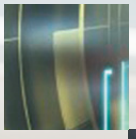
Manuel sur la cybersécurité destiné aux entreprises de transports publics



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'économie,
de la formation et de la recherche DEFR
Office fédéral pour l'approvisionnement économique du pays OFAE

VÖV UTP
Verband öffentlicher Verkehr
Union des transports publics
Unione dei trasporti pubblici

Préface

Chères lectrices, chers lecteurs,

Vous qui travaillez pour une entreprise de transport comptant parmi les infrastructures critiques de notre pays connaissez les attentes élevées en matière de sécurité, de fiabilité et de ponctualité vis-à-vis de notre branche. Vous avez conscience des nouveaux risques liés à l'interconnexion croissante des systèmes et des installations et à la complexité grandissante des systèmes informatiques, et savez que le danger de cyberattaques ciblées ne saurait être ignoré. Afin d'assurer, à l'avenir également, une protection optimale de ces infrastructures, il s'agit de trouver un juste équilibre, en alliant technologies de sécurité performantes, directives adéquates, stabilité des processus et sensibilisation des collaborateurs à la question de la cybersécurité.

Le présent manuel vous aide à mettre en place de manière efficace les principales mesures de protection en vue d'éviter des perturbations liées à des cyberincidents ou d'y remédier dans les plus brefs délais. Il s'adresse aussi bien aux petites qu'aux grandes entreprises de transport. En utilisant ce manuel, qui fournit des directives et des recommandations reconnues, vous appliquez la norme minimale pour les TIC recommandée par l'Office fédéral pour l'approvisionnement économique du pays (OFAE) et contribuez, dans le même temps, à renforcer la résilience informatique de votre exploitation et, plus largement, de toute la branche des transports publics.

Cette première édition du manuel, qui sera régulièrement actualisé et, le cas échéant, complété, a été réalisée conjointement par des spécialistes du secteur privé et des experts de l'OFAE sur mandat de l'UTP. L'UTP espère ainsi fournir à ses membres des recommandations pragmatiques, qui permettront une maîtrise commune des défis posés par la cybersécurité.

Je vous souhaite, chères lectrices, chers lecteurs, plein succès dans cette démarche !

Ueli Stückelberger
Directeur de l'UTP

Résumé

Le présent manuel, qui s'adresse aux entreprises de transports publics en Suisse, formule des recommandations sur la manière de réduire les cyberrisques à un niveau acceptable. Élaboré par les acteurs de la branche, il a pour but d'aider les prestataires de transports publics à améliorer la cybersécurité[1] au sein de leur entreprise. La mise en œuvre d'une stratégie dite de défense en profondeur (defence in depth), reconnue à l'heure actuelle comme une stratégie efficace pour faire face aux cybermenaces, fait partie des recommandations clés de ce document. Cette stratégie inclut des recommandations sur les technologies de l'information et de la communication (TIC) qui doivent être appliquées, par les collaborateurs des entreprises concernées, à l'aide de processus efficaces et efficients. Par ailleurs, le manuel passe en revue différents instruments et fournit notamment un cadre (framework) assorti d'un outil Excel qui permet à l'entreprise de recenser ses capacités, de les évaluer, de les comparer, et de les développer de manière ciblée. Le présent manuel, qui est compatible avec normes internationales, s'appuie sur le NIST Cybersecurity Framework Core[2] et sur les conclusions et mesures à prendre formulées dans l'analyse des risques et des vulnérabilités dans le sous-secteur transport et logistique[3].

[1] On entend par cybersécurité toutes les mesures organisationnelles et techniques visant à préserver la disponibilité, l'intégrité et la confidentialité des informations s'agissant aussi bien des TIC que des systèmes de contrôle industriel (SCI).

[2] Développé par le National Institut of Standards and Technology (autorité fédérale américaine), le NIST Cybersecurity Framework (NIST CSF) est un cadre de cybersécurité qui s'est imposé comme norme dans de nombreux pays.

[3] OFAE, Risiko- und Verwundbarkeitsanalyse des Teilsektors Transport und Logistik, Berne, 2017.

Tables des matières

Introduction et but

La Suisse est fortement tributaire de la continuité du fonctionnement des infrastructures critiques. Ces infrastructures assurent la fourniture de biens et services cruciaux comme l'énergie, la communication ou les transports. Leur défaillance, qu'elle soit partielle ou totale, a de lourdes conséquences sur l'économie et la population et compromet le fonctionnement, la sécurité et la prospérité de la Suisse. Conformément à l'art. 2, al. 2, de la Constitution, la Confédération est tenue de favoriser « la prospérité commune, le développement durable, la cohésion interne et la diversité culturelle du pays ». Il s'ensuit que la protection des infrastructures critiques est une des tâches principales de l'État, qui ne peut cependant être menée à bien sans le concours du secteur privé.

1.1 Généralités

La nouvelle loi sur l'approvisionnement du pays, entrée en vigueur le 1er juin 2017, donne à l'OFAE la compétence de mettre en œuvre, à titre subsidiaire, des mesures préventives pour accroître la sécurité de l'approvisionnement. Le présent manuel figure parmi ces mesures préventives. Conformément au principe de subsidiarité, il est conçu sous la forme d'une recommandation à l'intention des acteurs du secteur.

En application de la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC), l'Approvisionnement économique du pays (AEP), et plus précisément l'OFAE, a procédé à une analyse des failles informatiques dans le secteur des transports publics. Les analyses des risques et des vulnérabilités dans les sous-secteurs du transport routier (2015) et du transport ferroviaire (2017) ont été réalisées et vérifiées conjointement par la Confédération et les membres de l'AEP. Elles ont porté notamment sur le rapport de dépendance de ces sous-secteurs à l'égard des ressources informatiques. Il ressort que la dépendance du transport ferroviaire est tendanciellement plus élevée que celle du transport routier.

Les transports publics suisses sont uniques au monde. Grâce à un horaire cadencé en réseau et de bonnes options de correspondance, ils offrent aux voyageurs une chaîne de transport continue incluant tous les moyens de transport (train, bus, tram, bateau, téléphérique), comme illustré à la figure 1. En plus de répondre aux besoins grandissants en matière de mobilité, les transports publics ont une grande importance économique et assurent la desserte de l'entier du territoire.

Figure 1 : Types de transports publics

L'interconnexion croissante des moyens de transport facilite le déplacement d'un point A à un point B, tout en augmentant les efforts à fournir par les acteurs de la branche pour se conformer aux prescriptions légales toujours plus nombreuses et pour sécuriser les composants et systèmes de commande aussi bien à l'intérieur qu'à l'extérieur.

La figure suivante présente un scénario possible d'évolution et de développement de la chaîne de mobilité dans le contexte d'une ville intelligente grâce à des pôles (hubs) de mobilité intégrant un nombre grandissant de moyens de transport (covoiturage, vélos électriques, etc.) à l'offre de transports en commun.

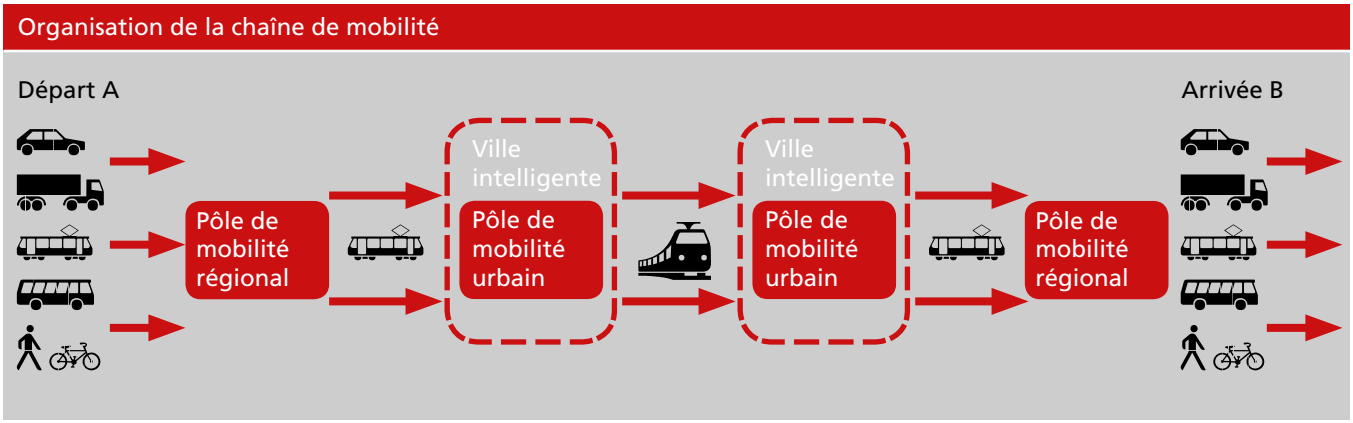


Figure 2 : La chaîne de mobilité du futur

L'informatisation et l'interconnexion croissantes de presque tous les domaines du quotidien offrent des potentiels qu'un pays industrialisé et très développé comme la Suisse se doit de saisir. La technicisation est déjà très avancée dans le domaine des transports publics. Tous les processus importants sont déjà pris en charge par des systèmes informatiques, lesquels sont indispensables au maintien de la cadence millimétrée des transports en commun. Dans le sillage de la progression de la dématérialisation de tous les éléments des transports publics, la dépendance à l'égard des systèmes informatiques s'accroît, tout comme les exigences en matière de cybersécurité. Or qui dit numérisation, dit nouveaux risques et nouvelles sources de vulnérabilité et d'erreurs pouvant déboucher sur des perturbations ayant des répercussions négatives sur l'activité de l'entreprise et, partant, appelant une réaction. Vu les exigences élevées en termes de sécurité à l'égard des transports en commun, les véhicules touchés par une panne affectant des systèmes importants pour la sécurité ne sont pas autorisés à poursuivre leur course, ou alors uniquement à vitesse réduite, ce qui limite considérablement la disponibilité de l'infrastructure.

1.2 But du manuel

Les entreprises de transports publics sont des cibles attrayantes pour les pirates informatiques. En effet, elles disposent d'interfaces web pour bon nombre de leurs plateformes informatiques et de leurs systèmes et installations SCADA. Elles risquent par conséquent d'être visées par des cyberattaques. Des versions de rançongiciels encore inconnues ou l'augmentation de vecteurs d'attaque et de failles sont autant de facteurs permettant l'émergence de « scénarios d'attaque » inédits. Afin de limiter autant que possible la vulnérabilité des processus et des systèmes informatiques, les entreprises de transports publics veillent à préserver la robustesse des processus, systèmes et installations. Ces derniers doivent faire l'objet de tests réguliers afin d'exclure tout impact sur la disponibilité et l'intégrité des transports en commun.

Les entreprises de transports publics doivent continuer à se protéger contre les attaques et améliorer les mesures préventives en continu. Il est à cet effet crucial qu'elles puissent compter sur une protection de base solide et conforme aux normes. Toutefois, il n'est pas possible de couvrir adéquatement tous les risques par des mesures préventives (ce ne serait d'ailleurs pas judicieux financièrement). À l'avenir, il faudra donc accorder nettement plus de poids aux mesures permettant de déceler les attaques ou tentatives d'attaque et à une réaction adéquate et rapide. Ce n'est que de cette manière que les entreprises de transports publics pourront gérer les cyberrisques de façon satisfaisante. À noter que les échanges et la coopération avec d'autres entreprises, des partenaires et des acteurs scientifiques font partie intégrante de la démarche.

La sécurité informatique présuppose que chaque exploitant assume ses responsabilités en étant conscient des risques et en recourant à des systèmes fiables. L'application des mesures éprouvées décrites dans ce manuel suffit déjà à prévenir bon nombre de perturbations informatiques et de cyberattaques

moyennant un investissement raisonnable. Le présent manuel a pour objectif de fournir aux entreprises et organismes un outil polyvalent grâce auquel ils pourront améliorer la résilience de leur infrastructure informatique. L'approche fondée sur les risques qui y est proposée permet aux entreprises et organismes d'instaurer différents niveaux de protection en fonction de leurs besoins.

1.3 Champ d'application

Le présent manuel a été élaboré par l'AEP en collaboration avec des experts externes. Il existe à ce jour plusieurs normes de sécurité informatique reconnues sur le plan international, qui vont pour la plupart au-delà du cadre posé ici (cf. tableau 54). Le manuel ne prétend pas concurrencer les normes existantes, mais il est compatible avec ces dernières, même si sa portée est moindre. Il se veut une bonne entrée en matière sur la question de la cybersécurité tout en assurant un niveau de protection élevé.

Les recommandations destinées aux acteurs de la branche relèvent de l'autorégulation et sont donc facultatives. Le manuel s'adresse à l'ensemble des entreprises et organismes participant à l'organisation des transports publics. Il sera actualisé au besoin.

Le manuel se concentre sur les processus internes ayant un impact direct sur la conception et la fourniture de prestations de transport des acteurs définis dans le tableau ci-dessous.

Gestionnaires de l'infrastructure ferroviaire (GI)	Entreprises bénéficiant d'une concession et d'un agrément de sécurité au sens de l'art. 5 de la loi fédérale sur les chemins de fer (LCdF) pour la construction et l'exploitation d'une infrastructure ferroviaire. Le terme *infrastructure ferroviaire* désigne les installations des chemins de fer, y compris les lignes de transport du courant de traction.
Entreprises de transport ferroviaire (ETF)	Entreprises assurant des prestations de transport ferroviaire. Selon l'art. 8*c* LCdF, quiconque veut effectuer des transports de personnes ou de marchandises en utilisant une infrastructure ferroviaire doit être en possession d'une autorisation d'accès au réseau et d'un certificat de sécurité.
Entreprises de transport de voyageurs concessionnaires	Entreprises disposant d'une concession au sens de l'art. 6 de la loi sur le transport de voyageurs (LTV) pour le transport régulier et professionnel de voyageurs par chemin de fer, tram, installation à câbles, bateau ou véhicule motorisé à propulsion thermique ou électrique.

Tableau 1 : Acteurs des transports publics

Le niveau de protection doit être garanti sur l'intégralité des itinéraires ayant une fonction de desserte selon l'art. 5 de l'ordonnance du 4 novembre 2009 sur le transport de voyageurs (OTV ; RS *745.11*). Une ligne a une fonction de desserte lorsqu'il y a un point de jonction avec le réseau supérieur des transports publics à au moins une des extrémités de la ligne et une localité à l'autre extrémité ou entre les extrémités. Sont considérés comme des localités les espaces construits habités toute l'année et comprenant au moins 100 habitants dans :

- les zones à bâtir continues au sens de la loi du 22 juin 1979 sur l'aménagement du territoire, y compris les zones de protection des eaux, les sites importants, les lieux historiques et les monuments culturels ;
- les habitats dispersés traditionnels ;
- les vallées des régions de montagne dont la desserte se fait à partir d'un point commun.

1.4 Mode d'emploi du manuel

Le manuel se compose de plusieurs chapitres : les chapitres 1 et 2 introduisent la thématique des transports publics, le chapitre 3 détaille l'approche de la défense en profondeur *(defence in depth)* et les chapitres 4 et 5 décrivent les mesures à mettre en œuvre et présentent des outils à cet effet.

Les entreprises et organismes peuvent recourir à l'outil d'évaluation « Norme minimale TIC » pour évaluer leur degré de maturité en matière de cybersécurité. La norme minimale pour les TIC est considérée comme satisfaite si la cote globale de l'évaluation de la cybersécurité correspond à la valeur minimale requise.

Processus critiques dans les transports publics

Pour aborder la question de la cybersécurité dans les transports publics, il convient tout d'abord de définir les principaux acteurs du secteur, les processus considérés comme critiques et les rapports de dépendance des systèmes d'importance systémique.

2.1 Principaux processus opérationnels

Le présent manuel vise à garantir la cybersécurité pour les processus importants dans le secteur des transports, plus particulièrement dans le sous-secteur des transports en commun par le rail et par la route. Les prescriptions et les mesures de mise en œuvre qu'il contient peuvent cependant également être appliquées au transport de voyageurs par installation à câbles et par bateau.

Les processus opérationnels informatisés sont détaillés ci-après.

2.1.1 Transport ferroviaire

Trois réseaux sont nécessaires au bon fonctionnement du trafic ferroviaire : *le réseau de communication* (réseaux fixe et mobile), qui permet d'échanger les données requises pour la sécurité, la qualité, le maintien et la poursuite du trafic, *le réseau électrique,* qui constitue la principale source d'alimentation en énergie, et enfin *le réseau ferroviaire* et les infrastructures s'y rapportant (installations de sécurité incluses), qui, une fois construits, nécessitent une maintenance régulière en vue de permettre la bonne circulation des trains et des tramways. Le schéma ci-dessous offre un aperçu des processus informatisés dans le transport ferroviaire.

Par ailleurs, les installations de maintenance et de sécurité ferroviaire s'apparentent de plus en plus à des « systèmes » numériques d'une grande complexité. Les installations de sécurité ferroviaire, qui comprennent notamment les systèmes de signalisation (comme ETCS), sont généralement télécommandées, grâce à des systèmes informatiques, depuis une centrale d'exploitation (contrôle-commande). Des réseaux de communications numériques, devenus indispensables au maintien et à la poursuite de l'exploitation du rail, relient et intègrent l'ensemble des installations de technique ferroviaire, y compris les applications informatiques d'exploitation ferroviaire (systèmes de gestion du trafic, p. ex.).

Tout passe par l'informatique, de la mise en réseau des installations fixes à la technique des véhicules, en passant par l'exploitation ferroviaire. Les systèmes et installations peuvent être classés en plusieurs catégories, selon leur fonction première : information, commande ou sécurité.

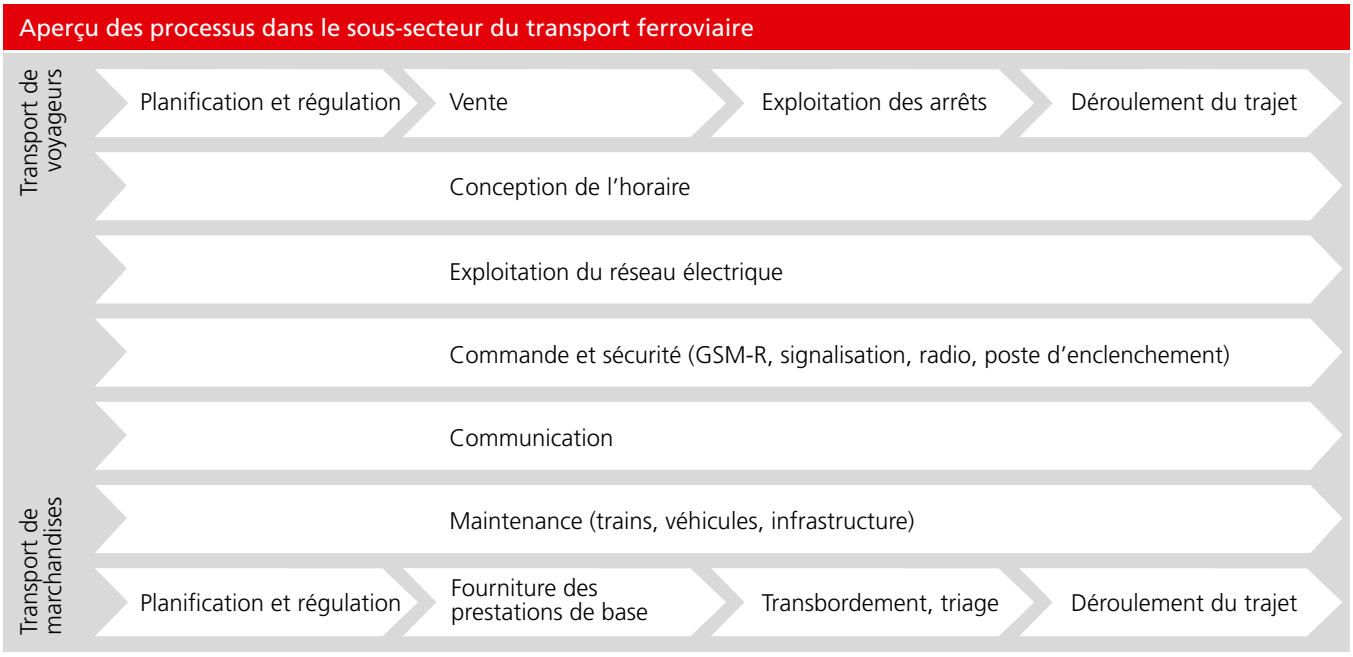


Figure 3 : Aperçu des processus informatisés dans le trafic ferroviaire

2.1.2 Transport routier

Caractérisé par l'interaction de plusieurs acteurs, le système des transports publics routiers se compose de processus complémentaires, se chevauchant sous les angles temporel et géographique. Les TIC sont utilisées non seulement pour la commande et la surveillance des éléments d'infrastructure (éclairage des routes, aération des tunnels, etc.), mais aussi pour la gestion et la surveillance du trafic (détecteurs d'embouteillages, caméras, déviations, systèmes d'affichage dynamique de la vitesse) et l'information des usagers (annonces d'embouteillages, systèmes de navigation). Par ailleurs, les véhicules modernes eux-mêmes sont équipés d'un nombre croissant de dispositifs électroniques. La palette est large : dispositifs d'immobilisation, électronique de loisirs, contrôle des performances moteur, systèmes d'antipatinage, systèmes d'aide au maintien dans la voie, etc.

En tant qu'usagers de la route, les entreprises de bus et de trams ont aussi recours à ces systèmes. Elles disposent en outre de tout un éventail de systèmes de commande (système de contrôle, radio, VoIP, système de localisation, etc.) et de systèmes d'information (dans et sur le véhicule, aux arrêts, sur l'internet).

Les entreprises de transports publics sont en outre connectées à plusieurs systèmes du réseau routier (commande des feux de circulation, p. ex.).

S'agissant des TIC dans les transports publics routiers, il faut considérer, d'une part, les TIC des propriétaires des routes (Confédération, cantons, communes), sur lesquelles les entreprises de transport concessionnaires (ETC) n'ont pas ou peu d'influence, et, d'autre part, les TIC de ces dernières, dont elles sont seules responsables.

2.2 Processus critiques dans les transports publics

Ces dernières années, le recours aux systèmes informatiques au sein des chaînes de transport et de services logistiques s'est encore accru. Cette révolution technologique permet la commande et la régulation centralisées d'informations en temps réel. La direction de l'exploitation du réseau en devient bien plus agile, avec la possibilité de réagir de manière automatisée et beaucoup plus rapide aux incidents critiques inattendus. Or la numérisation s'accompagne de nouveaux risques, que les entreprises de transport et de logistique se doivent d'identifier, d'évaluer et de gérer pour être en mesure d'accomplir leur mandat légal.

Processus critiques		
Infrastructure	Trafic, transport	Gouvernance d'entreprise
• Cycle de vie de l'infrastructure	• Cycle de vie des véhicules	• Gestion d'entreprise (normative, stratégique et opérationnelle)
• Maintenance de l'infrastructure	• Planification des prestations de transport	• Exploitation informatique et interface avec les SCI
• Gestion des voies de communication	• Fourniture des prestations de transport	• Finances et comptabilité
• Gestion du trafic	• Vente des prestations de transport	• Gestion de crise et des situations d'urgence

Tableau 2 : Processus critiques dans les transports publics

Les différents processus critiques sont décrits brièvement dans les paragraphes ci-après.

2.2.1 Processus liés à l'infrastructure

Cycle de vie de l'infrastructure

L'infrastructure des ETC englobe la totalité des réseaux, systèmes et installations nécessaires à l'exploitation des transports publics, comme les rails (*infra*structure), les lignes de contact (*super*structure), les installations de sécurité ou les centrales d'exploitation. Le cycle de vie de l'infrastructure comprend toutes les étapes allant de la conception à l'élimination, en passant par le développement, la réalisation et la mise hors service.

Maintenance de l'infrastructure

La maintenance de l'infrastructure fait l'objet d'une planification minutieuse. Elle comprend entre autres un contrôle régulier de l'état des installations d'infrastructure. Certaines entreprises de transports publics ont recours à des systèmes ERP *(enterprise resource planning)* pour planifier les travaux d'entretien, ce qui aboutit souvent à des solutions individuelles pour les différents travaux.

Gestion des voies de communication

La gestion des voies de communication passe par la planification des voies disponibles *(slots)* et leur attribution éventuelle aux ETC. Les lignes et créneaux attribués sont enregistrés dans les systèmes *back-end* (bases de données) des entreprises de transports publics.

Gestion du trafic

La gestion du trafic consiste à surveiller et à commander les trains, les trams et les bus, et à actionner les aiguillages et les signaux. Les systèmes de contrôle industriels (SCI ; cf. ch. 3.5.1) sont aujourd'hui indispensables à la surveillance et à la commande des transports publics. Une panne de ces systèmes de contrôle due, par exemple, à un cyberincident entraînerait des pertes de capacité voire une interruption du trafic sur les tronçons concernés.

2.2.2 Processus liés au trafic et au transport

Cycle de vie des véhicules

L'intégralité du cycle de vie des véhicules est planifiée et gérée par informatique. Sans TIC, les entreprises de transports publics seraient confrontées à un défi de taille, qui risquerait d'entraîner la suppression de liaisons de transport en l'espace de quelques jours. Seule une partie des processus du cycle de vie pourrait être assurée sans recours à l'informatique sur une durée prolongée.

Planification des prestations de transport

L'horaire, dont la planification est coordonnée au moins une année à l'avance, n'est pas pour autant un document statique. L'avancée de la numérisation entraîne une plus grande flexibilité, et il est aujourd'hui possible de procéder à des modifications ou améliorations en temps réel, et même parfois de manière automatisée. L'horaire sert de référence pour décider de l'affectation des véhicules et du personnel. Une défaillance des systèmes en jeu aurait des répercussions considérables sur les transports publics.

Fourniture de prestations de transport

Le bon déroulement d'un trajet en train, en tram ou en bus est largement tributaire des SCI et systèmes informatiques (information à la clientèle, p. ex.). Pour donner un exemple, seuls les véhicules équipés du système ETCS peuvent circuler sur les nouveaux tronçons ferroviaires, les signaux ne s'affichant désormais plus que sur un écran dans la locomotive. S'agissant des bus et des trams, le respect des distances entre les différents véhicules d'une même ligne peut être contrôlé par un système de commande. Sans un tel système, il ne serait aujourd'hui plus possible de garantir la fiabilité et la ponctualité des transports publics.

Vente de prestations de transport

Le processus de vente peut s'effectuer par plusieurs canaux, que ce soit au guichet, sur un site internet, grâce à une appli ou par un automate à billets. Une défaillance des systèmes de vente ou des interfaces avec des prestataires externes de services financiers (SIX Payment, banques, etc.) peut occasionner des pertes pour les entreprises de transport. Le comptage des passagers joue également un rôle important dans la répartition des recettes.

2.2.3 Processus liés à la gouvernance d'entreprise

Gestion d'entreprise

Une défaillance des systèmes centraux d'information servant à la gestion d'entreprise (système ERP, p. ex.) compromettrait aujourd'hui la conduite de n'importe quelle grande entreprise. Dans le domaine des transports en commun, cela vaut, entre autres, pour les *management cockpits* et les logiciels de gestion financière, de gestion de projets ou encore d'administration du personnel.

Exploitation informatique et interface avec les SCI

Dans le domaine des transports publics, tous les processus importants sont pris en charge par des systèmes informatiques et des SCI. Les centres de calcul, les réseaux de communication, les applications (TIC et SCI) en font notamment partie. La bonne marche des transports publics à long terme ne peut être assurée sans systèmes informatiques fonctionnels.

Finances et comptabilité

La comptabilité financière et la comptabilité d'exploitation sont gérées la plupart du temps à l'aide de systèmes centraux (ERP, p. ex.). Des pannes (lors du versement des salaires, p. ex.) ou des dysfonctionnements graves affectant ces systèmes peuvent entraîner à moyen terme une remise en cause de l'existence même des ETC.

Gestion de crise

Les systèmes de communication, en particulier, sont cruciaux dans l'optique de la gestion de crise. Selon le type de crise qui se présente, ils peuvent cependant n'être disponibles que de manière restreinte, voire être complètement hors service. Il est crucial pour les ETC d'être bien préparées en cas de crise. À cet effet, il est indispensable de mettre sur pied une prévention globale des situations d'urgence, avec des plans et systèmes d'urgence actualisés et testés régulièrement.

2.3 Dépendance des processus critiques à l'égard des systèmes informatiques

Les processus mentionnés plus haut dépendent du fonctionnement stable et sûr des systèmes informatiques nécessaires à leur mise en œuvre. Par conséquent, les systèmes et installations comptent aussi parmi les ressources critiques pour les transports publics. Un processus peut être tributaire de plusieurs systèmes informatiques ; à l'inverse, un système informatique peut représenter une ressource critique pour plusieurs processus opérationnels.

Il est donc primordial que chaque entreprise de transports publics documente de manière exacte et durable les processus, systèmes et installations qui sont les siens (architecture du système). La protection contre les risques suppose de connaître ce qui doit être sécurisé.

Les options de présentation ci-dessous illustrent comment visualiser et documenter les rapports de dépendance des processus opérationnels à l'égard des principaux systèmes informatiques ou des fonctionnalités de ces derniers. Il est possible d'opter pour différents niveaux de granularité et de combiner plusieurs modes de documentation.

La figure 4 met en évidence la complexité des processus critiques. Le nombre de liens entre un processus critique et les différents systèmes illustre la forte dépendance à l'égard des systèmes informatiques et des systèmes de commande de surveillance et d'acquisition de données (SCADA).

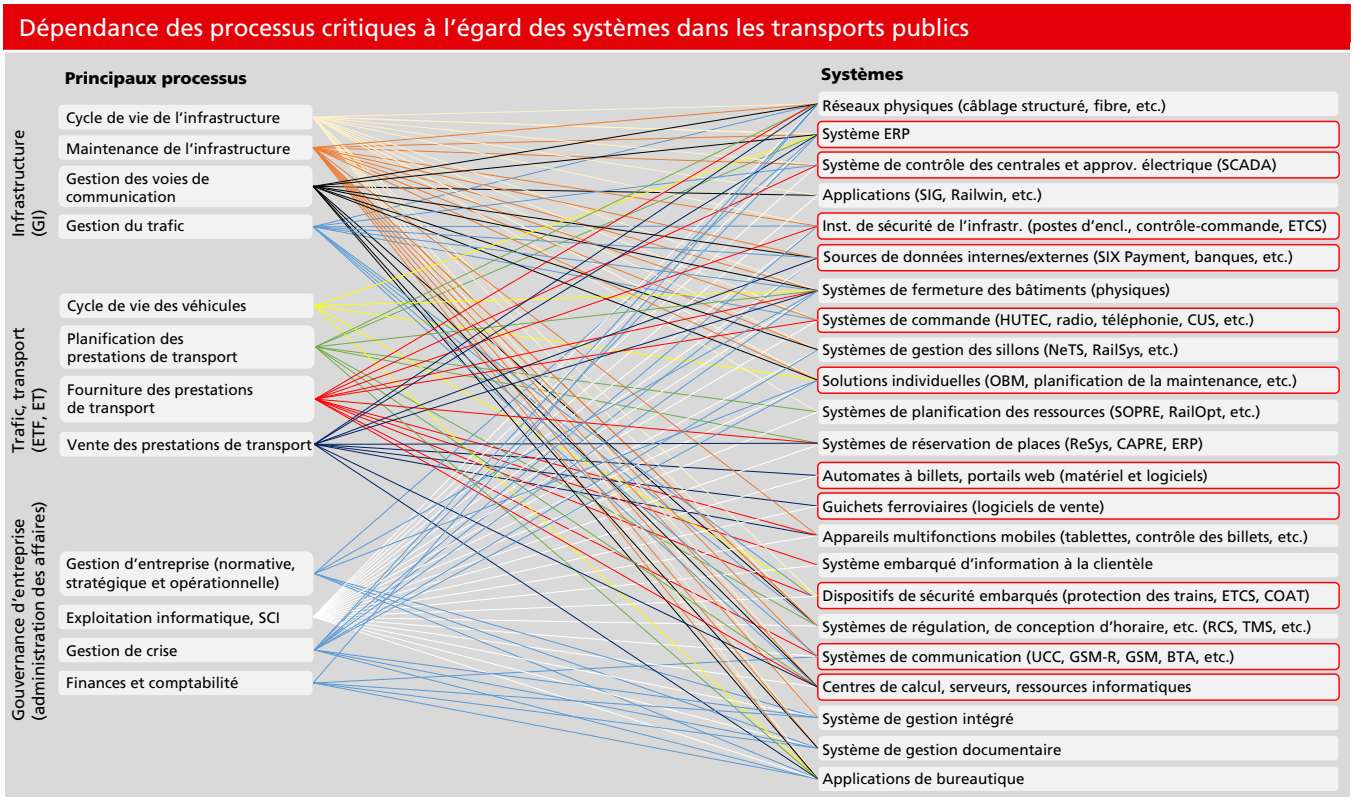


Figure 4 : Dépendance à l'égard des systèmes informatiques et SCADA

Le tableau ci-après montre, à l'aide d'une matrice, la dépendance des processus critiques à l'égard des systèmes dans le secteur des transports en commun. Il revient à chaque entreprise ou organisme de vérifier si chacun des rapports de dépendance prend effectivement cette forme dans son cas. À cette fin, les auteurs du présent manuel suggèrent d'effectuer des analyses concrètes sur la base des bilans d'impact sur l'activité (BIA) réalisés au sein de l'entreprise ou de l'organisme concerné. Des exemples de questions simples permettant de mettre au point un BIA figurent en annexe.

Gouvernance d'entreprise (administration des affaires)				Trafic, transport (ETF, ET)					Infrastructure (GI)				
Gestion de crise	Finances et comptabilité	Exploitation informatique, SCI	Gestion d'entreprise (normative, stratégique et opérationnelle)	Vente des prestations de transport	Fourniture des prestations de transport	Planification des prestations de transport	Cycle de vie des véhicules		Gestion du trafic	Gestion des voies de communication	Maintenance de l'infrastructure	Cycle de vie de l'infrastructure	
×	×	×		×	×	×			×	×	×	×	Réseaux physiques (câblage structuré, fibre, etc.)
	×	×	×	×		×	×			×	×	×	Système ERP
		×			×				×		×	×	Système de contrôle des centrales électriques (SCADA)
		×								×	×	×	Applications (géoapplications, SIG, Railwin, etc.)
×		×			×				×		×	×	Inst. de sécurité de l'infrastr. (postes d'encl., contrôle-commande, ETCS)
	×	×		×					×	×	×		Sources de données internes/externes (SIX Payment, banques, fournisseurs)
	×	×	×	×	×	×	×		×	×	×	×	Systèmes de fermeture des bâtiments (physiques)
		×			×				×		×	×	Systèmes de commande (HUTEC, radio, téléphonie, CUS, etc.)
	×	×								×	×	×	Systèmes de gestion des sillons (NeTS, RailSys, etc.)
	×	×	×				×			×	×	×	Solutions individuelles (OBM, planification, etc.)
		×				×						×	Systèmes de planification des ressources (SOPRE, RailOpt, etc.)
		×		×	×	×							Systèmes de réservation de places (ReSys, CAPRE, ERP)
		×		×									Automates à billets, portails web (matériel et logiciels)
		×		×									Guichets ferroviaires (logiciel de vente)
		×		×	×						×		Appareils multifonctions mobiles (tablettes, contrôle des billets, etc.)
		×			×								Système embarqué d'information à la clientèle
		×			×		×		×			×	Dispositifs de sécurité embarqués (protection des trains, ETCS, COAT)
		×			×	×			×	×	×		Systèmes de régulation, de conception d'horaire, etc. (RCS, TMS, etc.)
×		×			×				×		×		Systèmes de communication (UCC, GSM-R, GSM, BTA, etc.)
		×		×	×	×			×	×	×	×	Centres de calcul, serveurs, ressources informatiques
×	×	×	×								×	×	Système de gestion intégré
×	×	×	×							×	×	×	Système de gestion documentaire
×	×	×	×	×		×	×			×	×	×	Applications de bureautique

Dépendance des processus critiques à l'égard des systèmes dans les transports publics

Tableau 3 : Dépendance des processus critiques à l'égard des systèmes dans les transports publics

Le tableau ci-dessous indique le degré de dépendance informatique de chacun des processus critiques évalués plus haut. La question fondamentale qui se pose ici est la suivante : le processus peut-il aboutir sans recours aux TIC (dépendance informatique) ? Le degré de dépendance informatique est classé en trois catégories (faible, moyen ou élevé). Le degré de dépendance d'un processus est considéré comme faible dès lors que celui-ci peut être exécuté pour l'essentiel sans ressources informatiques. Il est jugé moyen lorsque l'exécution du processus nécessiterait un surplus de ressources (temps, personnel, etc.) en l'absence d'outils informatiques. Enfin, il est considéré comme élevé si le processus est impossible à réaliser en cas de panne informatique.

Par ailleurs, une proposition d'exigence minimale uniforme à atteindre en termes de maturité est définie (cf. ch. 4.3).

Processus critiques dans les transports publics		
Processus	Degré de dépendance informatique	Exigences en termes de maturité
Infrastructure	(faible, moyen ou élevé)	(cf. chap. 4)
Cycle de vie de l'infrastructure	moyen	2–3
Maintenance de l'infrastructure	élevé	2–3
Gestion des voies de communication	élevé	3–4
Gestion du trafic	élevé	3–4
Trafic, transport		
Cycle de vie des véhicules	moyen	3–4
Planification des prestations de transport	élevé	2–3
Fourniture des prestations de transport	élevé	3–4
Vente des prestations de transport	moyen	2–3
Gouvernance d'entreprise		
Gestion d'entreprise (normative, stratégique, opérationnelle)	moyen	3–4
Exploitation informatique et interface avec les SCI	élevé	2–3
Finances et comptabilité	moyen	2–3
Gestion de crise et des situations d'urgence	élevé	2–3

Tableau 4 : Degré de dépendance informatique des processus critiques

Cette proposition peut être adaptée au cas par cas en fonction des BIA et des analyses d'interfaces réalisés au sein des entreprises ou organismes. Le degré de maturité ne devrait toutefois pas être inférieur à 2.

2.4 Résilience des processus informatiques et des systèmes et installations

De manière générale, la résilience désigne la capacité de systèmes à surmonter les perturbations. Dans le contexte de la SNPC, « résilience » (ou « résilience informatique ») s'entend de la capacité des processus critiques évalués à résister aux perturbations touchant les systèmes informatiques.

La résilience va au-delà de la question de la redondance des systèmes et porte également sur des aspects organisationnels. Les mesures organisationnelles à prendre pour améliorer la résilience peuvent, entre autres, passer par l'élaboration de directives concernant les autorisations ainsi que la sauvegarde des données, une organisation stricte de la gestion des correctifs *(patches)* et la détection précoce des risques. En outre, la question de la réalisation d'un processus par un système redondant non informatisé se pose à chaque fois. Si un système d'information donné tombe inopinément en panne, les informations peuvent être communiquées de vive voix, par courriel ou par téléphone.

La résilience systémique doit par ailleurs être prise en considération en tout temps. Plusieurs systèmes peuvent, par exemple, assumer la même fonction, ou la vitesse de fonctionnement de certains systèmes peut être revue à la hausse ou à la baisse pour compenser le dysfonctionnement d'un autre système. Prenons l'exemple du réseau électrique : en cas de défaillance d'un producteur intégré au réseau (une centrale hydraulique, p. ex.), il est possible de compenser la diminution de la production indigène par l'importation d'électricité d'autres sources. Cette résilience systémique doit être prise en compte lors de l'évaluation de la résilience informatique.

Les entreprises ou organismes peuvent améliorer leur résilience en concrétisant et en mettant en œuvre les exigences et mesures exposées dans les deux prochains chapitres tout en respectant les normes de sécurité pertinentes.

2.5 Différence entre *security* et *safety*

Dans le jargon, *safety* (sécurité) s'emploie notamment pour désigner la protection des personnes et de l'environnement contre les dangers inhérents à un « système ». Elle englobe par exemple la prévention des accidents corporels. Le terme *security* (sûreté), quant à lui, s'entend plus particulièrement de la protection des personnes ou des systèmes en cas d'événement de force majeure ou d'acte de malveillance avec ou sans recours à la violence.

Il convient de garder toujours à l'esprit les aspects importants du point de vue de la sécurité dans l'analyse et l'exécution de mesures. Les entreprises de transports publics fournissent un service à la population de la Suisse (sous la forme de courses en bus, train, bateau, etc.). L'être humain est dès lors au cœur de ce service.

C'est pourquoi il y a lieu de combiner les prescriptions et mesures touchant à la sécurité avec celles relevant de la sûreté de façon à former un tout cohérent.

Éléments d'une stratégie de défense en profondeur

La défense en profondeur *(defence in depth)* désigne l'application coordonnée de plusieurs mesures de sécurité en vue de protéger les données et le traitement de l'information au sein d'une entreprise ou d'un organisme.

3.1 Grandes lignes de la défense en profondeur

Une entreprise doit axer sa stratégie de sécurité informatique sur la protection des actifs informatiques critiques qui sont indispensables aux processus opérationnels. À cette fin, elle doit adopter une approche à plusieurs niveaux, connue à l'international sous le nom de « stratégie de défense en profondeur », qui consiste à appliquer de façon coordonnée plusieurs mesures de sécurité en vue de protéger ses actifs informatiques. Cette approche s'inspire du principe militaire selon lequel un ennemi aura plus de difficultés à surmonter un système de défense multicouche complexe qu'à franchir une simple barrière. En parallèle, les méthodes et les modes opératoires des agresseurs potentiels sont étudiés pour y adapter les dispositifs de défense. Dans le contexte de la sécurité informatique, la défense en profondeur vise à détecter les atteintes à la sécurité informatique, à réagir à celles-ci et à atténuer leurs effets *(mitigate)*. Elle a recours à une approche globale, qui s'attache à protéger l'ensemble des actifs (y c. informatiques) contre n'importe quel risque. Une entreprise doit consacrer ses ressources à se prémunir efficacement contre les risques connus et à assurer une veille rigoureuse des risques potentiels. Des mesures appropriées doivent protéger l'intégralité des systèmes informatiques, y compris les personnes, les processus, les bâtiments, les données et les appareils. Un agresseur potentiel ne constitue une menace pour un système informatique que s'il parvient à exploiter une faille dans l'un de ces éléments. L'entreprise doit revoir régulièrement les mesures prises pour pouvoir, au besoin, les adapter aux nouvelles menaces.

La réalisation des différents plans de défense en profondeur peut fortement varier. Il existe d'importantes différences entre la bureautique et une technologie opérationnelle (TO ; autrement dit SCI ou SCADA), que ce soit au niveau des caractéristiques fondamentales ou des méthodes appliquées. Les quelques exemples présentés ci-dessous portant sur divers aspects touchant à la sécurité illustrent ces différences (cf. tableau 4).

Aspect touchant à la sécurité	TIC (bureautique, p. ex.)	TO (SCI ou SCADA) (gestion de la production, p. ex.)
Règles de sécurité	Prescriptions réglementaires générales, selon le secteur (pas tous les secteurs).	Directives réglementaires spécifiques, selon le secteur (pas tous les secteurs).
Cycle de vie de la technologie *(technology support life cycle)*	2 à 3 ans, plusieurs fournisseurs, développement continu et mises à niveau *(upgrades)* régulières.	10 à 20 ans, généralement un seul fournisseur ou prestataire de services sur tout le cycle de vie. La fin du cycle de vie implique de nouvelles mises en danger de la sécurité.
Mises à jour de sécurité *(update management)*	Clairement définies, effectuées à l'échelle de l'entreprise, automatisées grâce à des accès à distance.	Longs délais et périodes de planification jusqu'à l'aboutissement de l'installation d'un correctif *(patch)* ; toujours propres au fabricant ; peuvent provoquer un arrêt (temporaire) du SCI ; nécessité de définir le risque acceptable à cet égard.
Méthodes de test et d'audit *(testing and audit methods)*	Recours à des méthodes modernes (évent. automatisées). Les systèmes sont généralement suffisamment résilients et fiables pour supporter des évaluations au cours de l'exploitation.	Les méthodes d'évaluation automatisées ne sont pas toujours adaptées, notamment en raison du caractère très personnalisé des solutions développées. Il existe une forte probabilité d'erreur durant les évaluations. Il est donc généralement plus difficile de les réaliser au cours de l'exploitation.

Tableau 5 : Différences entre les TIC et les TO (SCI ou SCADA)

Aspect touchant à la sécurité	TIC (bureautique, p. ex.)	TO (SCI ou SCADA) (gestion de la production, p. ex.)
Gestion des modifications *(change management)*	Rythme régulier et planifié ; adaptée aux exigences de l'entreprise en matière de durée minimale et maximale d'utilisation.	Processus complexe ayant un impact possible sur l'activité de l'entreprise. Une planification stratégique individuelle est indispensable.
Classification des actifs *(asset classification)*	Opération courante effectuée chaque année ; dépenses et investissements planifiés en fonction des résultats.	Effectuée uniquement lorsqu'elle est nécessaire ou imposée. Sans inventaire, les contre-mesures ne sont généralement pas adaptées à l'importance de l'élément du système.
Réponse aux incidents et analyse technique des incidents *(incident response and forensics)*	Faciles à développer et à mettre en œuvre. Les prescriptions réglementaires applicables (protection des données) doivent être respectées.	Principalement axées sur le redémarrage du système. Processus d'investigation peu développés.
Sécurité physique *(physical security)*	Varie de faible pour les outils de bureautique à forte pour les centres de calcul sécurisés.	Généralement excellente.
Développement sécurisé de logiciels *(secure software development)*	Partie intégrante du processus de développement.	À l'origine, la plupart des SCI étaient des systèmes physiquement isolés. Les développeurs ne se souciaient guère de la sécurité. Les fournisseurs de SCI ont fait des progrès en la matière, mais moins que dans le domaine des TIC. Il n'existe guère de solutions pour sécuriser a posteriori les éléments centraux des SCI.
Antivirus	Largement répandus ; faciles à déployer et à actualiser. Les utilisateurs peuvent personnaliser leur antivirus. La protection antivirus peut être configurée au niveau des appareils ou à l'échelle de l'entreprise.	Les besoins de stockage et le ralentissement des échanges de données inhérents aux analyses antivirus peuvent avoir des répercussions négatives sur un SCI. Pour protéger les anciens éléments du SCI, les organisations doivent le plus souvent se tourner vers des produits du marché secondaire. En outre, la plupart des solutions antivirus prévoient que des dossiers de l'environnement SCI soient exclus de l'analyse afin d'éviter la mise en quarantaine de fichiers stratégiques.

Tableau 5 : Différences entre les TIC et les TO (SCI ou SCADA)

Les éléments suivants doivent être pris en compte lors de la mise en place d'un plan de défense en profondeur pour un SCI ou un système SCADA :

- coûts inhérents à la sécurisation des anciens systèmes en fonction des besoins actuels ;
- tendance croissante à connecter les SCI au réseau interne de l'entreprise ;
- possibilité de fournir un accès à distance aux utilisateurs des environnements TIC et SCI ;
- nécessité de faire confiance à sa propre chaîne d'approvisionnement ;
- solutions modernes de surveillance et de protection des protocoles propres aux SCI ;
- capacité de tenir à jour les connaissances techniques au sujet des nouvelles menaces planant sur les SCI.

L'approche de la défense en profondeur complique les attaques directes visant les systèmes informatiques et augmente la probabilité de détecter rapidement des comportements suspects ou inhabituels dans le système. Elle permet également de créer des zones distinctes pour mettre en œuvre des technologies permettant de détecter les intrusions dans le système *(intrusion detection technologies)*.

Les principaux éléments d'une stratégie de défense en profondeur sont présentés au tableau 6.

Éléments d'une stratégie de défense en profondeur	
Programme de gestion des risques	• identification des risques pour la sécurité • profil de risque • gestion des actifs informatiques (inventaire détaillé)
Architecture de cybersécurité	• normes, recommandations • directives • marche à suivre
Sécurité physique	• protection des terminaux • restriction de l'accès au centre de contrôle • vidéosurveillance, restriction des accès et barrières
Architecture de réseau	• zones de sécurité standard • « zones démilitarisées » (DMZ) • réseaux locaux (LAN) virtuels
Sécurité du périmètre du réseau	• pare-feu • accès à distance et authentification • serveurs et hôtes intermédiaires
Sécurité des hôtes	• gestion des correctifs (patches) et des failles • terminaux • appareils virtuels
Surveillance de la sécurité	• systèmes de détection d'intrusion *(intrusion detection systems, IDS)* • journalisation des audits de sécurité • surveillance *(monitoring)* des événements et des incidents de sécurité
Gestion des fournisseurs	• gestion et surveillance de la chaîne d'approvisionnement • services gérés *(managed services)* et externalisation *(outsourcing)* • utilisation de services cloud
Facteur humain	• directives • marche à suivre • formation et sensibilisation

Tableau 6 : Éléments d'une stratégie de défense en profondeur

3.2 Organisation, stratégie et gouvernance

La définition, l'application et le suivi d'une stratégie globale en matière de sécurité de l'information permettent aux instances dirigeantes de l'entreprise (ci-après : direction) d'adopter des directives claires et les aident aussi bien dans l'application des prescriptions que dans la gestion des risques.

3.2.1 Gouvernance de la sécurité informatique

Une mise en œuvre efficace et durable de la stratégie de défense en profondeur passe par la gouvernance de la sécurité. Il s'agit dans un premier temps de créer les conditions permettant de reconnaître, d'évaluer et de traiter les menaces planant sur le contrôle-commande des processus. La gouvernance fournit une structure générale qui contribue, sur les plans stratégique, fonctionnel et opérationnel, à la réalisation des objectifs de l'entreprise en matière de sécurité informatique. Le modèle de gouvernance définit :

- ce qui est fait (« quoi ? ») ;
- la manière de procéder (« comment ? ») ;
- les personnes responsables (« par qui ? ») ;
- la méthode de mesure.

La gouvernance fixe les règles, processus, systèmes de mesure et structures organisationnelles nécessaires à une planification et un pilotage efficaces, dans le but de satisfaire aux exigences et objectifs opérationnels de l'entreprise. Ces éléments doivent être consignés dans un document stratégique, qui, une fois validé par la direction, pourra circuler au sein de l'entreprise. En outre, la responsabilité de la sécurité de l'information doit être confiée à un membre de la direction, qui veillera à ce que l'élaboration et la mise en œuvre de la stratégie de défense en profondeur bénéficient du soutien requis. L'organe chargé de la sécurité doit régulièrement informer la direction du degré de maturité atteint, des incidents survenus et des indicateurs de performance clés *(key performance indicators,* KPI) liés à la sécurité.

Ce faisant, il est capital de bénéficier du soutien inconditionnel de la direction et de discuter des charges, des processus et des ressources nécessaires à une mise en œuvre efficace.

3.2.2 Organisation et responsabilités

L'existence, au sein de l'entreprise, d'un organe chargé de la sécurité qui se caractérise par des tâches, des responsabilités et des compétences clairement définies est cruciale pour la gouvernance de la sécurité. Il incombe à cet organe de définir, de mettre en œuvre et de développer la stratégie de défense en profondeur. La gestion active des risques joue à cet égard un rôle central dans la détection des menaces potentielles visant la sécurité informatique et la mise en place de mesures pour y parer. L'organe chargé de la sécurité doit se voir conférer les compétences requises par la direction et disposer des ressources nécessaires à l'accomplissement efficace de l'ensemble de ses tâches. Il doit être bien intégré et accepté au sein de l'entreprise. Les rôles et fonctions de ses membres doivent être décrits et documentés, et assortis de compétences précises. Il convient en outre de définir et consigner les points de recoupement avec les autres organes internes (importants du point de vue de la sécurité) et de clarifier les compétences en cas de chevauchement.

Si ses compétences lui ont été conférées par la direction, l'organe chargé de la sécurité peut exécuter sans restriction ses tâches essentielles en collaboration étroite avec les autres organes de l'entreprise. Ses tâches prioritaires sont décrites ci-après.

L'organe chargé de la sécurité doit veiller à ce que :

- la conduite technique de la sécurité de l'information liée aux TIC et aux SCI soit assurée, et les priorités au sein des activités adaptées à la situation ;
- tous les documents, instructions et directives requis en matière de la sécurité soient rédigés, actualisés si nécessaire et appliqués de manière conséquente ;
- les nouvelles questions touchant à la sécurité soient identifiées, analysées et traitées si nécessaire ;
- le savoir-faire et les ressources requis soient disponibles tout au long de la chaîne de gestion de la sécurité ;
- des vérifications, audits et tests d'intrusion soient effectués périodiquement ;
- les rapports rédigés à l'intention de la direction soient corrects quant au fond, et livrés dans les temps, de manière systématique et à l'échelon approprié ;
- le processus de sécurité soit imbriqué dans le processus de gestion des risques de l'entreprise par le biais d'une intégration méthodique, conformément aux exigences du processus de gestion des risques.

3.2.3 Instructions et directives

Tout comme dans les autres domaines, l'entreprise doit se fixer une orientation stratégique en matière de sécurité de l'information. Quels objectifs souhaite-t-elle atteindre d'ici 3 à 5 ans ? Quel est son goût du risque ? Quels sont les ressources et les moyens financiers qu'elle prévoit d'investir ?

Il convient d'aborder ces questions stratégiques et d'y répondre dans le cadre d'une politique en matière de sécurité à l'échelle de l'entreprise. La politique en matière de sécurité doit être définie par la direction et approuvée par le conseil d'administration. En règle générale, son élaboration incombe à l'organe chargé de la sécurité, sur mandat de la direction. Les aspects stratégiques suivants doivent être définis dans le cadre d'une telle politique et servir de référence à toutes les activités et les prescriptions relevant de la sécurité de l'information :

- but et champ d'application de la politique en matière de sécurité ;
- objectifs en matière de sécurité ;
- principes en matière de sécurité ;
- goût du risque ;
- collaboration avec les acteurs de la branche et les autorités ;
- application des normes de sécurité ;
- prise en considération de l'aspect économique ;
- culture de la sécurité ;
- exceptions aux prescriptions en matière de sécurité ;
- sécurité dans le cadre de projets ;
- rôles et fonctions de l'organe chargé de la sécurité.

Hormis la politique en matière de sécurité, qui réglemente la sécurité de l'information, d'autres documents ayant valeur d'instructions peuvent être nécessaires selon la taille et la structure de l'entreprise.

Il est en outre important de créer un cadre réglementaire général qui fixe la manière dont les instructions et directives sont appliquées au sein de l'entreprise (personne responsable de la procédure, validation, communication et formation, mise à jour régulière) et détermine quelles instructions ou directives s'appliquent également aux partenaires et prestataires externes ou doivent être spécialement définies.

3.3 Risque et gestion de la continuité d'activité

3.3.1 Établissement, évaluation et gestion de l'inventaire des actifs

Afin d'évaluer les risques, il faut commencer par déterminer quels sont les actifs à protéger et en dresser l'inventaire. C'est la seule manière de garantir que l'analyse des menaces puisse être complète et correcte.

Pour cela, il faut tenir un registre centralisé des actifs qui permette de représenter la totalité du cycle de vie d'un actif. En plus des informations nécessaires à une exploitation intègre des actifs, le registre doit contenir une évaluation des actifs du point de vue des exigences en matière de sécurité, à savoir : confidentialité, disponibilité, intégrité. Chaque actif doit avoir un propriétaire responsable de la mise en œuvre du processus du cycle de vie de l'actif.

3.3.2 Programme de gestion des risques

La mise en place d'une stratégie de défense en profondeur exige de comprendre les risques opérationnels qu'impliquent pour une entreprise les menaces liées aux TIC. Ces risques doivent être gérés en fonction du goût du risque de l'entreprise. Les responsables de l'exploitation et de la maintenance des systèmes informatiques doivent savoir identifier les risques, les évaluer et y répondre. Cela nécessite d'avoir une idée claire des scénarios de menace, des processus opérationnels et techniques, et des technologies impliquées. C'est à ces conditions seulement qu'une stratégie de défense en profondeur peut être intégrée aux affaires courantes. Il appartient à la direction de veiller à ce que la sécurité soit garantie dans toutes les activités informatisées au sein de l'entreprise.

Les considérations ci-dessus s'appliquent d'une manière générale. Certaines applications informatiques revêtent cependant une importance particulière en raison de leur criticité. C'est notamment le cas des systèmes de contrôle industriels (SCI). Concevoir une architecture de sécurité des SCI efficace demande de mettre en parallèle les risques de l'entreprise et les exigences opérationnelles posées au SCI. Cela peut aussi concerner le monde physique (périmètre de sécurité autour des centres de calcul, p. ex.). Les décideurs à tous les échelons hiérarchiques doivent connaître l'importance des cyberrisques et s'impliquer dans le processus de gestion des risques. Des analyses régulières des risques, portant sur une partie des systèmes, applications et processus ainsi que les réseaux correspondants, sont indispensables. Elles doivent suivre des prescriptions strictes et se dérouler de manière structurée et systématique.

3.3.3 Cadre de gestion des risques

Les analyses des risques liés aux TIC doivent s'inscrire dans un cadre de gestion des risques, être menées sur une base régulière (en général une fois par année) et porter sur des objets clairement définis. C'est notamment le cas pour les installations, processus et applications critiques (même en phase de développement) et leur dépendance à l'égard de systèmes, réseaux et services.

L'objectif du cadre de gestion des risques est de désigner des personnes ou rôles responsables des risques identifiés, qui surveillent les risques, les évaluent et mettent en œuvre des mesures adéquates afin de les maintenir dans les limites définies au préalable (selon le goût du risque).

3.3.4 Analyse des risques et des menaces

En gestion des risques, l'analyse des risques d'une entreprise porte sur les risques déterminés au moment de l'identification des risques. Elle donne des indications qualitatives et quantitatives sur les pannes et les menaces qui se présentent. L'accent est mis sur les coûts et conséquences pour l'entreprise de transport. L'analyse des menaces fait partie de l'analyse des risques. Alors que l'analyse des risques a pour objet les risques inhérents à un système informatique ou à un système de technologie opérationnelle, l'analyse des menaces se concentre plus spécifiquement sur les différentes menaces. En vue de la gestion des risques, les différents risques sont déduits des menaces identifiées et de l'estimation de la probabilité de leur survenance.

Pour les transports publics, des cyberincidents pourraient donner lieu aux scénarios de menace suivants :

- extorsion d'argent ;
- utilisation de la capacité de calcul (cryptominage, réseau de zombies, porte dérobée en vue d'autres attaques) ;
- utilisation (fortuite ou intentionnelle) de l'entreprise en tant que cible d'essai, pour tester une attaque ;
- manipulation ou vol de données relatives à des clients ou à des processus ;
- sabotage (perturbation ou interruption de liaisons de transport) ;
- espionnage (connaissances opérationnelles, données personnelles, données de marché) ;
- vol par émission ou détournement d'ordres de paiement.

Le champ de l'analyse des risques doit être clairement défini. Les processus opérationnels concernés, les systèmes informatiques ou de technologie opérationnelle et les éventuels facteurs externes doivent être décrits aussi précisément que possible.

3.3.5 Gestion de la continuité d'activité

La gestion de la continuité d'activité (GCA) ou gestion des situations d'urgence est un processus de gestion visant à identifier rapidement les risques susceptibles de mettre en péril la survie d'une entreprise ou d'un organisme et à prendre des mesures pour les éviter. Pour assurer le fonctionnement et donc la survie d'une entreprise ou d'un organisme, il faut prendre des mesures de prévention permettant, d'une part, d'augmenter la robustesse et la résilience des processus opérationnels et, d'autre part, de réagir rapidement et de manière ciblée en cas d'urgence ou de crise.

La GCA comprend la planification et l'organisation de la marche à suivre afin d'augmenter durablement la résilience des processus opérationnels critiques (éventuellement à caractère urgent) d'une entreprise ou d'un organisme, de pouvoir réagir de manière adéquate aux événements préjudiciables et de reprendre les activités le plus vite possible.

L'objectif est de garantir que, même dans des situations critiques, les processus opérationnels importants ne soient pas interrompus, ou seulement temporairement, et que la survie économique de l'entreprise ou de l'organisme soit assurée même en cas d'événement préjudiciable de grande ampleur.

Il est donc d'une importance cruciale d'avoir une vue d'ensemble. Tous les aspects nécessaires à la poursuite des processus opérationnels critiques en cas d'événement préjudiciable doivent être pris en compte, pas seulement la ressource que représente l'informatique. La gestion de la continuité des services informatiques fait donc partie de la GCA en général (cf. normes ISO 22301 et BSI 100-4, p. ex.).

Le plan de continuité des activités *(Business Continuity)* comprend les stratégies, les plans, les mesures et les processus qui sont à disposition d'une organisation afin qu'elle puisse minimiser les dommages causés par l'interruption de ses activités. Il permet d'assurer le fonctionnement d'une organisation dans des conditions de crise et permet un redémarrage rapide et sans problème des processus après une panne. L'objectif principal est d'assurer la pérennité de l'organisation et de son activité économique.

Une nette différenciation entre les méthodes relevant de la gestion des risques, de la gestion de crise et de la GCA est indispensable à une organisation de crise efficace. Elle permet de définir clairement les responsabilités et échelonner correctement les plans de mesures dans le temps (plans d'urgence, de continuité et de rétablissement).

La norme ISO 22301 définit la GCA comme un processus qui identifie les menaces potentielles pour un organisme et qui fournit un cadre pour construire la résilience de l'organisme avec une capacité de réponse efficace préservant les intérêts des (principales) parties intéressées, sa réputation, sa marque et ses activités productrices de valeur.

C'est le plan B de l'entreprise pour maintenir sa capacité opérationnelle (continuité d'activité) quand un événement ayant un impact sur l'activité (accident, sabotage, etc.) survient et que l'entreprise n'est plus en mesure de poursuivre la livraison de ses produits ou la fourniture de ses services.

3.3.6 Bilan d'impact sur l'activité

Dans le cadre d'un bilan d'impact sur l'activité (BIA), il faut identifier à la fois la conséquence la plus réaliste et la conséquence la plus néfaste (sur l'activité) que pourrait avoir la compromission d'un composant des TIC (y c. les personnes, données, processus, services et réseaux) à différents niveaux (financier, opérationnel, juridique, réputationnel, sanitaire, etc.).

Il s'agit, en fin de compte, de déterminer quelles conséquences sur son activité l'entreprise est prête à supporter au cas où les ressources informatiques nécessaires ne sont pas disponibles comme prévu. Sur cette base, il faut définir les exigences et les niveaux de protection requis pour garantir la disponibilité, l'intégrité et la confidentialité des ressources informatiques identifiées, dans les limites du risque acceptable.

Le BIA est un processus d'analyse des activités et de l'impact que les perturbations de l'exploitation peuvent avoir sur elles.

Un BIA doit avant tout permettre de comprendre quels processus opérationnels sont nécessaires pour maintenir l'activité et donc importants pour l'entreprise ou l'organisme, et quelles pourraient être les conséquences d'une panne. Ces processus opérationnels « critiques » font l'objet de mesures de sauvegarde particulières dans le cadre de la gestion des situations d'urgence, et des dispositions sont prises pour les situations de crise.

Dans le domaine de la GCA, « critique » signifie « à caractère urgent ». Un processus qualifié de tel doit être rétabli très rapidement, faute de quoi l'entreprise ou l'organisme risque de subir un dommage important, tel que des pertes financières, la violation de dispositions légales ou contractuelles, ou une atteinte à l'image. Le fait qu'un processus opérationnel ne soit pas désigné comme critique dans le BIA ne signifie pas qu'il n'est pas important pour l'entreprise ou l'organisme, mais simplement qu'il est moins urgent de le rétablir (norme BSI 100-4, ch. 5.1).

Il y a plusieurs méthodes et approches pour réaliser un BIA. L'une d'elles est de dresser l'état des lieux des données de base et des processus opérationnels :

- différencier les unités organisationnelles et les processus opérationnels à inclure (se limiter aux processus opérationnels utiles à la GCA) ;
- effectuer une analyse des dommages (définir une grille pour les catégories de dommages et les scénarios de dommage, déterminer les périodes d'évaluation et la stratégie de traitement des disponibilités particulières, évaluer pour chaque processus et chaque période d'évaluation les dommages encourus en cas de panne) ;
- définir les paramètres de reprise (fixer, pour chaque processus opérationnel, la durée de panne maximale tolérée, le délai de reprise et le niveau de reprise) ;
- prendre en compte les rapports de dépendance (examiner les paramètres de reprise à l'aune des rapports de dépendance des processus et des objectifs stratégiques de l'entreprise, apporter les corrections nécessaires) ;
- établir un ordre de priorité et déterminer le degré de criticité des processus opérationnels (fixer l'ordre de priorité des processus opérationnels en vue de la reprise, définir des catégories de criticité et leurs limites) ;
- répertorier les ressources nécessaires à l'exploitation en situation normale et en cas d'urgence (déterminer les ressources et la capacité nécessaires en situation normale et en cas d'urgence) ;
- déterminer la criticité et le délai de reprise des ressources (déterminer le délai de reprise, le délai de rétablissement et la criticité des ressources nécessaires aux processus critiques).

La norme BSI 100-4 traite en détail de la GCA, sous forme de guide.

3.3.7 Mesures de gestion de la continuité d'activité

Les mesures relatives aux risques décrits dans le BIA doivent être mises au point, vérifiées et validées par la direction. Leur validation doit avoir lieu en même temps que celle des plans indiquant la marche à suivre détaillée.

Il faut veiller à ce que le risque résiduel soit identifié pour chaque actif *(asset)* dans son contexte et géré (atténué, évité, reporté ou accepté, p. ex.) conformément au goût du risque de l'entreprise.

Pour chaque actif, il faut déterminer le risque maximal acceptable, afin de pouvoir calculer les risques (cumulés) liés aux TIC.

3.4 Architectures

3.4.1 Architecture de cybersécurité

L'architecture de cybersécurité comprend les mesures spécifiques et leur position stratégique au sein du réseau, en vue de créer une couche de sécurité dans la perspective de la défense en profondeur. Elle doit pouvoir fournir des informations sur le flux de données et les liens entre les différents systèmes. Elle doit aussi être adaptée à l'inventaire physique des installations et aux actifs informatiques, afin de permettre une compréhension globale des flux d'information au sein de l'organisme.

L'architecture de cybersécurité doit être conforme au *NIST Cybersecurity Framework Core.* Elle couvre la protection de la confidentialité, de l'intégrité et de la disponibilité des données, des services et des systèmes. Pour ce faire, il faut élaborer un plan de mise en œuvre qui respecte la culture de l'entreprise et les objectifs stratégiques, tienne dûment compte des besoins en matière de sécurité et précise les ressources nécessaires à cet effet. En règle générale, l'architecture de cybersécurité s'accompagne d'un plan intégré des tâches, qui indique les résultats escomptés (indicateurs et éléments déclencheurs d'un nouvel examen et d'une réorientation), fixe le calendrier des projets, donne une estimation des ressources nécessaires et cerne les principaux rapports de dépendance des projets.

3.4.2 Architecture du système

Les systèmes de contrôle industriels (SCI) doivent être surveillés et contrôlés conformément à leur besoin de protection. Ils doivent bénéficier d'une protection technique et physique particulière afin, notamment, de sécuriser les processus relevant de l'approvisionnement.

Une architecture de réseau sûre et robuste est l'un des principaux piliers d'une protection efficace contre les attaques. Chaque interface, chaque transfert, chaque connexion représente un danger potentiel. Il est donc absolument indispensable que toutes les opérations qui ont lieu au sein des différents réseaux et installations soient connues et traitées en conséquence. Cela passe par un groupement correct et la segmentation de l'architecture de réseau. Il est important que le réseau soit subdivisé en zones sécurisées.

Il est également important que l'architecture ne se limite pas aux infrastructures fixes (installations fixes) ou mobiles (systèmes de véhicules) ni ne soit considérée isolément. Il faut veiller à toujours prendre en compte l'ensemble de l'architecture, en intégrant tous les éléments. En effet, dans une architecture globale, c'est malheureusement le maillon le plus faible qui montre le degré de sécurité atteint.

Les exploitants d'infrastructures critiques doivent donc impérativement mener des analyses des risques portant sur l'ensemble de l'architecture du système afin d'en déduire le niveau de sécurité et la maturité à atteindre.

La figure suivante illustre comment représenter schématiquement l'exploitation d'un chemin de fer. Elle montre quels composants (TIC ou SCI) et canaux de communication sont nécessaires à une exploitation sécurisée[4].

[4] L'architecture de réseau SCI représentée ici est un exemple, qui doit être adapté aux besoins de l'entreprise.

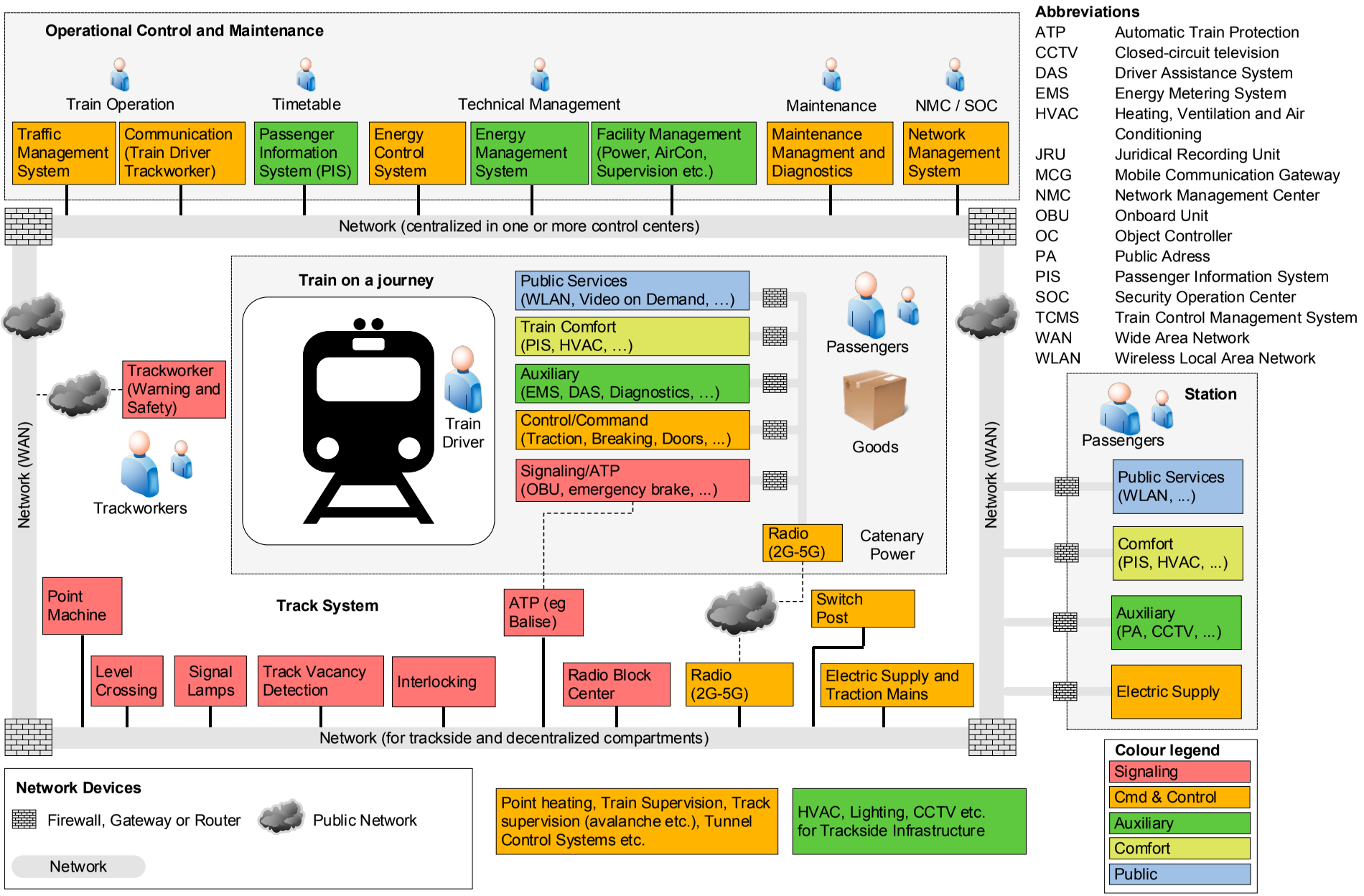


Figure 5 : Exemple d'architecture de système (tiré de : CENELEC prTS 50701 – D7E6)

3.5 Mesures de sécurité techniques

3.5.1 Systèmes de contrôle industriels

En raison de l'architecture complexe des SCI ou systèmes de commande de surveillance et d'acquisition de données (SCADA)[5], certaines failles de sécurité peuvent, dans les cas les plus graves, rester très longtemps insoupçonnées et leur exploitation éventuelle représente une menace. L'application du concept de défense en profondeur décrit ci-dessus offre une protection appropriée contre ces menaces.

Quelques méthodes d'attaque caractéristiques des SCI sont présentées ci-dessous :

- cyberattaques ciblant un SCI connecté à l'internet, dans le but d'établir un accès à distance longue durée ;
- accès à distance au SCI au moyen de données d'accès volées ;
- attaques ciblant un système SCADA à travers l'exploitation des failles de l'interface web ;
- infection d'un SCI par des logiciels malveillants provenant de supports compromis (clés USB, smartphones, etc.) ;
- attaques ciblant la bureautique (courriels d'hameçonnage *[phishing]*, infections par téléchargement furtif *[drive-by download]*, etc.) dans le but de pénétrer dans un SCI par n'importe quelle interface.

3.5.2 Sécurité des hôtes

Une couche de sécurité supplémentaire doit être mise en place au niveau des hôtes ou des postes de travail. La plupart des appareils sont protégés par des pare-feu contre les intrusions en provenance de l'extérieur, mais un bon modèle de sécurité nécessite plusieurs niveaux de défense. Pour sécuriser complètement le réseau, il faut sécuriser tous les hôtes. Cette couche de sécurité au niveau des hôtes doit permettre aux utilisateurs d'utiliser différents systèmes d'exploitation et applications tout en assurant une protection adéquate des appareils.

Il convient de créer un document qui énumère les règles de mot de passe et de renommer les comptes classiques (« administrateur », p. ex.). Des lignes directrices restrictives sont susceptibles d'être contournées : c'est notamment le cas lorsque des utilisateurs stockent leurs mots de passe de manière non sécurisée (sur un post-it, p. ex.) ou utilisent toujours des mots de passe similaires. La complexité des mots de passe doit être adaptée au niveau d'accès des utilisateurs. Des cycles de changement de mot de passe peuvent éventuellement être définis.

[5] Dans le présent manuel, les termes technologie opérationnelle (TO), système de contrôle industriel (SCI) et commande de surveillance et d'acquisition de données (SCADA) ont valeur de synonymes.

Les recommandations générales qui suivent doivent être mises en place par les organismes pour chaque hôte SCI et chaque appareil ayant accès au réseau interne (indépendamment du système d'exploitation) :

- installer et configurer un pare-feu spécifique aux hôtes ;
- instaurer dans la mesure du possible des économiseurs d'écran requérant la saisie du mot de passe à intervalles rapprochés ;
- appliquer les correctifs *(patches)* aux systèmes d'exploitation et veiller à ce que les micro-logiciels *(firmwares)* soient toujours à jour ;
- activer la configuration de journaux sur tous les appareils ;
- désactiver les services et les comptes qui ne sont pas utilisés ;
- remplacer les services non sécurisés (Telnet, Remote Shell, FTP, etc.) par leurs équivalents sécurisés (STelnet, SSH, SFTP, etc.) ;
- veiller à ce que les utilisateurs ne puissent pas désactiver des services ;
- effectuer des copies de sauvegarde *(backups)* des systèmes et les vérifier, surtout quand ces derniers ne sont pas gérés de manière centralisée ;
- activer les modules de sécurité fournis avec le système d'exploitation (scanners de sécurité, p. ex.) ou les remplacer par un logiciel adéquat ;
- appliquer les mêmes directives aux ordinateurs portables et autres appareils mobiles qui ne sont pas connectés en continu au réseau de l'entreprise ; verrouiller le disque dur des appareils mobiles.

3.5.3 Sécurité du périmètre du réseau

Après avoir développé et implanté une architecture de réseau robuste, l'entreprise doit mettre en place l'architecture de sécurité pour le réseau et les systèmes. L'architecture de sécurité comprend les contrôles spécifiques et le positionnement stratégique de détecteurs et de tests au sein du réseau ou des systèmes afin d'établir les différentes couches de sécurité de la défense en profondeur. Des diagrammes de réseau, des matrices de connexion et des diagrammes de flux d'information qui relient tous les systèmes et leurs points de contact avec les éléments de l'inventaire physique sont absolument nécessaires pour avoir une bonne compréhension des flux d'information et des connexions nécessaires au sein du réseau. Délimiter des aires, des zones et des secteurs et superposer les couches de sécurité pour chaque système ou sous-système inventorié permet de déterminer quels éléments de pilotage et de surveillance ont été mis en place pour protéger le système sans en restreindre la performance.

Les responsables système ne doivent pas négliger les contrôles de sécurité dans le réseau, le système, les applications et les couches physiques afin de garantir la sécurité de l'information. En font partie : la gestion des directives et de la sécurité, la sécurité des applications, des données, des plateformes, du réseau et du périmètre ainsi que la sécurité physique et celle des utilisateurs. L'architecture de sécurité réunit tous les mécanismes et contrôles de défense qui se superposent à l'architecture du réseau. Elle définit les mesures de défense en profondeur qui s'appliquent à l'ensemble de l'entreprise. Le référentiel NIST 800-82 *(« Guide to Industrial Control Systems [ICS] Security »)* propose un contrôle de sécurité SCI pour l'ensemble de l'entreprise, qui se superpose aux couches de sécurité existantes, sur la base du référentiel NIST 800-53 *(« Security and Privacy Controls for Federal Information Systems and Organizations »).*

En raison du coût d'une installation SCI et pour maintenir l'homogénéité de l'infrastructure réseau, il est souvent nécessaire de relier le réseau SCI et celui de l'entreprise. Cette connexion, qui représente un risque notable en matière de sécurité, devrait être protégée par des moyens techniques. Lorsque les réseaux doivent être reliés, il est vivement recommandé de n'autoriser que des connexions minimales (si possible uniques) et de recourir à un pare-feu et à une zone démilitarisée (*demilitarised zone,* DMZ), autrement dit un segment de réseau isolé. Les serveurs SCI qui contiennent des données du réseau de l'entreprise doivent être placés dans une DMZ. Les connexions externes doivent être connues et se limiter à un accès minimal à travers un pare-feu. L'échange de données peut en outre être surveillé et vérifié par des systèmes capables de détecter les anomalies.

3.5.4 Configuration des appareils mobiles

Afin de protéger les données contre les accès non autorisés, la perte ou le vol, les appareils mobiles (ordinateurs portables, tablettes, smartphones, etc.) doivent avoir une configuration par défaut conforme aux exigences en matière de sécurité.

L'objectif de la configuration par défaut est de garantir la sécurité des données enregistrées ou transmises sur les appareils mobiles, y compris en cas de perte ou de vol.

3.5.5 Sécurité physique

Les mesures de sécurité physique réduisent le risque de pertes ou dommages accidentels ou intentionnels touchant des actifs informatiques de l'organisme ou de son environnement. Parmi les actifs à protéger figurent notamment les actifs physiques (outils et installations, p. ex.), le milieu, l'environnement élargi et la propriété intellectuelle, y compris les données propriétaires (paramètres des processus, informations relatives à la clientèle, etc.). Les contrôles physiques de sécurité doivent souvent répondre à des exigences spécifiques, notamment concernant le milieu, la sécurité, la réglementation ou le droit. L'entreprise ou l'organisme doit adapter les contrôles physiques de sécurité (tout comme les contrôles techniques) aux besoins de protection. Afin de garantir une protection complète, la protection physique inclut la protection de composants informatiques *(= security)* et celle de données de l'environnement qui sont liées aux TIC. La sécurité de nombreuses infrastructures informatiques est étroitement liée à celle des installations *(= safety)*. L'objectif est d'éviter que les collaborateurs soient confrontés à des situations dangereuses, sans pour autant les empêcher de faire leur travail ou de suivre les procédures d'urgence. Les contrôles physiques de sécurité sont des mesures actives et passives qui restreignent l'accès physique à toutes les parties de l'infrastructure informatique. Ces mesures de protection doivent notamment empêcher les cas de figure suivants :

- accès physique non autorisé à des lieux sensibles ;
- altération physique, manipulation, vol ou autre forme de soustraction ou de destruction de systèmes, d'infrastructures, d'interfaces de communication ou de locaux ;
- observation non autorisée d'installations sensibles (directement, par photographie ou autre forme d'enregistrement) ;
- déploiement ou installation non autorisés de nouveaux systèmes, infrastructures, interfaces de communication ou matériel informatique ;
- introduction non autorisée d'appareils (clés USB, points d'accès sans fil, appareils mobiles ou Bluetooth) servant à effectuer des manipulations sur du matériel informatique, à intercepter des communications ou ayant d'autres conséquences néfastes.

Pour répondre aux exigences en matière de sécurité de l'information, les actifs physiques, y compris les systèmes et les équipements de réseau, le matériel de bureau (imprimantes réseau et appareils multifonctions, p. ex.) et les équipements spéciaux (SCI, p. ex.) doivent être protégés pendant tout leur cycle de vie, de leur acquisition (achat ou leasing, p. ex.) à leur élimination, en passant par la maintenance.

Les appareils mobiles (ordinateurs portables, tablettes, smartphones, etc.) et leurs données doivent également être protégés contre les accès non autorisés, la perte et le vol. Pour cela, il faut configurer les paramètres de sécurité, restreindre l'accès, installer un logiciel de sécurité et centraliser la gestion des appareils.

3.6 Gestion des fournisseurs, modèles d'exploitation et surveillance

3.6.1 Gestion des fournisseurs

Gérer les fournisseurs consiste à identifier et à maîtriser les risques liés aux informations fournies à des prestataires externes (fournisseurs de matériel et de logiciels, prestataires d'externalisation, prestataires de services cloud, etc.). La mise en œuvre d'un certain nombre d'exigences relatives à la sécurité de l'information et énoncées dans des contrats formels doit permettre de réduire les risques au minimum.

3.6.2 Externalisation, services gérés

De nombreux organismes recourent aux services gérés *(managed services)* et/ou à l'externalisation *(outsourcing)* pour assurer des fonctions exigeant des technologies ou aptitudes très pointues. Il n'est pas rare que des organismes externalisent un grand nombre de fonctions touchant à la sécurité informatique (réponse aux incidents *[incident response],* analyse technique des incidents *[forensics]*, évaluations de la cybervulnérabilité *[cyber vulnerability assessments]*, gestion des risques, gestion de la chaîne d'approvisionnement, etc.) qu'elles utilisent rarement ou qui ne requièrent leur savoir-faire que ponctuellement. Pour ces organismes, l'externalisation a pour avantage de nécessiter moins d'investissements et peut s'avérer moins onéreuse. L'engagement d'un expert forensic à temps plein, par exemple, coûte très cher, en raison notamment du niveau élevé de savoir-faire requis, mais est incontournable pour une entreprise s'agissant de l'analyse des enquêtes sur les incidents.

Un accord de niveau de service *(service level agreement, SLA)* permet à une entreprise qui externalise de convenir des services à fournir par le prestataire. Si ce dernier ne satisfait pas aux exigences du SLA, le bénéficiaire de prestations se réserve le droit de résilier le contrat. Dans le cas d'une entité externe proposant des services de sécurité, il est important que les deux parties s'entendent sur les rôles, les responsabilités, la gestion et le reporting des incidents ainsi que sur la sécurité des interfaces (directives et procédures d'accès à distance, p. ex.) qu'un utilisateur peut exiger. En plus du SLA, les entreprises devraient établir un mémorandum d'entente (*memorandum of understanding,* MoU) ou d'accord (*memorandum of agreement,* MoA) et un accord de sécurité d'interconnexion (*interconnection security agreement,* ISA) afin de décrire les exigences de gestion spécifiques et les exigences techniques relatives aux prestations.

Lorsque les évaluations techniques sont réalisées ou contrôlées par une entité externe, l'ensemble des parties devraient fixer et avaliser les règles de collaboration. Les évaluations de la cybervulnérabilité, par exemple, nécessitent habituellement d'effectuer un certain nombre de scans actifs ou passifs ou de tests des systèmes cibles, de sorte que les évaluateurs doivent soit disposer d'un accès personnel à ces systèmes, soit suivre l'accès de tiers aux actifs numériques *(cyber assets)* critiques au sein de l'environnement du système de contrôle. L'équipe d'évaluation collabore avec son homologue en charge de l'organisation afin de garantir que les activités de test n'interfèrent pas avec l'exploitation client, et de convenir de mesures de surveillance *(monitoring)* des protocoles pour le cas où les activités réalisées seraient source de problèmes pour l'entreprise. Les règles d'engagement *(rules of engagement, ROE)* établissent quels sont travaux à effectuer sur tel ou tel système et quelles sont les personnes habilitées à les mener. Elles englobent les décisions déterminant si les tests sont effectués sur le système de commande primaire (système de production) ou un substitut fiable, tel qu'un système de commande de sauvegarde *(backup)*, un système de contrôle secondaire, un réseau de test ou un système autonome. Il y a lieu d'éviter les scans actifs des systèmes de production, car ils peuvent perturber l'exploitation ou créer une situation de déni de service *(denial of service)*. Les activités passives telles que le reniflage de réseau *(network sniffing)* peuvent être appropriées. En cas de recours à un substitut, il conviendrait de comparer celui-ci au système actif pour s'assurer qu'ils sont identiques en termes de fonctionnement. L'équipe d'évaluation et l'organisme doivent désigner d'un commun accord la « personne aux commandes » durant la phase de test, en particulier si l'objectif porte sur des systèmes de commande (systèmes de production) actifs. Le personnel local devrait procéder à l'ensemble des tests portant sur le pilotage actif de l'équipe d'évaluation.

3.6.3 Utilisation de services d'informatique cloud

Le recours à des prestations informatiques cloud a perdu son caractère novateur pour devenir une réalité quotidienne. L'informatique cloud *(cloud computing)* est un modèle permettant un accès généralisé, confortable et sur mesure à un pool de ressources informatiques mutualisées paramétrables (réseaux, serveurs, mémoire, applications et services, p. ex.), lesquelles peuvent être mises à disposition et libérées rapidement avec un minimum de charge administrative ou d'interactions avec le ou les prestataires. Par-delà les considérations économiques, la question de la sécurité de l'information est cruciale, en particulier pour les prestataires de transports publics. Dans le contexte de la numérisation, les aspects relatifs à la sécurité du cloud impactent non seulement les systèmes informatiques, mais aussi, de plus

en plus, les SCI. Toutefois, les aiguillages, les trains ou les autobus s'avèrent difficiles à virtualiser ou à mettre en conteneurs, de sorte qu'une partie au moins des systèmes de commande correspondants devront encore être exploités au niveau local à moyen ou même à long terme.

Il s'ensuit presque toujours une approche hybride, qui exige un concept de sécurité applicable aussi bien aux services d'informatique cloud *(cloud services)* qu'aux services locaux.

L'informatique en cloud n'est pas exempte de risques. Les principaux, pour les transports publics, sont les suivants :

- une défaillance de la connexion internet ou réseau empêchant d'accéder aux données ou aux applications ;
- des attaques de déni de service visant les fournisseurs de services cloud, activités qui sont certainement appelées à s'intensifier ;
- des erreurs dans l'administration du cloud qui, du fait de sa complexité, sont susceptibles de causer de graves problèmes de sécurité (interruption de service, perte de données, etc.). Des erreurs ou pannes minimes peuvent avoir de lourdes conséquences sur une infrastructure cloud (et pas uniquement en termes de sécurité) ;
- le vol d'identités et l'utilisation abusive de comptes ;
- la perte de contrôle sur les données et les applications ;
- une violation des prescriptions et directives en vigueur (exigences en matière de protection des données, p. ex.) ;
- la sécurité des terminaux utilisés pour accéder aux services cloud ;
- l'absence de stratégie d'informatique cloud, de sorte que les objectifs à atteindre ne sont ni clairs ni vérifiables ;
- la volonté d'utiliser l'informatique en cloud à tout prix, qui entraîne des hypothèses trompeuses et des analyses coût-utilité « enjolivées », avec des pertes financières à la clé ;
- la mise en place potentiellement laborieuse de l'informatique en cloud, souvent sans prévoir de solution pour « sortir » du cloud, ce qui peut engendrer une forte dépendance vis-à-vis du fournisseur de services cloud ainsi que des conséquences financières ;
- le recourt fréquent, par les fournisseurs de services cloud, aux services de sous-traitants (administration ou copie de sauvegarde des données, p. ex.). Il se peut dès lors que des données personnelles, par exemple, soient transmises à des organismes non autorisés (ce qui, le cas échéant, est passible d'une amende) ou qu'un certificat de sécurité soit compromis du fait de l'incapacité d'un auditeur à vérifier le sous-traitant ;
- l'hypothèse erronée d'une disponibilité permanente du cloud, de sorte que les utilisateurs n'ont souvent aucun plan de secours.

Recourir à des services d'informatique cloud suppose dès lors de prendre en compte les aspects décrits dans les paragraphes qui suivent.

Définir une stratégie d'informatique cloud

Quelle que soit la dimension du projet d'informatique en cloud, il est nécessaire de connaître les exigences et principes fondamentaux et, à partir de là, d'établir une feuille de route. Faute de quoi, le projet est mal engagé avant même de démarrer. Les entreprises se fient trop facilement aux promesses des prestataires et s'étonnent lorsqu'elles comprennent que le bénéfice escompté, les économies visées ou la sécurité voulue ne sont pas au rendez-vous.

Réaliser des études de faisabilité

Les études de faisabilité permettent notamment de répondre aux questions suivantes :

- Examen du cadre juridique (protection des données, protection du secret, autorités de surveillance, p. ex.) et des directives émanant de l'entreprise ou d'une autorité (conformité). Quel type de données convient-il de traiter dans le cloud ? Le transfert de données sur le cloud est-il autorisé ? Existe-t-il des restrictions concernant le lieu de stockage ou de traitement des données (préoccupations concernant l'accès aux informations par des tiers ou l'espionnage, p. ex.) ?
- L'informatique de l'entreprise a-t-elle le degré de maturité nécessaire pour pouvoir recourir à des services cloud ? Avant de réaliser une infrastructure sous forme de service *(infrastructure as a service, IaaS)* à large échelle, il faut se poser les questions suivantes : les services visés peuvent-ils vraiment être virtualisés ? peuvent-ils être standardisés ? Dans des entreprises de transports publics, ce n'est pas toujours le cas en raison de la multitude des applications et systèmes spéciaux exploités.
- Choix du modèle de service et de déploiement (SaaS, PaaS, IaaS).

Identifier et gérer les risques en matière de cloud

La classification (le besoin de protection) des informations à traiter selon leur confidentialité, leur disponibilité et leur intégrité est primordiale s'agissant des exigences à l'égard d'un service d'informatique en cloud.

Alors que la question de la confidentialité (intervention des services de renseignement, des autorités de poursuite pénale, etc.) occupe l'essentiel du débat public sur la sécurité du cloud, les questions de la disponibilité et de l'intégrité sont tout aussi importantes pour les entreprises de transports publics. Lorsque des systèmes ne sont pas opérationnels, les véhicules ne peuvent pas rouler et, s'ils utilisent des informations erronées, cela peut s'avérer dangereux pour le trafic.

C'est pourquoi l'analyse des risques doit accorder une attention particulière aux menaces suivantes tout au moins :

- accès aux données par le fournisseur de services cloud ;
- possibilités d'accès par les autorités étatiques compte tenu de la juridiction (évent. étrangère) compétente pour le fournisseur de services cloud ;
- indisponibilité des données et des services ;
- authentification compromise ;
- perte de données ;
- manipulation des données ;
- dépendance à l'égard d'un seul fournisseur *(vendor lock-in)* : il est généralement difficile – et même parfois impossible – d'échapper à l'emprise d'un prestataire ;
- perte de savoir *(brain drain)* : en recourant durablement à des services d'informatique cloud, une entreprise perd progressivement les compétences techniques internes lui permettant de se doter de tels services de manière autonome.

Cette analyse pointe déjà les domaines dans lesquels des mesures de sécurité particulières s'imposent ou qui présentent des risques difficilement contrôlables. Pour les entreprises de transports publics, l'accent doit être mis sur les risques d'indisponibilité des données et des services, et d'éventuelles manipulations des données, car s'ils venaient à se concrétiser, ces risques préteriteraient l'exploitation à court ou long terme. Un point est à souligner : il n'existe pas de solution d'informatique cloud qui soit sûre dans tous les cas d'utilisation.

Évaluer le rapport coût-utilité

Une fois les points susmentionnés clarifiés, il y a lieu de procéder à une première évaluation du rapport coût-utilité prenant en considération les aspects suivants :

- coûts de l'utilisation du service ;
- charge administrative interne ;
- formation des collaborateurs et des administrateurs ;
- le cas échéant, nouvelle infrastructure informatique ou nouvelle connexion réseau ;
- coûts de l'adaptation des processus ;
- coûts de la migration ;
- économies internes.

Cette évaluation donne une première indication sur la rentabilité d'un service d'informatique cloud. Les résultats doivent être compilés avant d'être remis aux décideurs, lesquels se prononcent sur la suite des opérations.

Définir les exigences de sécurité

Une fois que la décision de mettre en place un service cloud a été prise sur la base d'une étude de faisabilité, d'une analyse des risques et d'une évaluation du rapport coût-utilité, il s'agit de passer aux étapes de réalisation concrètes du projet.

En plus des exigences fonctionnelles, il importe de fixer des exigences en matière de sécurité de l'information et de disponibilité des services cloud. Celles-ci ne se limitent pas aux règles définies par le fournisseur, mais intègrent également celles de l'entreprise. Il est essentiel que les exigences de sécurité ne soient pas influencées par la décision d'hébergement ou qu'elles ne soient pas revues à la baisse pour permettre l'achat d'un service cloud.

Si l'entreprise ne fixe pas ses propres exigences de sécurité, il lui sera difficile d'expliquer au fournisseur de services cloud ce qu'elle attend de lui. Exiger d'un prestataire une informatique cloud « sûre » et « toujours disponible » sans énoncer d'exigences concrètes est voué à l'échec : soit le niveau de sécurité est insuffisant, soit la solution proposée est trop onéreuse. Si les exigences de sécurité fixées sont impossibles à satisfaire par une solution cloud, il y a lieu de stopper le processus engagé.

Élaborer un concept de sécurité

La documentation existante en matière de sécurité doit être étendue aux aspects relatifs à l'informatique en cloud. Les mesures énoncées dans le concept doivent s'appliquer aussi bien aux systèmes locaux qu'au cloud. Les principaux aspects à prendre en considération sont les suivants :

- Concepts transversaux de gestion des identités et des accès (*identity and access management,* IAM) : il faut veiller à ce que les identités et les rôles numériques de l'entreprise soient, dans la mesure du possible, gérés de manière centralisée et en une seule opération. L'authentification peut ensuite se faire de manière décentralisée au moyen de mécanismes fédératifs (OAuth2, SAML2.0, etc.).
- Systèmes de sécurité : les systèmes de journalisation et de surveillance (SIEM, p. ex.) doivent être conçus pour pouvoir surveiller et corréler aussi bien les services d'informatique cloud que les services locaux. Une faille au sein du périmètre peut affecter immédiatement les services cloud et inversement.

- Modèles zéro confiance *(zero-trust models)* : comme il manque au cloud certaines couches du système de défense par rapport à l'approche de la défense en profondeur décrite au chapitre 3 et qu'il n'est plus possible de les coordonner avec celles présentes dans l'entreprise (typiquement la sécurité du périmètre), une importance particulière doit être accordée non seulement à la surveillance, mais encore à la protection de l'identité, à la qualité de l'authentification et à la gestion des accès. Concrètement, les systèmes et les processus doivent être conçus pour fonctionner de manière sécurisée même si l'environnement n'est pas fiable (internet, p. ex.). Disposer d'un terminal sécurisé et, si possible, éprouvé est ici primordial.

Garantir la protection des données et la conformité

Si des données personnelles sont collectées, traitées ou utilisées dans le cloud, leur protection doit être assurée conformément aux dispositions légales en la matière.

Outre les exigences relatives à la protection des données, l'utilisateur de services cloud doit se conformer aux dispositions juridiques énoncées (conformité). Dans tous les cas, le traitement de telles données dans un cloud implique (généralement) la responsabilité de l'utilisateur, ce dernier devant s'assurer que les données sont traitées chez le fournisseur de services cloud conformément auxdites prescriptions et lois.

3.6.4 Surveillance de la sécurité

L'utilisation de systèmes de surveillance *(monitoring)* et de composants réseau qui détectent les comportements et signatures d'attaque anormaux ajoute un degré de complexité supplémentaire à un environnement informatique ou SCI. En tout état de cause, les fonctionnalités de surveillance et de détection du plan de défense en profondeur visant à protéger les moyens de production critiques sont indispensables. Pour protéger les actifs critiques contre les accès non autorisés, une barrière électronique entourant le réseau du SCI ne suffit pas. Le concept de défense en profondeur prévoit qu'un système de surveillance alerte un organe à un stade précoce en cas d'incident de sécurité. La plupart des organismes disposent d'une forme de surveillance standard dans leur environnement informatique, mais, le plus souvent, ils n'en font pas usage dans leurs réseaux SCI.

Sont incontournables :

- la tenue d'audits approfondis, indépendants et réguliers concernant le statut de sécurité (environnements opérationnels critiques, processus, applications, systèmes et réseaux de soutien) ;
- la surveillance des risques liés à l'information, le respect des exigences légales, réglementaires et contractuelles touchant à la sécurité, et l'établissement de rapports réguliers sur la sécurité de l'information à l'intention de la direction de l'entreprise.

3.6.5 Gestion du cycle de vie du matériel

L'acquisition (achat ou leasing) de matériel résistant et fiable doit toujours satisfaire aux exigences de sécurité. Il s'agit dans tous les cas d'identifier les failles potentielles du matériel.

Il convient de s'assurer que le matériel offre les fonctionnalités requises et ne compromet pas la sécurité des informations et des systèmes critiques ou sensibles tout au long de son cycle de vie.

3.7 Facteur humain

La manipulation des données par l'homme pose de nombreux défis aux entreprises. Les mesures techniques prises ne sauraient exclure totalement les erreurs de manipulation, qu'elles soient malveillantes ou non intentionnelles. Plus la part de collaborateurs inexpérimentés ou non qualifiés est importante dans une entreprise, plus cette entreprise est exposée. Lutter contre les actes de collaborateurs internes mal intentionnés constitue un autre défi. Dans ce contexte, les entreprises doivent traiter les questions décrites dans les paragraphes qui suivent.

3.7.1 Cycle d'emploi des collaborateurs

La sécurité de l'information doit faire partie intégrante du cycle d'emploi, autrement dit de l'embauche du collaborateur jusqu'à son départ. S'inscrivent dans ce cadre les mesures de sécurité relatives, par exemple, à la remise des équipements de travail (matériel, accès aux systèmes) ou à l'accès aux bâtiments et locaux, sans oublier la responsabilité en matière de protection qui en découle. Une formation ad hoc doit être dispensée aux collaborateurs pour les sensibiliser aux enjeux de sécurité et les inciter à adopter les bons réflexes. L'organisme doit garder trace de la tenue et du contenu de ces formations.

L'objectif est de fournir aux collaborateurs les compétences, connaissances et outils leur permettant de défendre les valeurs de l'entreprise ou de l'organisme et de respecter les directives en matière de sécurité de l'information.

3.7.2 Instructions et directives

Le comportement à adopter par les collaborateurs d'une entreprise ou d'un organisme dans les domaines touchant à la sécurité fait l'objet d'instructions et de directives claires et applicables. Ces dernières permettent de mener des contrôles visant à protéger les systèmes et à faire respecter les règles. Elles fixent les procédures et clarifient les attentes de l'entreprise ou de l'organisme vis-à-vis de ses collaborateurs. Elles définissent les règles à respecter et les sanctions à appliquer en cas de violation.

3.7.3 Processus

La gestion de la sécurité, qui est structurée en processus, relève de la responsabilité de l'organe chargé de la sécurité informatique. Son but est de protéger les informations et les données de l'entreprise. Les organismes sont tenus d'appliquer les processus de gestion de la sécurité, y compris aux SCI. Cela vaut pour la définition des processus, l'application des procédures et la configuration des différents systèmes. Ces processus doivent toujours être standardisés et reproductibles, ce qui permet de former tous les nouveaux collaborateurs au même niveau de sécurité et de garantir que toutes les prescriptions et normes requises sont connues.

3.7.4 Tâches et responsabilités dans les environnements opérationnels critiques

Les tâches et responsabilités afférentes aux environnements opérationnels, aux processus, aux applications (y c. les systèmes et réseaux de soutien) et aux informations critiques doivent être clairement définies et confiées à des personnes compétentes.

Le but est que chaque collaborateur développe un sens aigu des responsabilités. La culture d'entreprise ainsi créée contribue à ce que les collaborateurs exécutent leurs tâches dans le respect des impératifs de la sécurité de l'information.

3.7.5 Communication et sensibilisation à la sécurité

La mise en place d'un plan de sensibilisation à la sécurité associée à une communication adaptée induit chez tous les collaborateurs la prise de conscience et le comportement souhaités, et ce à tous les échelons hiérarchiques de l'entreprise.

Le but est d'instaurer une culture d'entreprise favorisant le comportement individuel visé en matière de sécurité. Chacun, dans son domaine de compétence propre, doit être en mesure de prendre des décisions fondées sur les risques.

Exigences et cadre d'évaluation

4 Cadre

Il existe dans le monde une multitude de normes et de sources d'information ayant trait à la gestion des risques informatiques. Certaines sont déjà reconnues et utilisées par les acteurs économiques. Il y a lieu, le cas échéant, de les compléter à l'aide d'autres normes industrielles internationalement reconnues.

Le présent manuel destiné aux entreprises de transports publics s'inspire du cadre de cybersécurité international *NIST Cybersecurity Framework Core* [6]. L'objectif de ce dernier et des recommandations énoncées est de mettre à la disposition des exploitants d'infrastructures critiques et d'autres organismes présentant une dépendance informatique un instrument susceptible d'accroître leur résilience aux risques de sécurité informatique, ce de manière autonome et sous leur propre responsabilité. Ce cadre, qui s'appuie sur une série de normes, de directives et de bonnes pratiques, est neutre sur le plan technologique.

Le cadre mis au point par le NIST est en outre compatible avec les normes ISO 27000 ss. et ISO/CEI 62443, dont l'application constitue un objectif en vertu des dispositions d'exécution de l'ordonnance sur les chemins de fer (DE-OCF 2020). Dans l'optique d'une application de la norme minimale pour les TIC, les différentes normes sont précisées à l'annexe 4.

4.1 Principes

Les principes suivants sont pertinents pour la mise en œuvre :

1. Responsabilité propre : les exploitants d'infrastructures critiques sont responsables du maintien de leurs processus informatiques ou SCI critiques.
2. Gestion des risques : il incombe aux utilisateurs du présent manuel d'évaluer en continu les risques informatiques potentiels tels que la violation de la disponibilité, de l'intégrité et de la confidentialité des données. Les organismes doivent déterminer les risques à atténuer *(mitigate)* et ceux dont ils peuvent s'accommoder.
3. Gestion de la continuité d'activité : tous les aspects relatifs à la sécurité informatique et à la sécurité des SCI doivent être intégrés au système général de gestion de la continuité d'activité.
4. Exhaustivité : le présent manuel regroupe les composantes de mise en œuvre essentielles. L'exhaustivité des mesures de sécurité à appliquer dépend du bilan d'impact sur l'activité et de l'analyse des risques. Il faut tenir compte à cet égard des normes additionnelles nécessaires et des instructions internes et externes données.
5. Culture de la sécurité : afin de garantir une cybersécurité durable, il faut promouvoir une culture de la sécurité au sein des organismes.

4.2 Vue d'ensemble

Ce cadre s'inspire du *NIST Cybersecurity Framework Core* et prend en compte une approche fondée sur les risques et conçue pour aborder et gérer les risques de cybersécurité. Il se compose de cinq fonctions :

1. *identifier (identify) ;*
2. *protéger (protect) ;*
3. *détecter (detect) ;*
4. *réagir (respond) ;*
5. *récupérer (recover).*

Ensemble, ces cinq fonctions forment une vision stratégique de la gestion des risques d'un organisme.

4.3 Niveaux d'implémentation

Le *NIST Cybersecurity Framework* comprend quatre niveaux d'implémentation *(implementation tiers)*, qui décrivent le degré de protection mis en place par un organisme. Ces niveaux vont de partiel (*tier* 1) à dynamique (*tier* 4). Pour déterminer son degré de protection, un organisme doit parfaitement connaître ses pratiques de gestion des risques, son infrastructure, son architecture informatique et TO, le genre de menaces possibles, les exigences légales et réglementaires, ses objectifs et ses besoins organisationnels.

[6] *https://www.nist.gov/cyberframework/online-learning/components-framework*

Les niveaux d'implémentation se définissent comme suit :

Tier 0 : pas mis en œuvre

Bien que l'organisme soit conscient que la mesure considérée devrait en fait déjà être réalisée depuis longtemps, il n'a encore rien entrepris.

Tier 1 : partiel *(partial)*

Le niveau 1 signifie que les processus de gestion des risques et les exigences organisationnelles en matière sécurité informatique ne sont pas formalisés (pas de règles fixées) et que les risques informatiques sont généralement gérés au jour le jour, en mode réactif. L'organisme a mis en place un programme intégré pour gérer les risques au niveau organisationnel, mais il n'y a pas de véritable prise de conscience des risques informatiques ni d'approche globale pour y faire face au sein de l'organisme. Ce dernier ne dispose généralement pas de processus pour relayer en son sein les informations sur la cybersécurité. Il en va de même pour les autres risques informatiques, l'organisme n'a le plus souvent pas prévu de processus standardisés pour communiquer ou coordonner ses activités avec ses partenaires externes.

Tier 2 : conscient des risques *(risk informed)*

Un organisme qui opte pour un classement au niveau 2 dispose généralement de processus de gestion des risques informatiques. Cependant, ces processus ne sont pas concrètement appliqués ni obligatoires. Au niveau organisationnel, les risques informatiques sont intégrés dans un système de gestion global et tous les niveaux hiérarchiques ont été sensibilisés aux risques informatiques. Généralement, aucune approche globale n'a été mise en place pour gérer et améliorer la sensibilisation aux risques informatiques, actuels et futurs. Les processus et méthodes approuvés sont définis et mis en œuvre. Les collaborateurs disposent de ressources suffisantes pour effectuer leurs tâches de cybersécurité. Les informations sur la cybersécurité sont partagées de manière informelle au sein de l'organisme. Ce dernier est conscient de son rôle et n'hésite pas à communiquer avec ses partenaires externes (clients, fournisseurs, prestataires de services, etc.) sur les questions de cybersécurité. Il n'existe cependant aucun processus standardisé pour collaborer ou échanger des informations avec ces partenaires.

Tier 3 : reproductible *(repeatable)*

Un organisme de niveau 3 a formellement validé ses plans de gestion des risques et les prescriptions internes régissant l'application de ces derniers. La gestion des risques informatiques est définie dans les directives de l'organisme. Les risques informatiques sont appréhendés de manière standardisée et les prescriptions en la matière font l'objet de mises à jour régulières. Cette pratique tient compte des nouveaux besoins de l'organisme, des progrès technologiques et d'un environnement où les menaces sont mouvantes, que ce soit à cause de nouveaux acteurs ou de l'évolution du contexte politique.

La documentation interne décrit les processus et procédures pour gérer les nouveaux risques. Des méthodes standardisées sont définies pour répondre à l'évolution des menaces. Les collaborateurs ont les connaissances et les compétences nécessaires pour accomplir leurs tâches.

L'organisme sait qu'il est tributaire de ses partenaires externes. Il partage les informations qui lui permettent, face à des incidents, de prendre lui-même des décisions.

Tier 4 : dynamique *(adaptive)*

Le niveau 4 signifie qu'un organisme répond entièrement aux exigences des niveaux 1 à 3 et que, de plus, il analyse en permanence ses propres processus, méthodes et capacités pour les adapter, le cas échéant. L'amélioration continue exige de bien documenter tous les incidents de cybersécurité. L'organisme tire les leçons nécessaires de l'analyse des incidents passés et adapte, de manière dynamique, ses processus et techniques de sécurité aux technologies de pointe et à l'évolution des menaces. La gestion des risques informatiques est partie intégrante de la culture d'entreprise. Les enseignements tirés des incidents passés, les informations provenant de sources externes et la surveillance constante des systèmes et réseaux internes sont constamment intégrés dans le processus de gestion des risques. L'organisme partage régulièrement ses informations avec ses partenaires en recourant à des processus standardisés.

n/a : non applicable

Cette mesure n'est délibérément pas mise en œuvre par l'organisme, après avoir effectué sa propre évaluation des risques.

Profils

Un profil est le résultat de l'ajustement aux normes, aux directives et aux bonnes pratiques du cadre de cybersécurité, conjugué à un scénario d'implantation individuel. Les profils peuvent servir à identifier les options envisageables pour améliorer la cybersécurité, par exemple en comparant un profil réel et un profil souhaité. L'outil d'évaluation fourni avec le présent manuel sert précisément à paramétrer un tel profil. L'évaluation des 106 activités répertoriées dans le questionnaire donne des résultats agrégés d'après les cinq fonctions du cadre de cybersécurité (identifier, protéger, détecter, réagir et rétablir). Le niveau minimal requis est réputé atteint lorsque la cote globale de l'évaluation de la cybersécurité indique des valeurs empiriques (« réalité ») égales ou supérieures aux valeurs minimales requises (« cible »). L'outil d'évaluation inclut une marche à suivre.

Exemple d'évaluation de la cybersécurité

Cote globale de l'évaluation de la cybersécurité	réalité	cible
Identifier *(Identify)*	2.8	2.6
Protéger *(Protect)*	2.7	2.6
Détecter *(Detect)*	2.9	2.6
Réagir *(Respond)*	2.0	2.6
Récupérer *(Recover)*	1.4	2.6

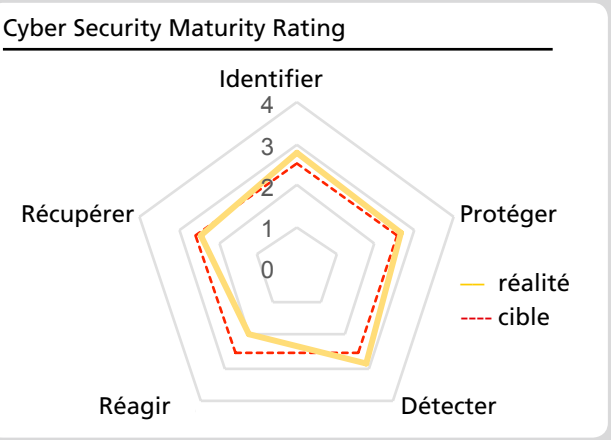


Figure 6 : Exemple de cote globale de l'évaluation de la cybersécurité

4.4 Identifier *(Identify [ID])*

Inventaire et organisation *(Assest Management [AM])*

Les données, les personnes, les appareils, les systèmes et les installations d'une entreprise sont identifiés, catalogués et évalués. L'évaluation se fait en fonction de leur criticité pour les processus opérationnels à mettre en place et de la stratégie de l'entreprise en matière de risque.

Désignation	Tâche
ID.AM-1	Développez un processus d'inventaire garantissant en permanence un recensement exhaustif de vos équipements TIC *(Asset)*.
ID.AM-2	Inventoriez toutes les plateformes, licences et applications logicielles dans votre entreprise.
ID.AM-3	Listez tous les flux de communication et de transferts de données en interne.
ID.AM-4	Listez tous les systèmes TIC externes cruciaux pour votre entreprise.
ID.AM-5	Établissez des priorités pour les ressources inventoriées (équipements, applications, données) selon leur criticité.
ID.AM-6	Définissez clairement les rôles et les responsabilités en matière de cybersécurité.

Tableau 7 : Tâches ID.AM

Norme	Référence
CCS CSC 1	1, 2, 13, 14, 17,19
COBIT 5	BAI09.01, BAI09.02, BAI09.05, DSS05.02, APO02.02, APO10.04, DSS01.02, APO03.03, APO03.04, APO12.01, BAI04.02, APO01.02, APO07.06, APO13.01, DSS06.03
ISA 62443-3:2013	SR 7.8
ISO 27001:2013	A.6.1.1, A.8.1.1, A.8.1.2, A.8.2.1, A.11.2.6, A.12.5.1, A.13.2.1, A.13.2.2
NIST-SP-800-53 Rev. 4	AC-4, CA-3, CA-9, PL-8, CM-8, PM-5, AC-20, SA-9, CP-2, RA-2, SA-14, SC-6, PS-7, PM-11

Tableau 8 : Références ID.AM

Environnement de l'entreprise *(Business Environment [BE])*

Les objectifs, les tâches et les activités de l'entreprise sont hiérarchisés et évalués.
Cette information sert à répartir les responsabilités.

Désignation	Tâche
ID.BE-1	Définissez, documentez et communiquez le rôle exact de votre entreprise dans la chaîne d'approvisionnement (critique).
ID.BE-2	Identifiez et communiquez l'importance de votre entreprise en tant qu'infrastructure vitale et sa position dans le secteur critique.
ID.BE-3	Évaluez et hiérarchisez les objectifs, les tâches et les activités dans l'entreprise.
ID.BE-4	Listez tous les systèmes TIC externes cruciaux pour votre entreprise.
ID.BE-5	Priorisez les ressources inventoriées (équipements, applications, données) selon leur criticité.

Tableau 9 : Tâches ID.BE

Norme	Référence
CCS CSC 1	1, 2
COBIT 5	APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05, APO02.06, APO03.01, APO02.01, APO10.01, BAI04.02, BAI03.02, DSS04.02, BAI09.02
ISA 62443-3:2013	SR 7.8
ISO 27001:2013	A.6.1.1, A.8.1.1, A.8.1.2, A.8.2.1, A.11.2.6
NIST-SP-800-53 Rev. 4	SA-12, CP-2, SA-14, CP-2, PM-11, PM-8, CP-8, PE-9, PE-11, CP-11, SA-13

Tableau 10 : Références ID.BE

Règles *(Governance [GV])*

Une bonne gouvernance fixe les responsabilités, surveille et s'assure que les exigences réglementaires, juridiques et opérationnelles soient respectées dans la sphère d'activité.

Désignation	Tâche
ID.GV-1	Édictez des directives sur les besoins en sécurité informatique dans votre entreprise.
ID.GV-2	Convenir entre les responsables internes (gestion des risques par ex.) et des partenaires externes, des rôles et des responsabilités en matière de sécurité informatique.
ID.GV-3	Vérifiez que votre entreprise respecte toutes les exigences légales et réglementaires en matière de cybersécurité, y compris au niveau de la protection des données.
ID.GV-4	Assurez-vous que les cyber-risques sont bien intégrés dans la gestion des risques pour toute l'entreprise.

Tableau 11 : Tâches ID.GV

Norme	Référence
COBIT 5	APO13.01, APO01.02, APO10.03, DSS05.04, APO13.02, MEA03.01, MEA03.04, DSS04.02, BAI02.01, EDM03.02, APO12.02, APO12.05
ISA 62443-3:2013	
ISO 27001:2013	A.5.1.1, A.6.1.1, A.7.2.1, A.15.1.1, A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5, Clause 6
NIST-SP-800-53 Rev. 4	PM-1, PM-2, PS-7, PM-9, PM-10, PM-11, Rev.4-1 *controls from all security control families,* SA-2, PM-3, PM-7

Tableau 12 : Références ID.GV

Analyse de risque *(Risk Assessment [RA])*

L'entreprise analyse l'impact des cyber-risques sur ses activités, ses équipements et son personnel, y compris les risques réputationnels.

Désignation	Tâche
ID.RA-1	Identifiez les faiblesses (techniques) de vos équipements et documentez-les.
ID.RA-2	Participez à des forums et à des réunions d'experts pour échanger des informations et être au courant des cybermenaces.
ID.RA-3	Identifiez et documentez les cybermenaces, aussi bien internes qu'externes.
ID.RA-4	Identifiez l'impact potentiel des cybermenaces sur vos activités et évaluez leur probabilité d'occurrence.
ID.RA-5	Évaluez les risques pour votre entreprise en fonction des menaces, des vulnérabilités, de l'impact (sur ses activités) et de leur probabilité d'occurrence.
ID.RA-6	Définissez les mesures à prendre immédiatement lorsqu'un risque se concrétise et fixez des priorités.

Tableau 13 : Tâches ID.RA

Norme	Référence
COBIT 5	APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02, BAI08.01, APO 12.05, APO 13.02, DSS04.02
ISA 62443-3:2013	4.2.3, 4.2.3.9, 4.2.3.12
ISO 27001:2013	A.12.6.1, A.18.2.3, A.6.1.4, Clause 6.1.2, A.16.1.6, Clause 6.1.3
NIST-SP-800-53 Rev. 4	CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5, PM-15, PM-16, SI-5, RA-3, SI-5, PM-12, RA-2, PM-9, PM-11, SA-14, PM-4

Tableau 14 : Références ID.RA

Stratégie pour gérer les risques *(Risk Management Strategy [RM])*

Définissez les priorités, les restrictions et les risques maximaux supportables pour votre entreprise. Évaluez vos risques opérationnels sur cette base.

Désignation	Tâche
ID.RM-1	Définissez les processus de gestion des risques, gérez-les activement et faites-les confirmer par les personnes impliquées ou les parties prenantes.
ID.RM-2	Définissez et communiquez les risques supportables pour votre entreprise.
ID.RM-3	Assurez-vous que les risques supportables sont évalués en prenant en compte l'importance de votre entreprise du fait qu'elle exploite une infrastructure critique. Prenez également en considération, dans votre analyse, les risques propres au secteur.

Tableau 15 : Tâches ID.RM

Norme	Référence
COBIT 5	APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02, APO12.06, APO12.02
ISA 62443-3:2013	4.3.4.2, 4.3.2.6.5
ISO 27001:2013	Clause 6.1.3, Clause 8.3, Clause 9.3
NIST-SP-800-53 Rev. 4	PM-8, PM-9, PM-11, SA-14

Tableau 16 : Références ID.RM

Gestion des risques liés à la chaîne d'approvisionnement *(Supply Chain Riskmanagement [SC])*

Définissez les priorités, les restrictions et les risques maximaux que votre entreprise peut accepter par rapport à ses fournisseurs.

Désignation	Tâche
ID.SC-1	Définissez des processus clairs pour gérer les risques liés à une perturbation dans la chaîne d'approvisionnement. Faites contrôler et valider ces processus par toutes les parties prenantes.
ID.SC-2	Identifiez les fournisseurs et les prestataires de services cruciaux pour vos systèmes, composants et services critiques à partir des processus définis ci-dessus et fixez les priorités.
ID.SC-3	Exigez de vos fournisseurs et prestataires de services qu'ils s'engagent contractuellement à développer et mettre en œuvre des mesures appropriées pour atteindre les objectifs du processus pour gérer les risques liés à la chaîne d'approvisionnement.
ID.SC-4	Faites un suivi systématique pour vous assurer que tous vos fournisseurs et prestataires de services remplissent leurs obligations conformément aux exigences. Faites-le vérifier régulièrement par des rapports d'audit ou par les résultats des tests techniques.
ID.SC-5	Définissez avec vos fournisseurs et prestataires les processus pour réagir et récupérer après des problèmes de cybersécurité. Validez ces processus par des simulations.

Tableau 17 : Tâches ID.SC

Norme	Référence
COBIT 5	APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI01.03, BAI02.03, BAI04.02, APO10.03, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05, DSS04.04
ISA 62443-3:2013	4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14, 4.3.2.6., 4.3.2.5.7, 4.3.4.5.11
ISO 27001:2013	A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2, A.15.2.1, A.15.2.2, A.17.1.3
NIST-SP-800-53 Rev. 4	SA-9, SA-12, PM-9, RA-2, RA-3, SA-14, SA-15, SA-11, AU-2, AU-6, AU-12, AU-16, PS-7, CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9

Tableau 18 : Références ID.SC

4.5 Protéger *(Protect [PR])*

Gestion des accès *(Access Control [AC])*

Veiller à ce que l'accès physique et logique (à distance) aux équipements et installations TIC ne soient possibles que pour les personnes, processus et appareils autorisés et à ce que seules les activités prévues soient permises.

Désignation	Tâche
PR.AC-1	Définissez un processus clair pour octroyer et gérer les autorisations et les données d'identification pour utilisateurs, appareils/machines et processus.
PR.AC-2	Assurez-vous que seules les personnes autorisées ont physiquement accès aux équipements TIC. Prenez des mesures concrètes pour garantir que les ressources TIC sont protégées contre tout accès physique non autorisé.
PR.AC-3	Définissez les processus pour gérer les accès à distance.
PR.AC-4	Définissez les niveaux d'autorisation en étant le plus restrictif possible et séparez les fonctions.
PR.AC-5	Contrôlez que l'intégrité de votre réseau est protégée. Séparez votre réseau au niveau logique comme physique, si c'est nécessaire et judicieux.
PR.AC-6	N'attribuez des identités numériques qu'à des personnes ou à des processus que vous avez clairement identifiés.

Tableau 19 : Tâches PR.AC

Norme	Référence
COBIT 5	DSS05.04, DSS06.03, DSS01.04, DSS05.05, APO13.01, DSS01.04, DSS05.03, DSS01.05, DSS05.02, DSS05.07, DSS05.10, DSS06.10
ISA 62443-3:2013	SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.13, SR 2.1, SR 2.6, SR 3.1, SR 3.8, SR 2.2, SR 2.3, SR 1.10
ISO 27001:2013	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8, A.6.2.1, A.6.2.2, A13.1.1, A.13.2.1, A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.6.1.2, A.7.1.1, A.9.1.2, A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.6, A.13.1.3, A.14.1.2, A.14.1.3, A.9.3.1, A.18.1.4, A.9.4.1, A.9.4.4
NIST-SP-800-53 Rev. 4	AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11, PE-2, PE-3, PE-4, PE-5, PE-6, PE-8, AC-17, AC-19, AC-20, SC-15, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24, AC-4, AC-10, SC-7, AC-7, AC-8, AC-9, AC-11, AC-12, AC-14

Tableau 20 : Références PR.AC

Sensibilisation et formation *(Awareness and Training [AT])*

Assurez-vous que vos employés et vos partenaires externes sont correctement formés et conscients de tous les aspects de la cybersécurité. Veillez à ce qu'ils exécutent les Tâches impactant la sécurité conformément aux exigences et aux processus définis.

Désignation	Tâche
PR.AT-1	Veillez à ce que tous vos collaborateurs soient sensibilisés et formés en matière de cybersécurité.
PR.AT-2	Veillez à ce que les utilisateurs ayant des niveaux d'autorisation élevés soient conscients de leur rôle et de leurs responsabilités.
PR.AT-3	Veillez à ce que tous les acteurs extérieurs à votre entreprise (fournisseurs, clients, partenaires) soient conscients de leur rôle et de leurs responsabilités.
PR.AT-4	Veillez à ce que tous les cadres soient conscients de leurs rôles spécifiques et de leurs responsabilités.
PR.AT-5	Veillez à ce que les responsables de la sécurité physique et de la sécurité informatique soient conscients de leurs rôles spécifiques et de leurs responsabilités.

Tableau 21 : Tâches PR.AT

Norme	Référence
COBIT 5	APO07.03, BAI05.07, APO07.02, DSS05.04, DSS06.03, APO07.06, APO10.04, APO10.05, EDM01.01, APO01.02
ISA 62443-3:2013	4.3.2.4.2, 4.3.2.4.3
ISO 27001:2013	A.7.2.2, A.12.2.1, A.6.1.1, A.7.2.1
NIST-SP-800-53 Rev. 4	AT-2, AT-3, PM-13, PS-7, SA-9, SA-16, IR-2

Tableau 22 : Références PR.AT

Sécurité des données *(Data Security [DS])*

Assurez-vous que les informations, les données et leurs supports sont gérés de manière à protéger la confidentialité, l'intégrité et la disponibilité des données, conformément à la stratégie de votre entreprise pour gérer les risques.

Désignation	Tâche
PR.DS-1	Assurez-vous que les données stockées sont protégées (contre toute atteinte ou préjudice en termes de confidentialité, d'intégrité et de disponibilité).
PR.DS-2	Assurez-vous que les données sont protégées pendant leur transmission (contre toute atteinte ou préjudice en termes de confidentialité, d'intégrité et de disponibilité).
PR.DS-3	Veuillez à ce qu'un processus formel soit défini pour votre matériel TIC afin de protéger les données lorsque des équipements sont supprimés, déplacés ou remplacés.
PR.DS-4	Veillez à disposer d'une réserve de capacité suffisante afin que vos données soient toujours disponibles.
PR.DS-5	Assurez-vous que des mesures appropriées sont mises en œuvre contre les fuites de données (« pompage »).
PR.DS-6	Définissez un processus pour vérifier l'intégrité du micrologiciel, des systèmes d'exploitation, des logiciels d'application et des données.
PR.DS-7	Ayez un environnement informatique pour le développement et les tests qui soit totalement indépendant des systèmes de production.
PR.DS-8	Définissez un processus pour vérifier l'intégrité du matériel utilisé.

Tableau 23 : Tâches PR.DS

Norme	Référence
COBIT 5	APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06, DSS05.02, BAI09.03, APO13.01, BAI04.04, DSS05.04, DSS05.07, DSS.06.02, BAI03.08, BAI07.04, BAI03.05
ISA 62443-3:2013	SR 3.4, SR 4.1, SR 3.1, SR 3.8, SR 4.1, SR 4.2, SR 7.1, SR 7.2, SR 5.2, SR 3.3
ISO 27001:2013	A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7, A.11.2.5, A.12.1.3, A.17.2.1, A.12.3.1, A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.13.1.3, A.13.2.1, A.13.2.4, A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4, A.12.1.4, A.11.2.4
NIST-SP-800-53 Rev. 4	MP-8, SC-12, SC-28, SC-8, SC-11, CM-8, MP-6, PE-16, AU-4, CP-2, SC-5, AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-13, SC-31, SI-4, SI-7, SC-16, CM-2, SA-10

Tableau 24 : Références PR.DS

Règles de protection des données *(Information Protection Processes and Procedures [IP])*

Assurez-vous que les données sont protégées pendant leur transmission (contre toute atteinte ou préjudice en termes de confidentialité, d'intégrité et de disponibilité).

Désignation	Tâche
PR.IP-1	Générez une configuration standard pour l'infrastructure d'information et de communication, ainsi que pour les systèmes de contrôle industriel. Assurez-vous que cette configuration par défaut obéit aux règles usuelles de sécurité (par ex. redondance N-1, configuration minimale, etc.).
PR.IP-2	Définissez un processus « cycle de vie » pour le développement de systèmes.
PR.IP-3	Définissez un processus pour contrôler les changements de configuration.
PR.IP-4	Assurez-vous que des sauvegardes informatiques *(Backups)* sont effectuées, gérées et testées régulièrement (+ qu'on peut restaurer les données sauvegardées).
PR.IP-5	Contrôlez que toutes les exigences (réglementaires) et les directives concernant les équipements « physiques » soient respectées.
PR.IP-6	Contrôlez que les données soient toujours détruites selon les prescriptions.
PR.IP-7	Développez et améliorez régulièrement vos processus de sécurité informatique.
PR.IP-8	Discutez de l'efficacité des différentes technologies de protection avec vos partenaires.
PR.IP-9	Instaurez des processus pour réagir aux cyberincidents *(Incident Response-Planning, Business Continuity Management, Incident Recovery, Disaster Recovery)*.
PR.IP-10	Testez les plans d'intervention et de récupération.
PR.IP-11	Tenez compte de la cybersécurité dès le processus de recrutement (en vérifiant les antécédents ou par des contrôles de sécurité personnels, par ex.).
PR.IP-12	Développez et mettez en œuvre un processus pour traiter les failles repérées.

Tableau 25 : Tâches PR.IP

Norme	Référence
COBIT 5	BAI10.01, BAI10.02, BAI10.03, BAI10.05, APO13.01, BAI03.01, BAI03.02, BAI03.03, BAI06.01, BAI01.06, APO13.01, DSS01.01, DSS04.07, DSS01.04, DSS05.05, BAI09.03, DSS 05.06, APO11.06, APO12.06, DSS04.05, BAI08.04, DSS03.04, DSS04.03, DSS04.04, APO07.01, APO07.02, APO07.03, APO07.04, APO07.05, BAI03.10, DSS05.02
ISA 62443-3:2013	SR 7.6, SR 7.3, SR 7.4, SR 4.2, SR 3.3
ISO 27001:2013	A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5, A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4, A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3, A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3, A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7, A.16.1.6, Clause 9, Clause 10, A.16.1.1, A.17.1.1, A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4, A.17.1.2, A.17.1.3, A.12.6.1, A.16.1.3, A.18.2.2, A.18.2.3
NIST-SP-800-53 Rev. 4	CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10, SA-3, SA-4, SA-8, SA-11, SA-12, SA-15, SA-17, PL-8, SI-12, SI-13, SI-14, SI-16, SI-17, CP-4, CP-6, CP-9, PE-10, PE-12, PE-13, PE-14, PE-15, PE-18, MP-6, CA-2, CA-7, CP-2, IR-8, PL-2, PM-6, AC-21, SI-4, CP-7, CP-12, CP-13, IR-7, IR-9, PE-17, IR-3, PM-14, PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21, RA-3, RA-5, SI-2

Tableau 26 : Références PR.IP

Maintenance *(Maintenance [MA])*

Veillez à ce que la maintenance et la réparation des composantes des systèmes TIC et du SCI soient effectuées conformément aux directives et méthodes en vigueur.

Désignation	Tâche
PR.MA-1	Veillez à ce que le fonctionnement, la maintenance et les éventuelles réparations des équipements soient enregistrés et documentés (journalisation). Assurez-vous qu'elles sont effectuées rapidement et en ne recourant qu'à des moyens testés et approuvés.
PR.MA-2	Enregistrez et documentez également les travaux de maintenance de vos systèmes distants. Assurez-vous qu'aucun accès non autorisé n'est possible.

Tableau 27 : Tâches PR.MA

Norme	Référence
COBIT 5	BAI03.10, BAI09.02, BAI09.03, DSS01.05, DSS05.04
ISA 62443-3:2013	
ISO 27001:2013	A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6, A.15.1.1, A.15.2.1
NIST-SP-800-53 Rev. 4	MA-2, MA-3, MA-4, MA-5, MA-6

Tableau 28 : Références PR.MA

Technologie de protection *(Protective Technology [PT])*

Installez des solutions techniques pour assurer la sécurité et la résilience de votre système et de vos données selon les exigences et processus.

Désignation	Tâche
PR.PT-1	Définissez les exigences pour les audits et les enregistrements de journaux. Générez et vérifiez ces journaux régulièrement, selon les exigences et les directives.
PR.PT-2	Assurez-vous que les supports amovibles sont protégés et que leur utilisation se fait dans le strict respect des directives.
PR.PT-3	Veillez à ce que votre système soit configuré pour toujours fonctionner, même en mode dégradé (système renforcé).
PR.PT-4	Assurez la protection de vos réseaux de communication et de contrôle.
PR.PT-5	Définissez des scénarios pour les différents modes de fonctionnement de vos systèmes. Par ex. : fonctionnalités en cas d'attaque, fonctionnalités pendant la phase de récupération, fonctionnalités normales pendant l'exploitation.

Tableau 29 : Tâches PR.PT

Norme	Référence
COBIT 5	APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01, DSS05.02, DSS05.06, APO13.01, DSS05.05, DSS06.06, BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05
ISA 62443-3:2013	SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 2.3, SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.4, SR 2.5, SR 2.6, SR 2.7, SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.2, SR 7.6
ISO 27001:2013	A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1, A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9, A.9.1.2, A.13.1.1, A.13.2.1, A.14.1.3, A.17.1.2, A.17.2.1
NIST-SP-800-53 Rev. 4	AU *Family,* MP-2, MP-3, MP-4, MP-5, MP-7, MP-8, AC-3, CM-7, AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43, CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6

Tableau 30 : Références PR.PT

4.6 Détecter *(Detect [DE])*

Anomalies et incidents *(Anomalies and Events [AE])*

Veillez à ce que les anomalies et autres événements (exceptionnels) soient détectés à temps et que le personnel soit conscient de l'impact potentiel de ces incidents.

Désignation	Tâche
DE.AE-1	Définissez des valeurs par défaut pour les opérations réseau licites et les flux de données prévus pour les utilisateurs et les systèmes. Surveillez ces valeurs en permanence.
DE.AE-2	Assurez-vous que les incidents de cybersécurité détectés sont analysés quant à leurs objectifs et méthodes.
DE.AE-3	Assurez-vous que les informations sur les incidents de cybersécurité provenant de différentes sources et capteurs sont compilées et exploitées.
DE.AE-4	Déterminez les conséquences probables des incidents.
DE.AE-5	Définissez les valeurs limites au-delà desquelles les incidents de cybersécurité doivent générer des alertes.

Tableau 31 : Tâches DE.AE

Norme	Référence
COBIT 5	DSS03.01, DSS05.07, APO12.06, BAI08.02
ISA 62443-3:2013	SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2
ISO 27001:2013	A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2, A.12.4.1, A.16.1.1, A.16.1.4, A.16.1.7
NIST-SP-800-53 Rev. 4	AC-4, CA-3, CM-2, SI-4, AU-6, CA-7, IR-4, IR-5, IR-8, SI-4, CP-2, RA-3

Tableau 32 : Références DE.AE

Surveillance *(Security Continuous Monitoring [CM])*

Veillez à ce que le système TIC, équipements compris, soit régulièrement contrôlé pour pouvoir détecter les incidents de cybersécurité et vérifier l'efficacité des mesures de protection.

Désignation	Tâche
DE.CM-1	Mettez en place une surveillance permanente du réseau pour détecter les incidents de cybersécurité potentiels.
DE.CM-2	Mettez en place une surveillance continue (monitorage) de tous les équipements et des bâtiments pour détecter les incidents de cybersécurité.
DE.CM-3	Mettez en place un monitorage des cyberactivités des employés pour détecter les incidents de cybersécurité potentiels.
DE.CM-4	Veillez à pouvoir détecter les maliciels.
DE.CM-5	Veillez à pouvoir détecter les maliciels sur les appareils portables.
DE.CM-6	Assurez-vous que les activités des prestataires de services externes sont surveillées (monitorées) pour détecter d'éventuels incidents de cybersécurité.
DE.CM-7	Surveillez votre système en permanence pour être certain que des activités ou accès liés à des personnes, équipements ou logiciels non autorisés seront détectés.
DE.CM-8	Procédez à des tests de vulnérabilité.

Tableau 33 : Tâches DE.CM

Norme	Référence
COBIT 5	DSS05.07, DSS05.01, APO07.06, BAI03.10, DSS01.03, DSS03.05, DSS01.04, DSS01.05, APO10.05, DSS05.02, DSS05.05
ISA 62443-3:2013	SR 6.2, SR 3.2, SR 2.4
ISO 27001:2013	A.11.1.1, A.11.1.2, A.12.4.1, A.12.4.3, A.12.2.1, A.12.5.1, A.12.6.2, A.14.2.7, A.15.2.1, A.12.6.1
NIST-SP-800-53 Rev. 4	AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4, AU-13, CM-10, CM-11, SI-3, SI-8, SC-18, SC-44, PS-7, SA-4, SA-9, CM-8, PE-3, PE-6, PE-20, RA-5

Tableau 34 : Références DE.CM

Processus de détection *(Detection Processes [DP])*

Maintenez, testez et entretenez les processus et les instructions pour détecter les incidents de cybersécurité.

Désignation	Tâche
DE.DP-1	Définissez clairement les rôles et les responsabilités pour que tous sachent bien qui est responsable de quoi et qui a telles ou telles compétences.
DE.DP-2	Assurez-vous que les processus de détection correspondent aux exigences et conditions fixées.
DE.DP-3	Testez vos processus de détection.
DE.DP-4	Communiquez aux personnes concernées (par ex. fournisseurs, clients, partenaires, autorités) les incidents que vous avez détectés.
DE.DP-5	Améliorez en permanence vos processus de détection.

Tableau 35 : Tâches DE.DP

Norme	Référence
COBIT 5	APO01.02, DSS05.01, DSS06.03, DSS06.01, MEA03.03, MEA03.04, APO13.02, DSS05.02, APO08.04, APO12.06, DSS02.05, APO11.06, DSS04.05
ISA 62443-3:2013	SR 3.3, SR 6.1
ISO 27001:2013	A.6.1.1, A.7.2.2, A.18.1.4, A.18.2.2, A.18.2.3, A.14.2.8, A.16.1.2, A.16.1.3, A.16.1.6
NIST-SP-800-53 Rev. 4	CA-2, CA-7, PM-14, AC-25, SA-18, SI-3, SI-4, PE-3, PM-14, AU-6, RA-5, PL-2

Tableau 36 : Références DE.DP

4.7 Réagir *(Respond [RS])*

Plan d'intervention *(Response Planning [RP])*

Élaborez un plan d'intervention pour traiter les incidents de cybersécurité détectés. Assurez-vous qu'en cas d'incident ce plan d'intervention est exécuté correctement et en temps utile.

Désignation	Tâche
RS.RP-1	Assurez-vous que le plan d'intervention est correctement suivi et rapidement exécuté si un incident de cybersécurité est détecté.

Tableau 37 : Tâches RS.RP

Norme	Référence
COBIT 5	APO12.06, BAI01.10
ISA 62443-3:2013	
ISO 27001:2013	A.16.1.5
NIST-SP-800-53 Rev. 4	CP-2, CP-10, IR-4, IR-8

Tableau 38 : Références RS.RP

Communications *(Communications [CO])*

Contrôlez que vos processus de réaction soient coordonnés avec ceux des parties prenantes, internes et externes. Selon le type d'incident, veillez à pouvoir bénéficier du soutien des autorités si la situation l'exige.

Désignation	Tâche
RS.CO-1	Assurez-vous que toutes les personnes connaissent leurs tâches et la marche à suivre lorsqu'elles doivent réagir à un incident de cybersécurité.
RS.CO-2	Définissez des critères pour les communications et assurez-vous que les incidents de cybersécurité sont signalés et traités conformément à ces critères.
RS.CO-3	Partagez les informations sur les incidents de cybersécurité relevés – ainsi que les enseignements qui en découlent – selon ces critères prédéfinis.
RS.CO-4	Coordonnez-vous avec les parties prenantes selon ces critères.
RS.CO-5	Améliorez la sensibilisation aux incidents de cybersécurité grâce à des échanges réguliers avec vos partenaires.

Tableau 39 : Tâches RS.CO

Norme	Référence
COBIT 5	EDM03.02, APO01.02, APO12.03, DSS01.03, DSS03.04, BAI08.04
ISA 62443-3:2013	
ISO 27001:2013	A.6.1.1, A.7.2.2, A.16.1.1, A.6.1.3, A.16.1.2, Clause 7.4, Clause 16.1.2, A.6.1.4
NIST-SP-800-53 Rev. 4	CP-2, CP-3, IR-3, IR-8, AU-6, IR-6, CA-2, CA-7, IR-4, PE-6, RA-5, SI-4, SI-5, PM-15

Tableau 40 : Références RS.CO

Analyses *(Analysis [AN])*

Effectuez régulièrement des analyses afin de réagir correctement en cas d'incidents de cybersécurité.

Désignation	Tâche
RS.AN-1	Assurez-vous que les alertes émanant de systèmes de détection sont prises en compte et déclenchent des enquêtes.
RS.AN-2	Veillez à pouvoir évaluer correctement l'impact d'un incident de cybersécurité.
RS.AN-3	Effectuez une analyse technique après chaque incident.
RS.AN-4	Classez les incidents selon les exigences du plan d'intervention.

Tableau 41 : Tâches RS.AN

Norme	Référence
COBIT 5	DSS02.04, DSS02.07, DSS02.02, APO12.06, DSS03.02, DSS05.07, EDM03.02
ISA 62443-3:2013	SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1
ISO 27001:2013	A.12.4.1, A.12.4.3, A.16.1.5, A.16.1.6, A.16.1.7, A.16.1.4
NIST-SP-800-53 Rev. 4	AU-6, CA-7, IR-4, IR-5, PE-6, SI-4, CP-2, AU-7, IR-8, SI-5, PM-15

Tableau 42 : Références RS.AN

Circonscrire les dommages *(Mitigation [MI])*

Faites tout pour éviter qu'un incident de cybersécurité se propage afin de limiter les éventuels dommages.

Désignation	Tâche
RS.MI-1	Assurez-vous que les incidents de cybersécurité peuvent être circonscrits et que vous pouvez stopper leur impact.
RS.MI-2	Assurez-vous de pouvoir réduire l'impact des incidents de cybersécurité.
RS.MI-3	Veillez à réduire au maximum les failles ainsi découvertes ou référencez-les comme des risques acceptables.

Tableau 43 : Tâches RS.MI

Norme	Référence
COBIT 5	APO12.06
ISA 62443-3:2013	SR 5.1, SR 5.2, SR 5.4
ISO 27001:2013	A.12.2.1, A.16.1.5, A.12.6.1
NIST-SP-800-53 Rev. 4	IR-4, CA-7, RA-3, RA-5

Tableau 44 : Références RS.MI

Améliorations *(Improvements [IM])*

Améliorez régulièrement la réactivité de votre entreprise face aux incidents de cybersécurité en tirant les enseignements des incidents précédents.

Désignation	Tâche
RS.IM-1	Assurez-vous que les enseignements tirés des précédents incidents de cybersécurité sont intégrés à vos plans d'intervention.
RS.IM-2	Actualisez vos stratégies de réaction.

Tableau 45 : Tâches RS.IM

Norme	Référence
COBIT 5	BAI01.13, DSS04.08
ISA 62443-3:2013	
ISO 27001:2013	A.16.1.6, Clause 10
NIST-SP-800-53 Rev. 4	CP-2, IR-4, IR-8

Tableau 46 : Références RS.IM

4.8 Récupérer *(Recover [RC])*

Plan de restauration *(Recovery Planning [RP])*

Contrôlez que les processus de récupération sont tenus à jour pour être exécutés en tout temps, permettant ainsi une récupération rapide des systèmes.

Désignation	Tâche
RC.RP-1	Assurez-vous que le plan de récupération est suivi à la lettre en cas d'incident de cybersécurité.

Tableau 47 : Tâches RC.RP

Norme	Référence
COBIT 5	APO12.06, DSS02.05, DSS03.04
ISA 62443-3:2013	
ISO 27001:2013	A.16.1.5
NIST-SP-800-53 Rev. 4	CP-10, IR-4, IR-8

Tableau 48 : Références RC.RP

Améliorations *(Improvements [IM])*

Améliorez constamment vos processus de récupération après les incidents de cybersécurité en tirant les enseignements des incidents précédents.

Désignation	Tâche
RC.IM-1	Assurez-vous que les enseignements tirés des précédents incidents de cybersécurité sont intégrés à vos plans de récupération.
RC.IM-2	Actualisez vos stratégies de récupération.

Tableau 49 : Tâches RC.IM

Norme	Référence
COBIT 5	APO12.06, BAI05.07, DSS04.08, BAI07.08
ISA 62443-3:2013	
ISO 27001:2013	A.16.1.6, Clause 10
NIST-SP-800-53 Rev. 4	CP-2, IR-4, IR-8

Tableau 50 : Références RC.IM

Communication *(Communications [CO])*

Veillez à coordonner vos actions de récupération avec vos partenaires internes et externes (fournisseurs de services Internet, CERT, autorités, intégrateurs de systèmes, etc.).

Désignation	Tâche
RC.CO-1	Anticipez les réactions du public pour ne pas dégrader la réputation de votre entreprise.
RC.CO-2	Veillez à ce que votre entreprise retrouve vite une image positive après un incident de cybersécurité.
RC.CO-3	Communiquez à l'interne aux parties prenantes tout ce que vous avez entrepris en matière de récupération, sans oublier les cadres et la direction.

Tableau 51 : Tâches RC.CO

Norme	Référence
COBIT 5	EDM03.02, MEA03.02, APO12.06
ISA 62443-3:2013	
ISO 27001:2013	
NIST-SP-800-53 Rev. 4	CP-2, IR-4

Tableau 52 : Références RC.CO

Conclusion

La défense en profondeur privilégie l'approche proportionnelle aux risques : chaque entreprise ou organisme peut définir par lui-même sa sensibilité aux risques, les mesures à prendre pour réduire ces risques et leur ordre de priorité. La responsabilité de la cybersécurité reste ainsi l'apanage de l'entreprise ou l'organisme. Le présent manuel propose un outil d'évaluation, le *NIST Cybersecurity Framework Core,* qui permet aux acteurs des transports publics d'accroître la résilience de leurs processus informatisés. Il existe bien d'autres possibilités de valorisation (analyse comparative, échanges d'expériences au sein de la branche ou dans le cadre de la banque de données nationale, analyses d'écart, audits tiers, etc.). La mise en œuvre pratique et les échanges entre acteurs, associations et Confédération inciteront à expérimenter encore d'autres possibilités d'application.

Outre le présent manuel, l'AEP propose aux entreprises de transports publics un outil d'évaluation au format Excel, qui reprend les recommandations de la norme informatique pour les TIC[7]. Cet outil est particulièrement utile pour évaluer la cote de maturité d'une entreprise ou d'un organisme. Le présent manuel est un document d'accompagnement qui introduit le sujet tout en servant de référentiel en cas de question.

Le présent manuel n'est pas une directive, sa mission est de susciter la réflexion chez les acteurs des transports publics sous l'angle de la cybersécurité. La sécurité informatique n'étant pas un état en soi, mais un processus, ce manuel a pour mission d'encourager le processus de maturation et d'aider à sa réalisation.

[7] *À télécharger à l'adresse suivante : https://www.bwl.admin.ch/bwl/fr/home/themen/ikt/ikt_minimalstandard.html.*

Annexe

6.1 Recommandations visant à améliorer la sécurité de l'information

Le cadre et l'outil d'évaluation proposés dans le présent manuel sont d'une aide précieuse pour appréhender et améliorer la sécurité de l'information dans l'entreprise. La sécurité de l'information englobe tous les processus, méthodes et règles visant à garantir la confidentialité, l'authenticité et la disponibilité des informations, qu'elles soient analogiques ou numériques. La cybersécurité est l'un des aspects de la sécurité de l'information. Des chevauchements existent donc entre les deux domaines. À titre d'exemple, la cybersécurité comprend également la protection contre les accidents (collisions de trains), tandis que la sécurité de l'information s'applique aussi aux propos tenus par des collaborateurs à titre personnel.

Les organismes qui disposent de ressources suffisantes et de collaborateurs bien formés n'auront aucune difficulté à mettre en œuvre la présente recommandation. Il est du reste possible que certaines entreprises de transports publics aient déjà mis en place le cadre d'évaluation proposé dans le présent manuel, ou un autre :

Technique

Les solutions techniques augmentent la complexité et les coûts. Il vaut mieux s'appuyer sur les bonnes pratiques éprouvées et renoncer aux expérimentations coûteuses.

Exemples :

- deux centres de calcul, systèmes redondants ;
- chiffrage des appareils mobiles ;
- pare-feu, filtre web, protection contre les maliciels ;
- banc d'essai ;
- système de contrôle d'accès au réseau *(network access control system)* ;
- logiciel de gestion des appareils mobiles *(mobile device management software)* ;
- système électronique de contrôle d'accès.

Organisation

Des mesures organisationnelles sont mises en place lorsque des mesures techniques ne sont pas pertinentes ou s'avèrent trop complexes.

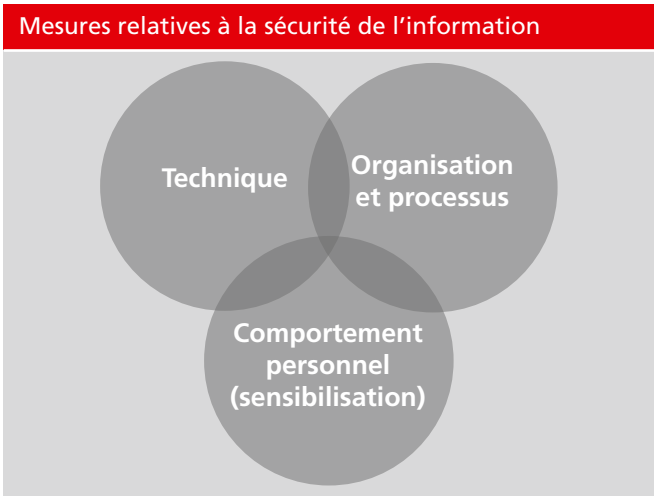


Figure 7 : Mesures relatives à la sécurité de l'information

Exemples :

- processus d'attribution des droits d'accès (principe des quatre yeux, double signature) ;
- prévention des cas d'urgence (scénarios, alerte, organisation, mesures d'urgence, décisions réservées, exploitation d'urgence, retour à l'exploitation normale, etc.) ;
- accord de maintien du secret avec les collaborateurs ;
- accord de confidentialité avec les partenaires externes ;
- classification des documents ;
- programme d'élimination des documents.

Comportement personnel

Chaque collaborateur peut identifier toute nouvelle méthode d'attaque et mettre en place les mécanismes de protection ad hoc. Mais le facteur humain constitue aussi l'une des principales menaces. La sensibilisation des collaborateurs au traitement responsable des données et l'appel à la responsabilité personnelle sont les vecteurs de motivation visant à améliorer la sécurité de l'information.

Exemples :

- ranger toujours l'ordinateur portable et la mallette dans un coffre ;
- utiliser des mots de passe complexes ;
- faire preuve de prudence dans le traitement des courriels de provenance inconnue ;
- détruire les documents confidentiels (en utilisant une déchiqueteuse de bureau, p. ex.) au lieu de les jeter simplement à la corbeille ;
- proscrire les discussions confidentielles par téléphone dans les lieux publics.

6.2 Principes, documents et normes

Le présent manuel tient compte de concepts, recommandations et mesures reposant sur diverses normes et autres documents normatifs (cf. tableau 52).

Titre	Année	Éditeur(s) et description
Mesures de protection des systèmes de contrôle industriels (SCADA)	2013	Éd. : **Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI** Basées sur des documents du Département américain de la sécurité intérieure (DHS), de l'Industrial *Control Systems Cyber Emergency Response Team* (ICS-CERT) et du National *Institute of Standards and Technology* (NIST), ces instructions décrivent en huit pages, de façon succincte et pragmatique, les onze mesures principales à mettre en œuvre par les exploitants de systèmes SCADA.
Analyse des risques et des vulnérabilités du sous-secteur	2015/ 2017	Éd. : **Office fédéral pour l'approvisionnement économique du pays (OFAE)** L'analyse des risques et des vulnérabilités repose sur la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) et sur la stratégie nationale pour la protection des infrastructures critiques (PIC). Elle a pour but d'examiner la vulnérabilité aux pannes ou perturbations informatiques.
Guide pour la protection des infrastructures critiques (Guide PIC)	2015	Éd. : **Office fédéral de la protection de la population (OFPP)** Le guide PIC constitue un instrument d'analyse et, le cas échéant, d'amélioration de la résilience des infrastructures critiques. Il est notamment conçu pour être utilisé dans des sous-secteurs critiques par les exploitants, les associations sectorielles et les autorités compétentes. Ce guide propose pour l'essentiel une procédure en matière de gestion des risques : analyse (identification des ressources, vulnérabilités, risques), évaluation, mesures (définition, mise en œuvre, contrôle et amélioration). Cette procédure peut tout à fait, voire devrait être intégrée aux processus de gestion existants ou être exécutée sur la base de ces derniers.
Stratégie nationale pour la protection des infrastructures critiques (PIC)	2012	Éd. : **Office fédéral de la protection de la population (OFPP)** La stratégie nationale PIC définit le champ d'application, désigne les infrastructures critiques et fixe les principes directeurs de la PIC. Elle s'adresse à tous les services assumant des responsabilités dans ce domaine, en particulier aux différentes autorités compétentes, aux responsables politiques et aux exploitants d'infrastructures critiques.
Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC)	2018	Éd. : **Unité de pilotage informatique de la Confédération (UPIC)** Vu l'intérêt majeur que revêt la protection des infrastructures informatiques contre les cyberrisques pour la Suisse, le Conseil fédéral a chargé l'UPIC d'élaborer une stratégie nationale visant à protéger notre pays contre de tels risques. La SNPC a pour but de dresser un panorama actuel des cyberrisques et de recenser les moyens dont dispose la Suisse pour y faire face, où se situent les lacunes et comment y remédier le plus efficacement possible. La SNPC identifie les structures existantes et définit des objectifs assortis de mesures ad hoc (analyses des risques et des vulnérabilités d'un sous-secteur, p. ex.).

Tableau 53 : Publications de la Confédération suisse, des services administratifs et des associations

Titre	Année	Éditeur(s) et description
Loi fédérale sur l'approvisionnement économique du pays (loi sur l'approvisionnement du pays, LAP)	2016	Éd. : **Assemblée fédérale de la Confédération helvétique** La LAP régit les mesures visant à garantir l'approvisionnement du pays en biens et services vitaux lors d'une pénurie grave à laquelle les milieux économiques ne peuvent pas faire face par leurs propres moyens. La Confédération peut encourager, dans les limites des crédits autorisés, des mesures prises par des entreprises de droit privé ou public pour garantir l'approvisionnement économique du pays si ces mesures contribuent à renforcer substantiellement les préparatifs nécessaires pour garantir les systèmes d'approvisionnement et infrastructures vitaux en cas de pénurie grave. Le présent manuel constitue l'une de ces mesures.

Tableau 53 : Publications de la Confédération suisse, des services administratifs et des associations

Le tableau ci-après répertorie les normes internationales prises en compte (du moins partiellement) dans le présent manuel.

Titre	Éditeur(s) et description
ISO 27001 **Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences** **ISO 27002** **Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour le management de la sécurité de l'information**	Éd. : **Organisation internationale de normalisation (ISO)** Cette norme détaille les exigences relatives à un système de gestion de la sécurité de l'information (SGSI). Les normes ISO 27000 ss. constituent une une série de normes concernant la sécurité de l'information, dont les suivantes présentent un intérêt ici : • 27000 Vue d'ensemble et vocabulaire ; • 27001 Exigences (principes de base avec contrôles et objectifs de contrôle en annexe) ; • 27002 Code de bonne pratique pour le management de la sécurité de l'information ; • 27003 Systèmes de management de la sécurité de l'information – Lignes directrices (pour la mise en œuvre) ; • 27005 Gestion des risques liés à la sécurité de l'information ; • 27019 Mesures de sécurité de l'information pour l'industrie des opérateurs de l'énergie. Largement appliquées à l'heure actuelle, les normes ISO 27000 ss. devraient s'imposer comme le principal cadre de référence dans les années à venir. Les observer aujourd'hui déjà constitue donc la bonne approche. Contrairement à d'autres normes ou cadres, elles ne sont pas trop détaillées, sont modulables et peuvent être continuellement améliorées et développées sur une longue période. Le SGSI et le contenu des mesures doivent être adaptés et mis en œuvre en tenant compte des spécificités du secteur.
ISO 22301 **Sécurité et résilience – Systèmes de management de la continuité d'activité – Exigences**	Éd. : **Organisation internationale de normalisation (ISO)** Cette norme détaille les exigences relatives aux systèmes de gestion de la continuité d'activité.
CEI 62443 ss. **Réseaux industriels de communication – Sécurité dans les réseaux et les systèmes**	Éd. : **Commission électrotechnique internationale (CEI)** Cette série compte treize normes de sécurité et spécifications techniques applicables aux systèmes d'automatisation de commande industriels *(industrial automation and control systems, IACS)*. Les normes CEI 61508 ss. (principes fondamentaux régissant la sécurité des IACS), qui englobent le thème de la sécurité de l'information, couvrent de manière complète et indépendante la thématique des IACS. Quatre aspects ou niveaux de sécurité de l'information différents sont retenus : • les aspects généraux (concepts, terminologie, unités de mesure, etc.) : CEI 62443-1-x ; • la gestion de la sécurité informatique : CEI 62443-2-x ; • le niveau « système » : CEI 62443-3-x ; • le niveau « composants » : CEI 62443-4-x. À relever que cette série de normes couvre également l'architecture de réseau et l'architecture zonale, alors que d'autres normes ne le font pas, ou alors de manière moins détaillée. Cette série de normes est en train de devenir une prescription normative fondamentale dans le contexte des normes du CENELEC (EN 50126, entre autres) en matière de fiabilité, de disponibilité, de maintenabilité et de sécurité (FDMS).

Tableau 54 : Normes nationales et internationales relatives à la sécurité informatique

Titre	Éditeur(s) et description
(pr)TS 50701 Applications ferroviaires – Cybersécurité	Éd. : **Comité européen de normalisation électrotechnique (CENELEC)** Cette spécification technique vise à certifier qu'un système ferroviaire qui l'applique est à la pointe sous l'angle de la cybersécurité, satisfait au niveau de sécurité souhaité et est en mesure de le garantir durant l'exploitation et la maintenance. Elle se fonde sur les normes CEI 62443 ss. et a été définie avec les objectifs suivants : • formuler des lignes directrices concernant la documentation relative à la cybersécurité, les résultats à fournir et les étapes du processus ; • pouvoir être adaptée aux différents cycles de vie des systèmes et les soutenir ; • s'appliquer aussi bien aux systèmes ferroviaires qui sont importants pour la sécurité qu'à ceux qui ne le sont pas (architecture de référence) ; • soutenir l'identification et la gestion aux points de chevauchement entre la cybersécurité et d'autres tâches du cycle de vie du système ; • être compatible et cohérente avec la norme EN 50126 notamment ; • opérer – mais aussi permettre – autant que possible une distinction entre homologation de sécurité *(safety)* et assurance de sécurité *(security)* ; • permettre, de manière harmonisée et standardisée, de fixer des exigences techniques en matière de sécurité de l'information ; • fixer des principes de construction afin de promouvoir des systèmes simples et modulaires ; • permettre l'utilisation de produits (solutions industrielles disponibles dans le commerce, p. ex.) selon la norme CEI 62443, au niveau « composants ».
CEI 62264 ss. Intégration des systèmes entreprise-contrôle	Éd. : **Commission électrotechnique internationale (CEI)** Cette série compte quatre normes relatives à l'intégration des systèmes informatiques d'entreprise et de contrôle-commande.
CEI 62351 ss. Gestion des systèmes de puissance et échanges d'informations associés – Sécurité des communications et des données	Éd. : **Commission électrotechnique internationale (CEI)** Les normes CEI 62351 ss. décrivent le standard de sécurité pour les systèmes de gestion énergétique et l'échange de données énergétiques. Elles définissent les mesures visant à satisfaire aux quatre exigences de base en matière de communication et de traitement sécurisés des données.
BDEW Livre blanc *Anforderungen an sichere Steuerungs- und Telekommunikationssysteme*	Éd. : ***Bundesverband der Energie- und Wasserwirtschaft (BDEW), Österreichs E-Wirtschaft*** Le livre blanc de la BDEW pointe les mesures de sécurité fondamentales touchant aux systèmes de commande et de télécommunication de l'industrie de l'énergie. L'objectif stratégique de ce document est d'influencer favorablement le développement de produits destinés aux systèmes susmentionnés, sous l'angle de la sécurité informatique, et de renforcer la compréhension de la branche eu égard aux enjeux de la protection de ces systèmes. Dans la région D-A-CH (Allemagne, Autriche, Suisse), le livre blanc de la BDEW est devenu un document de référence pour la passation de marchés dans le domaine du courant de traction. Il est complété par des recommandations d'exécution.

Tableau 54 : Normes nationales et internationales relatives à la sécurité informatique

Titre	Éditeur(s) et description
Guide to Industrial Control Systems (ICS) Security SP 800-82	Éd. : ***National Institute of Standards and Technology (NIST)*** Ce guide donne une vue générale des typologies et architectures SCADA, identifie les menaces et les vulnérabilités et énonce des recommandations concernant les contre-mesures et l'atténuation des risques. Il présente en outre des contrôles spécifiques SCADA fondés sur le cadre NIST 800-53.
Framework for Improving Critical Infrastructure Cybersecurity	Éd. : ***National Institute of Standards and Technology (NIST)*** Ce cadre donne suite à un décret présidentiel américain de 2013 intitulé « *Improving Critical Infrastructure Cybersecurity* » (améliorer la cybersécurité des infrastructures critiques). Il fait la synthèse de différentes lignes directrices visant à dresser l'état des lieux d'une entreprise dans le domaine de la cybersécurité et à définir une feuille de route pour améliorer les pratiques en la matière, en se référant à d'autres cadres et normes (ISO 27001, ISA 62443, NIST 800-53, COBIT, etc.).
Recommended Practice: Improving Industrial Control System Cybersecurity with Defense in Depth Strategies	Éd. : ***Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)*** du Département américain de la sécurité intérieure (DHS) Ce document constitue une introduction générale à la stratégie de défense en profondeur des systèmes de contrôle industriels.
IT-Grundschutz-Kompendium – Werkzeug für Informationssicherheit	Éd. : ***Bundesamt für Sicherheit in der Informationstechnik (BSI)*** Ce compendium est la publication de référence en matière de protection informatique de base *(IT-Grundschutz)*. Il constitue, avec les normes édictées par le BSI, une base solide pour appréhender la thématique de la sécurité de l'information. Le document détaille les différentes composantes de la protection informatique de base. Les menaces potentielles sont présentées dans une première partie, suivies des exigences fondamentales en matière de sécurité. Les composantes de la protection informatique de base sont réparties en dix sous-catégories thématiques allant des applications (APP) à la gestion de la sécurité (SGSI) en passant par l'informatique industrielle (IND). Différents niveaux de protection sont systématiquement examinés.
Normes BSI	Éd. : ***Bundesamt für Sicherheit in der Informationstechnik (BSI)*** Les normes BSI sont une composante clé de la méthodologie relative à la protection informatique de base. Elles comprennent des recommandations sur les méthodes, les processus et les procédures ainsi que sur les marches à suivre et les mesures touchant aux différents aspects de la sécurité de l'information. Quelques exemples de normes BSI : 200-1 (SGSI), 200-2 (marche à suivre concernant la protection informatique de base), 200-3 (analyse des risques fondée sur la protection informatique de base) et 100-4 (analyse détaillée de la gestion des situations d'urgence sous la forme d'un guide pratique).
BSI-Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz	La mise en place et le contrôle du dispositif de sécurité peuvent être réalisés selon les modalités de la protection informatique de base définies par le BSI, mais aussi selon les normes ISO 27000 ss. Ces deux approches sont compatibles. Toutes deux permettent de mettre en place et d'exploiter un SGSI, autrement dit d'identifier les risques en matière de sécurité de l'information et de les réduire à un niveau acceptable grâce à des mesures appropriées.
Zuordnungstabelle ISO zum modernisierten IT-Grundschutz	La norme BSI 200-2 relative à la protection informatique de base interprète les exigences et les mesures prévues par les normes ISO 27001 et 27002. Le tableau de correspondance aide les utilisateurs dans la transposition du contenu de ces deux normes ISO.

Tableau 54 : Normes nationales et internationales relatives à la sécurité informatique

Titre	Éditeur(s) et description
Industrielle Steuerungs- und Automatisierungssysteme (ICS) – Allgemeine Empfehlungen	Éd. : ***Bundesamt für Sicherheit in der Informationstechnik (BSI)*** Le compendium est un ouvrage de référence destiné à permettre d'appréhender facilement la sécurité informatique des systèmes SCADA. Il présente les principes généraux de l'automatisation et précise les spécificités et les normes pertinentes dans ce domaine. Il contient en outre un ensemble de mesures et une marche à suivre pour la mise en œuvre. Des outils techniques supplémentaires sont proposés aux utilisateurs sur le site internet du BSI.
Mapping of Dependencies to International Standards (tableau de correspondance)	Éd. : **Agence de l'Union européenne pour la cybersécurité (ENISA)** Ce rapport analyse les dépendances et les interactions entre les opérateurs de services essentiels *(operators of essential services, OES)* et les fournisseurs de services numériques *(digital service providers, DSP)*, et propose une série d'indicateurs en vue de leur évaluation. Ces indicateurs sont mis en regard de normes et conditions-cadre internationales (ISO/CEI 27002, COBIT 5, mesures de sécurité du groupe de coopération SRI et *NIST Cybersecurity Framework*).
Communication Network Dependencies for ICS/SCADA Systems	Éd. : **Agence de l'Union européenne pour la cybersécurité (ENISA)** Ce rapport se penche sur les réseaux de communication, sur l'intercommunication entre les SCI ou systèmes SCADA, sur l'identification des vulnérabilités, des risques et des menaces, et sur l'impact des systèmes cyberphysiques sur la sécurité. Il comprend également une série de recommandations sur l'atténuation *(mitigation)* des risques identifiés. L'étude préliminaire a permis d'établir une liste de pratiques et de lignes directrices éprouvées visant à limiter autant que possible la vulnérabilité des SCI ou systèmes SCADA. Ce document vise principalement à donner un aperçu des interdépendances des réseaux de communication (SCI ou systèmes SCADA), et à identifier les ressources critiques sous l'angle de la sécurité, ainsi que les scénarios d'attaque et les menaces concrètes contre ces réseaux de communication.
Paysage des menaces de l'ENISA (taxonomie)	Éd. : **Agence de l'Union européenne pour la cybersécurité (ENISA)** Ce document donne une vue d'ensemble des menaces et des tendances actuelles ou émergentes. Basé sur des données publiques, il offre une vision indépendante des menaces identifiées, de leurs auteurs et des tendances qui se dessinent. La taxonomie catégorise les menaces de façon systématique.
Branchenanforderungen an die IT-Sicherheit (VDV Schrift 400)	Éd. : ***Verband Deutscher Verkehrsunternehmen (VDV)*** Ce document décrit les exigences de sécurité informatique posées aux infrastructures critiques. Il suggère les approches possibles pour mettre en œuvre ces exigences (méthodes, processus et procédures). À travers ce document, la VDV met à la disposition de ses membres une norme de sécurité spécifique à la branche (B3S) et basée sur les travaux du BSI.

Tableau 54 : Normes nationales et internationales relatives à la sécurité informatique

6.3 Développement des normes

Le progrès technologique et les changements continus que connaît le secteur des transports publics imposent une évolution constante des normes. Voici quelques nouveautés connues au moment de finaliser le présent manuel :

- DE-OCF 2020 (art. 5c) : nouvelle exigence relative à la mise en place d'un système de gestion de la sécurité de l'information (SGSI). Il est recommandé de s'appuyer sur des normes ;
- directive européenne sur l'interopérabilité : il est prévu de traiter la thématique de la cybersécurité dans les nouvelles STI 2022 (étendue et contenu à définir) ;
- CENELEC prTS 50701 (cf. tableau 54) : la dernière révision de la norme est prévue à l'été 2020.

6.4 Glossaire

Terme ou abréviation	Signification
AC	*Identity Management, Authentification and Access Control*
AE	*Anomalies and Events*
AEP	Approvisionnement économique du pays
AM	*Asset Management*
AN	*Analysis*
AT	*Awareness and Training*
ATP	Protection automatique des trains *(Automatic Train Protection)*
BCM	Gestion de la continuité d'activité *(Business Continuity Management)*
BE	*Business Environment*
BIA	Bilan d'impact sur l'activité *(Business Impact Analysis)*
BLS	BLS SA (anciennement *Bern-Lötschberg-Simplon-Bahn*)
BSI	*Bundesamt für Sicherheit in der Informationstechnik* (Allemagne)
BTA	Installation technique *(Betriebstechnische Anlage)*
CAPRE	*Capacity and Reservations :* système de gestion des places (successeur de PLABE)
CCTV	Vidéo en circuit fermé *(Closed-Circuit Television)*
CENELEC	Comité européen de normalisation électrotechnique
CFF	Chemins de fer fédéraux suisses
CM	*Security Continous Monitoring*
CO	Communications
COAT	*CCS onboard application platform for trackside related functions*
contrôle-commande	Système servant au pilotage des réseaux, stations, chemins de fer ou centrales électriques

Tableau 55 : Glossaire

Terme ou abréviation	Signification
DAS	Système d'aide à la conduite *(Driver Assistance System)*
DE	*Detect*
DE-OCF	Dispositions d'exécution de l'ordonnance sur les chemins de fer
DMS	Système de gestion documentaire *(Document Management System)*
DMZ	Zone démilitarisée *(Demilitarised Zone) :* réseau informatique avec accès sécurisé (souvent utilisé pour garantir une séparation logique entre deux zones de réseau)
DP	*Detection Processes*
DS	*Data Security*
EMS	Système de mesure de l'énergie *(Energy Metering System)*
ENISA	Agence de l'Union européenne pour la cybersécurité
ERP	Planification des ressources d'entreprise *(Enterprise Resource Planning)*
ET	Entreprise de transport
ETC	Entreprise de transport concessionnaire
ETCS	*European Train Control System :* système de contrôle de la marche des trains
ETF	Entreprise de transport ferroviaire
FTP	*File Transfer Protocol :* protocole de transfert de fichiers
GI	Gestionnaire de l'infrastructure ferroviaire
GSM	*Global System for Mobile Communications :* système mondial de communications avec les mobiles
GSM-R	*Global System for Mobile Communications – Rail(way) :* système GSM du rail
GV	*Governance*
HVAC	Chauffage, ventilation et air conditionné *(Heating, Ventilation and Air Conditioning)*
IaaS	Infrastructure sous forme de service *(Infrastructure as a Service)*
IAM	Gestion des identités et des accès *(Identity and Access Management)*
ID	*Identify*
IDS	Système de détection d'intrusion *(Intrusion Detection System)*
IM	*Improvements*
IMS	Système de gestion intégré *(Integrated Management System)*
IP	*Information Protection Processes and Procedures*
IP	*Internet Protocol :* protocole de l'internet
ISA	Accord de sécurité d'interconnexion *(Interconnection Security Agreement)*
ISA	*International Society of Automation*
ISO	Organisation internationale de normalisation
JRU	*Juridical Recording Unit*
KPI	Indicateur de performance clé *(Key Performance Indicator)*

Tableau 55 : Glossaire

Terme ou abréviation	Signification
LAN	Réseau local *(Local Area Network)*
LCdF	Loi fédérale sur les chemins de fer
LTV	Loi sur le transport de voyageurs
MA	*Maintenance*
MCG	Passerelle de communication mobile *(Mobile Communication Gateway)*
MELANI	Centrale d'enregistrement et d'analyse pour la sûreté de l'information (rattachée à l'Unité de pilotage informatique de la Confédération)
MI	*Mitigation*
MoA	Mémorandum d'accord *(Memorandum of Agreement)*
MoU	Mémorandum d'entente *(Memorandum of Understanding)*
NAC	Contrôle d'accès au réseau *(Network Access Control)*
NeTS	*Network-wide Track Management System :* système de sillons pour le réseau entier
NIST	*National Institute of Standards and Technology* (États-Unis)
NIST CSF	*National Institute of Standards and Technology Cybersecurity Framework*
NMC	Centre de gestion du réseau *(Network Management Centre)*
OBM	Gestion à livre ouvert *(Open-Book Management)*
OBU	Unité embarquée *(On-Board Unit)*
OC	Contrôleur d'objet *(Object Controller)*
OFAE	Office fédéral pour l'approvisionnement économique du pays
OFPP	Office fédéral de la protection de la population
OFT	Office fédéral des transports
OTV	Ordonnance sur le transport de voyageurs
PaaS	Plateforme sous forme de service *(Platform as a Service)*
PIS	Système d'information aux passagers *(Passenger Information System)*
PR	*Protect*
PT	*Protective Technology*
RA	*Risk Assessment*
RailOpt	Logiciel de planification (entre planification des infrastructures et planification opérationnelle)
RailSys	Logiciel de planification
RC	*Recover*
RCS	*Rail Control System*
ReSys	Système de réservation de places
RhB	*Rhätische Bahn AG*

Tableau 55 : Glossaire

Terme ou abréviation	Signification
RM	*Risk Management Strategy*
ROE	Règles d'engagement *(Rules of Engagement)*
RP	*Recovery Planning*
RP	*Response Planning*
RS	*Respond*
SaaS	Logiciel sous forme de service *(Software as a Service)*
SC	*Supply Chain Riskmanagement*
SCADA	Commande de surveillance et acquisition de données *(Supervisory Control and Data Acquisition)* ; utilisé dans le présent manuel comme synonyme des abréviations « SCI » et « TO »
SCI	Système de contrôle industriel ; utilisé dans le présent manuel comme synonyme des abréviations « TO » et « SCADA »
SFTP	*Secure File Transfer Protocol* : protocole de transfert de fichiers sécurisé
SGSI	Système de gestion de la sécurité de l'information
SIEM	Gestion des informations et des événements de sécurité *(Security Information and Event Management)*
SIG	Système d'information géographique
SLA	Accord de niveau de service *(Service Level Agreement)*
SNPC	Stratégie nationale de protection de la Suisse contre les cyberrisques
SOB	*Schweizerische Südostbahn AG*
SOC	Centre d'opérations de sécurité *(Security Operation Centre)*
SOPRE	Logiciel de planification d'engagement du personnel et du matériel roulant
SRI	Sécurité des réseaux et de l'information
SSH	*Secure Shell*
STI	Spécifications techniques d'interopérabilité
TCMS	Système de contrôle et de gestion des trains *(Train Control and Management System)*
TI	Technologies de l'information, plus particulièrement la bureautique ; tout ce qui ne relève pas de la TO
TIC	Technologies de l'information et de la communication
tl	Transports publics de la région lausannoise
TMS	Système de gestion du trafic *(Traffic Management System)*
TO	Technologie opérationnelle ; utilisée dans le présent manuel comme synonyme des abréviations « SCADA » et « SCI »
TPF	Transports publics fribourgeois Holding (TPF) SA

Tableau 55 : Glossaire

Terme ou abréviation	Signification
UCC	Collaboration et communications unifiées *(Unified Communications and Collaboration)*
UPIC	Unité de pilotage informatique de la Confédération
UTP	Union des transports publics
VBZ	*Verkehrsbetriebe Zürich*
VoIP	Voix par IP *(Voice over Internet Protocol)*
WAN	Réseau longue distance *(Wide Area Network)*
WLAN	Réseau local sans fil *(Wireless Local Area Network)*

Tableau 55 : Glossaire

6.5 Liste des figures

6.6 Liste des tableaux

Auteurs et experts ayant contribué à la première édition

Prénom, nom	Organisation	Fonction
Hans-Peter Käser	OFAE	Auteur principal/ direction du projet
Daniel Caduff	OFAE	Coauteur
Nathalie Gratzer	OFAE	Coauteure
Marcus Griesser	AEP, CFF	Chef de projet UTP, coauteur, expert
Patrick Favre	OFT	Expert, assurance qualité
Tobias Hubschmid	OFT	Expert, assurance qualité
Ulrich Schär	OFT	Expert, assurance qualité
Andreas Klopfenstein	BLS	Expert, assurance qualité
Daniel Noger	BLS	Expert, assurance qualité
Martin Wyss	BLS	Expert, assurance qualité
Stephan Berger	BLS	Expert, assurance qualité
Urs Hoerler	RhB	Expert, assurance qualité
Jean-Luc Nottaris	CFF	Expert, assurance qualité
Stefan Käser	CFF	Expert, assurance qualité
Olaf Zanger	CFF	Expert ,assurance qualité
Peter Häberli	SOB	Expert, assurance qualité
Roland Kressbach	SOB	Expert, assurance qualité
Giorgio Anastopoulos	tl	Expert, assurance qualité
Marc Striffeler	TPF	Expert, assurance qualité
Marcel Gahler	VBZ	Expert, assurance qualité

Chronologie

Date	Étape de travail
Août 2019	Début des travaux du groupe de travail sur la sécurité informatique des infrastructures critiques
Septembre 2019 à juin 2020	Rédaction de la première ébauche du manuel
Juin 2020	Validation par le groupe de travail
Juin à juillet 2020	Consultation de l'UTP (commission Infrastructure)
Août 2020	Validation par l'UTP

Exclusion de responsabilité

Le présent document, qui contient des recommandations visant à améliorer la sécurité des systèmes d'information et communication ainsi que des systèmes de commande des transports publics, a été rédigé de bonne foi par les parties prenantes.

L'Office fédéral pour l'approvisionnement économique du pays, ainsi que les experts, entreprises et collaborateurs ayant contribué au présent document, ne fournit aucune garantie explicite ou implicite concernant celui-ci. L'exploitation sûre des TIC incombe au seul utilisateur, qui assume également la responsabilité d'éventuels dommages.

Impressum et contact

Éditeur
Office fédéral pour l'approvisionnement économique du pays OFAE
Bernastrasse 28, CH-3003 Bern
info@bwl.admin.ch, www.bwl.admin.ch
Téléphone +41 58 462 21 71

Association consulté
Union des transports publics UTP


Jeremias Gotthelf