevant to Switzerland. The analysis compared central and decentralized governance approaches, ultimately providing clear justification for a centralized model and establishing a concrete implementation roadmap. Overall, the project's findings and recommendations are closely aligned with Swiss needs and reflect international best practices, ensuring robust and pragmatic solutions for the secure operation of C-ITS infrastructure.

Déductions et recommandations :

The analysis confirms that Cooperative Intelligent Transport Systems (C-ITS), being a critical part of Switzerland's infrastructure, face significant and growing cyber risks due to their increasing complexity, interconnectivity, and exposure. It was found that decentralized or cantonal approaches are impractical because they add unnecessary complexity and cause fragmentation. Instead, a centralized approach, specifically a hybrid SOC model that combines in-house oversight of sensitive operations with selective outsourcing, offers the best balance of control, compliance, and operational efficiency needed to protect Swiss C-ITS effectively.

Based on these findings, it is recommended to move forward with establishing a centralized, hybrid SOC tailored for C-ITS. This should be done by following a phased roadmap that begins with focused pilot deployments and gradually expands both technologically and geographically. Early priority should be given to building a comprehensive asset inventory and setting clear governance structures to provide a solid foundation. Furthermore, SOC operations must continuously adapt to evolving regulatory demands and emerging best practices, supported by regular training, process improvements, and strong stakeholder engagement to ensure ongoing resilience and operational success.

Publications :

None
- [Bulletin.ch] publication to be prepared, and scheduled for Q1 2026

Chef/cheffe de projet :

Nom : Marty Prénom : Kilian

Service, entreprise, institut : CertX SA

Signature du chef/de la cheffe de projet :

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'environnement, des transports, de l'énergie et de la communication DETEC
Office fédéral des routes OFROU

RECHERCHE DANS LE DOMAINE ROUTIER DU DETEC

Formulaire N° 3 : Clôture du projet

Appréciation de la commission de suivi :

Evaluation :

Ce projet de recherche s'est focalisé sur la création d'un centre national d'opérations de sécurité pour les systèmes de transports intelligents coopératifs. Avec pour objectifs d'évaluer la nécessité d'un tel centre de compétences, d'examiner les modèles possibles pour sa mise en place et de fournir une feuille de route adaptée à sa mise en œuvre en Suisse. Une analyse multicritères a permis d'identifier une version hybride comme modèle optimal.
Les objectifs prédéfinis ont été atteints.

Mise en oeuvre :

Les structures de gouvernance d'un tel centre de compétences cyber sécuritaires nécessitent d'être clarifiées, de concert avec les exigences réglementaires et les avancées technologiques.
La mise en œuvre pourrait progressivement se faire de manière adaptative via des projets pilote, en intégrant toutes les parties prenantes pertinentes.

Besoin supplémentaire en matière de recherche :

Il y a un besoin supplémentaire en matière de recherche, notamment au niveau des enjeux critiques de la mise à l'échelle d'un tel centre d'opérations cyber sécuritaires à l'échelle nationale. Comme susmentionné, cela pourrait se faire via des projets pilotes de manière incrémentale.

Influence sur les normes :

Le travail s'est appuyé sur des règlements et directives suisse et internationales, dont la liste non exhaustive figure en fin de rapport.

Président/Présidente de la commission de suivi :

Nom : Ndzana Prénom : Bertrand

Service, entreprise, institut : DETEC - OFROU

Signature du président/ de la présidente de la commission de suivi :

Recherche dans le domaine routier du DETEC : Formulaire 3 **Page 3 / 3**