Manuel Protection de base pour les «technologies opérationnelles» (OT) dans l'approvisionnement en électricité

OT_SCTY, édition juillet 2018

Verband Schweizerischer Elektrizitätsunternehmen
Association des entreprises électriques suisses
Associazione delle aziende elettriche svizzere

Telefon +41 62 825 25 25, Fax +41 62 825 25 26, info@strom.ch, www.strom.ch

Impressum et contact

Éditeur
Association des entreprises électriques suisses AES
Hintere Bahnhofstrasse 10, case postale
CH-5001 Aarau
Téléphone +41 62 825 25 25
Fax +41 62 825 25 26
info@electricite.ch
www.electricite.ch

Auteurs de la première édition

Reto Amsler	Swissgrid SA	Auteur
Mattia Bardelli	AET	Auteur
Reto Bondolfi	EWZ	Auteur
Daniel Caduff	OFAE	Auteur
Beate Fiedler	Alpiq SA	Auteure
Olivier Hauert	Alpiq SA	Auteur
Hendrik la Roi	AES	Secrétaire
Stefan Mattmann	Forces Motrices de la Suisse centrale SA (CKW)	Auteur
Michele Paganini	Repower AG	Auteur
Markus Rauber	BKW Energie SA	Auteur
Daniel Rudin	MELANI	Auteur
Daniel Schirato	Axpo WZ-Systems AG	Responsable de projet
Wolfgang Sutter	KWO	Auteur
Peter Waldegger	Axpo Power AG	Responsable de projet

Responsabilité commission
La Commission EAE-TSO de l'AES est désignée responsable de la tenue à jour et de l'actualisation du document.

Chronologie

Septembre 2016	Début des travaux du groupe de travail ICT Security pour les infrastructures critiques
Décembre 2017	Finalisation du document
Mars/avril 2018	Consultation au sein de la branche
11 juin 2018	Approbation par la Direction de l'AES

Ce document a été élaboré avec l'implication et le soutien de l'AES et de représentants de la branche.

Imprimé n° 1047 / f, édition 2018

Sommaire

Liste des figures

Liste des tableaux

Avant-propos

Le présent document est un document de la branche publié par l'AES. Il fait partie d'une large réglementation relative à l'approvisionnement en électricité sur le marché ouvert de l'électricité. Les documents de la branche contiennent des directives et des recommandations reconnues à l'échelle de la branche concernant l'exploitation des marchés de l'électricité et l'organisation du négoce de l'énergie, répondant ainsi à la prescription donnée aux entreprises d'approvisionnement en électricité (EAE) par la loi sur l'approvisionnement en électricité (LApEl) et par l'ordonnance sur l'approvisionnement en électricité (OApEl).

Les documents de la branche sont élaborés par des spécialistes de la branche selon le principe de subsidiarité; ils sont régulièrement mis à jour et complétés. Les dispositions qui ont valeur de directives au sens de l'OApEl sont des normes d'autorégulation. En principe, les documents de la branche font foi pour toutes les personnes impliquées ayant déclaré que lesdits documents faisaient partie intégrante d'un contrat donné.

Les documents sont répartis en quatre catégories hiérarchisées:

- Document principal: Modèle de marché pour l'énergie électrique (MMEE)
- Documents clés
- Documents d'application
- Outils / Manuels

Le présent document «Protection de base pour les «technologies opérationnelles» (OT) dans l'approvisionnement en électricité» est un Outil / manuel.

Structure des documents

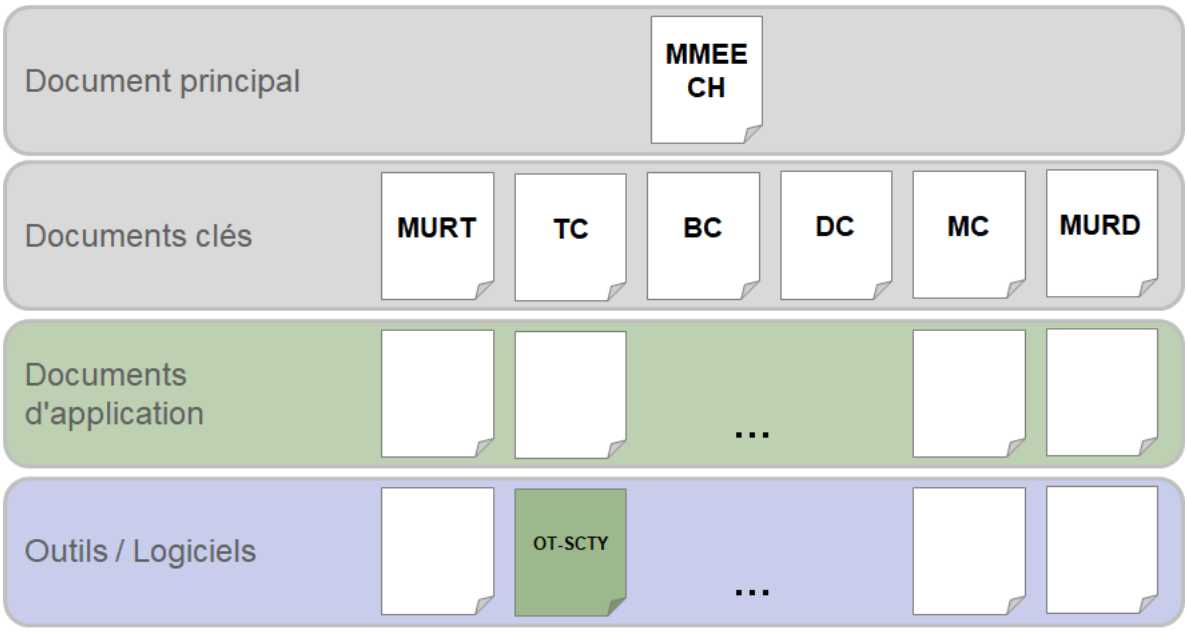

Figure 1 Structure des documents

Clause de non-responsabilité

Le présent document, qui contient des recommandations sur la manière d'améliorer la sécurité des systèmes de commande industriels grâce à la stratégie de défense en profondeur, a été établi en toute bonne foi par les personnes et services impliqués. Toutes les informations sont fournies sous toutes réserves quant à leur intégralité et à leur exactitude. Ni l'AES, ni les services fédéraux impliqués n'assument la responsabilité pour les éventuels dommages qui résulteraient de l'utilisation d'informations issues de ce document ou du manque d'informations.

Synthèse

L'automatisation s'est depuis longtemps répandue dans les environnements commerciaux et industriels, sans lien entre les uns et les autres. Ces dernières années toutefois, la normalisation (p. ex. les appareils X86) et la mise en réseau (p. ex. Internet), déjà caractéristiques de l'informatique de gestion, se sont de plus en plus propagées au sein de l'informatique industrielle également. Les systèmes industriels sont de ce fait eux aussi exposés aux mêmes «cybermenaces» que celles que connaît depuis longtemps l'informatique de gestion.

Les systèmes de contrôle-commande industriels (ICS) font aujourd'hui partie intégrante des infrastructures critiques telles que l'électricité, le pétrole et le gaz, l'eau, les transports, la production et l'industrie chimique, dont ils facilitent le fonctionnement. La question de plus en plus prégnante de la cybersécurité et de ses conséquences sur les ICS fait apparaître des risques fondamentaux pour l'infrastructure critique d'une nation. Une gestion efficace des problématiques liées à la cybersécurité des ICS nécessite une compréhension claire des enjeux de sécurité actuels ainsi que des contre-mesures défensives spécifiques.

Le présent document s'adresse aux gestionnaires de réseau de distribution des niveaux de réseau 1 à 4 ainsi qu'aux installations de production d'énergie (producteurs). Il préconise une recommandation permettant de réduire à un niveau acceptable les cybermenaces pesant sur l'infrastructure critique que constitue l'approvisionnement en électricité. Cette recommandation porte essentiellement sur la mise en œuvre d'une stratégie dite «de défense en profondeur» («defense in depth»), aujourd'hui considérée comme la stratégie défensive reconnue contre les cybermenaces. Celle-ci se fonde sur le principe militaire selon lequel il est plus difficile pour un ennemi de vaincre un système de défense complexe et hétérogène qu'une seule et unique barrière. La stratégie repose sur des technologies de l'information et de la communication (TIC) devant être employées par les personnes dans le cadre de processus efficaces et efficients. Ce manuel renvoie par ailleurs à différents instruments, et propose notamment un cadre assorti d'un outil Excel, qui permet aux entreprises de recenser, d'évaluer et de comparer leurs capacités propres et de continuer à les développer de façon ciblée.

Le présent manuel s'adresse aux personnes assumant la responsabilité globale de la sécurité informatique et/ou de la sécurité des systèmes de contrôle-commande de processus et de réseaux dans le secteur de l'approvisionnement en énergie. Il peut s'agir de Chief Information Officers (CIO), de Chief Information Security Officers (CISO), de Security Managers, de responsables de projet ou de conseillers en sécurité des TIC assumant également des fonctions de direction. Mais les experts et les spécialistes de la cybersécurité pourront également trouver dans ce document des informations utiles concernant la mise en œuvre des normes et des directives sur la sécurité des TIC dans la branche. Sont également concernés les Chief Operating Officers (COO) des petites entreprises d'approvisionnement en énergie et toutes les personnes chargées de la responsabilité globale de l'exploitation dans ce secteur, laquelle s'effectue de plus en plus par le biais de moyens informatiques.

La présente première version fournit le bagage nécessaire pour garantir une protection de base concrète des technologies opérationnelles de l'approvisionnement en électricité. Il revient à chaque gestionnaire de réseau des niveaux de réseau 1 à 4 ou aux exploitants des installations de production d'énergie de déterminer le degré de mise en œuvre. Dans un second temps, les expériences acquises devront permettre d'établir une norme minimale dans le cadre d'une version remaniée.

La première section propose une introduction détaillée à la stratégie de défense en profondeur, abordant plus spécifiquement les problèmes posés par les TIC et les technologies OT dans la branche de l'énergie et

de l’électricité. Ceux qui ne sont pas encore familiarisés avec la cybersécurité ou qui souhaitent réactualiser leurs connaissances en la matière y trouveront de précieuses informations. Il est également possible de consulter cette section pour vérifier certains points.

La seconde section présente des mesures et des outils concrets dont la mise en œuvre est recommandée. En nous appuyant sur le *Framework for Improving Critical Infrastructure Cybersecurity* («Cadre pour l’amélioration de la cybersécurité des infrastructures critiques») américain, également disponible en allemand dans la norme minimale visant à renforcer la résilience des TIC de l’Office fédéral pour l’approvisionnement économique du pays, nous recommandons un outil concret que les entreprises d’approvisionnement en énergie et en électricité pourront utiliser et qui devrait correspondre au plus petit dénominateur commun de la cyberdéfense active.

Les bases légales en lien avec la confidentialité des données ne sont explicitement pas traitées dans cette recommandation.

Contexte et vue d’ensemble

(1) Au cours des 15 dernières années, les technologies de l’énergie ont connu une évolution fortement marquée par les systèmes informatiques et TIC. Cette mutation technologique permet de piloter et de réguler des informations en temps réel de manière centralisée. La gestion de l’exploitation du réseau a ainsi nettement gagné en agilité, et la réaction aux événements critiques qui viennent de survenir s’avère beaucoup plus rapide et automatisée. Ce changement au profit des technologies de l’information s’accompagne cependant de nouveaux risques que les entreprises énergétiques doivent identifier, évaluer et traiter afin de pouvoir remplir leur mandat légal, conformément à la loi sur l’approvisionnement en électricité, à l’ordonnance sur l’approvisionnement en électricité ou à la loi sur l’énergie.

(2) L’Office fédéral pour l’approvisionnement économique du pays OFAE a réalisé une analyse des risques et des vulnérabilités du secteur partiel de l’approvisionnement électrique, et établi les constats suivants:

- Sur l’ensemble de la chaîne d’approvisionnement, la production d’électricité dans les centrales et les sous-stations est aujourd’hui moins vulnérable aux menaces liées aux TIC que l’exploitation des réseaux de distribution et de transport.
- Il demeure possible en théorie de manœuvrer les centrales électriques et les sous-stations sur place. En cas de défaillance de grande ampleur, il serait toutefois extrêmement difficile pour les entreprises d’approvisionnement en énergie de dépêcher suffisamment de personnel aussi vite qu’il le faudrait sur tous les sites critiques.
- Dans le cas où la menace affecterait le prestataire TIC des entreprises d’approvisionnement en énergie, la communication entre les installations et les postes de conduite ne pourrait plus être maintenue que par le biais de systèmes d’urgence.
- L’exploitation des réseaux de distribution s’effectue aujourd’hui de manière décentralisée; la surveillance est en grande partie assurée par des systèmes numériques, qui prennent également en charge une partie du contrôle-commande. L’exploitation des réseaux est par conséquent beaucoup plus vulnérable aux menaces des TIC que la production d’électricité en elle-même. Dans ce domaine, les systèmes SCADA jouent un rôle de premier plan.
- Le risque induit par les erreurs de manipulation commises, volontairement ou non, par des collaborateurs sur les systèmes SCADA est donc également significatif, et continue d’augmenter du fait du processus de centralisation des postes de conduite.
- Sous l’effet de l’intégration de «smart meters» et d’appareils «smart grid», le réseau électrique suisse se transforme en un agrégat de multiples petits ordinateurs, ce qui présente des avantages en termes d’efficacité pour l’exploitation des réseaux de distribution, mais génère également de nouvelles vulnérabilités en matière de TIC.
- La vulnérabilité globale de l’approvisionnement électrique en termes de TIC va continuer de croître.

(3) À l’exception des installations nucléaires, qui aujourd’hui déjà sont soumises à un large éventail de dispositions régulatoires émanant de l’Inspection fédérale de la sécurité nucléaire IFSN, il n’existe pas à l’heure actuelle d’exigences minimales (juridiquement) contraignantes en matière de sécurité des TIC dans le domaine de l’approvisionnement en électricité.

(4) La nouvelle loi sur l'approvisionnement du pays, entrée en vigueur le 1er juin 2017, confère cependant également à l'OFAE la compétence pour mettre en œuvre, à titre subsidiaire, des mesures préventives visant à garantir l'approvisionnement en énergie.

(5) La norme minimale en matière de TIC figurant dans le présent document correspond à une mesure préventive de ce type au sens de la loi sur l'approvisionnement du pays. Conformément au principe de subsidiarité, cette norme a été rédigée en tant que document de la branche.

1. Situation initiale et objectifs

(1) Le présent manuel adopte l'approche d'une stratégie de défense en profondeur, laquelle traite la totalité des risques relevant de la sécurité des TIC. L'objectif est de mettre à la disposition des responsables TIC des EAE suisses, à travers ce document, un outil qui leur permette d'évaluer, d'apprécier et d'améliorer la sécurité informatique dans leurs entreprises, ce qui devrait améliorer la résilience des EAE helvétiques face aux risques liés aux TIC, et ainsi accroître la sécurité d'approvisionnement dans son ensemble.

(2) La première partie décrit en détail la stratégie de défense en profondeur et propose des mesures concrètes dont la mise en œuvre est recommandée, accompagnées d'exemples issus de la pratique. La seconde partie présente le *Framework for Improving Critical Infrastructure Cybersecurity* du NIST américain, que nous conseillons aux entreprises d'utiliser comme outil pour réaliser une auto-évaluation de leur maturité propre en termes de résilience vis-à-vis des cybermenaces. Il leur est en outre recommandé de s'appuyer sur cette auto-évaluation pour continuer de développer en permanence leurs capacités et leurs compétences propres.

(3) Les «risques liés aux TIC» s'entendent de manière globale. Le présent document traite des risques de toute nature afférents aux TIC, de la protection contre l'accès physique à la protection contre les cyberattaques à visée destructrice, en passant par la protection contre la perte ou la manipulation de données. Il vise cependant plus particulièrement les risques identifiés lors de l'analyse des vulnérabilités menée dans le cadre de la stratégie nationale de protection de la Suisse contre les cyberrisques.

1.1 Objectifs et principes

(1) La présent manuel a pour ambition de proposer un guide permettant de mettre en place, d'appliquer et de mener une stratégie de défense en profondeur en matière de sécurité. La méthode de défense en profondeur garantit une approche holistique, dont l'objectif est de permettre l'identification et le traitement de tous les risques de sécurité dans le domaine des systèmes critiques d'information et de communication. Cela inclut des mesures techniques, mais également les processus et formations des collaborateurs nécessaires, ainsi que la gouvernance de la sécurité requise pour pouvoir mettre en œuvre et déployer cette stratégie avec succès.

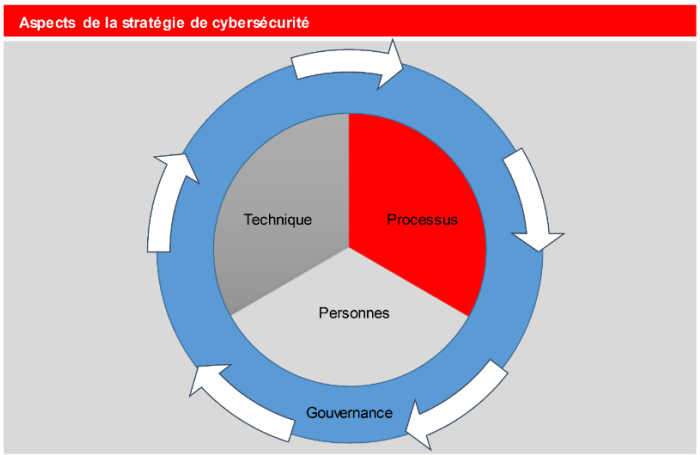

Figure 2 Aspects de la stratégie de cybersécurité

(2) La défense en profondeur a pour objectif de garantir une sécurité de l'information adaptée aux besoins pour les systèmes énergétiques critiques. Elle se concentre notamment sur la mise à disposition correcte, sûre et en temps utile de toutes les informations nécessaires au cercle de personnes autorisées pour exploiter un réseau en toute sécurité. Les concepts de sécurité courants, p. ex. le concept de défense en profondeur, reposent sur les critères suivants:

- Disponibilité
  Garantir que les systèmes d'information, les informations qu'ils contiennent et les ressources nécessaires à leur acheminement sont disponibles au moment requis.
- Intégrité
  Faire en sorte que les informations soient à tout moment complètes, exactes et fiables et qu'elles ne puissent pas être modifiées ni détruites sans autorisation.
- Confidentialité
  Garantir que les informations sont accessibles uniquement aux personnes ou aux systèmes autorisés.

1.2 Délimitations

(1) Le présent manuel se concentre uniquement sur les processus opérationnels exerçant une influence directe sur la régulation et le pilotage sûrs des réseaux énergétiques. Elle ne prend pas en compte d'autres aspects de la sécurité dans le domaine de l'énergie, comme par exemple les smart meters ou les smart grids. La portée de ce manuel est précisée par les définitions et les délimitations ci-dessous:

- La sécurité des TIC pour les infrastructures critiques englobe tous les actifs TIC nécessaires à une exploitation sûre et intègre du réseau.
- La sécurité de la bureautique et de l'informatique de gestion n'est pas abordée dans ce document. Des exigences sont néanmoins posées aux interfaces et à l'échange d'informations avec les zones contenant les actifs TIC critiques.
- La sécurité électrique et opérationnelle des moyens d'exploitation du réseau haute tension n'est pas traitée dans le présent manuel.
- Le présent manuel ne comporte pas de mesures visant à assurer la sécurité au travail. Dans ce domaine, on appliquera les dispositions de l'ordonnance sur le courant fort.
- Cette recommandation s'adresse principalement aux entreprises d'approvisionnement en énergie des niveaux de réseau 1 à 4.
- Une protection de base doit être mise en place à l'échelle de la branche en vue d'assurer un niveau de sécurité accru. Le niveau visé doit garantir qu'en cas d'incident de sécurité, il demeure possible à tout moment de fournir en temps utile une quantité d'énergie de 50 MWh[1] ou plus.
- Les niveaux de réseau 5 à 7 sont concernés dans la mesure où il faut veiller à ce qu'ils ne causent aucune perturbation aux niveaux de réseau supérieurs. Il convient donc de prendre notamment en compte les systèmes de contrôle-commande interconnectés.

[1] Voir Recommandation de la branche ICT-Continuity, paragraphe 4.2 pour la définition d'un événement pertinent (crise).

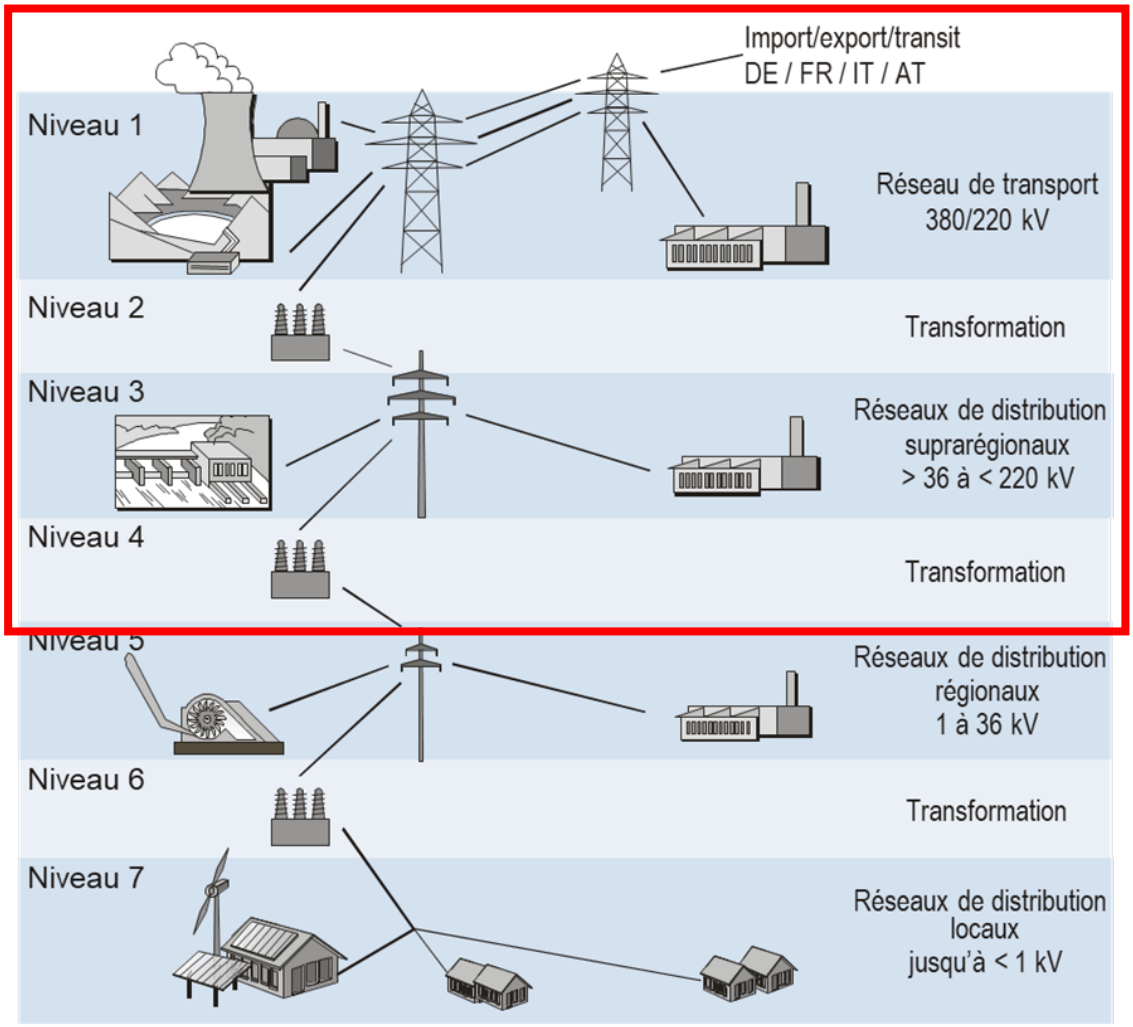

Figure 3 Principales cibles du manuel: les niveaux de réseau 1 à 4

1.3 Introduction à la stratégie de défense en profondeur

(1) Le concept de «défense en profondeur» est issu de la philosophie de nombreuses cultures et stratégies militaires en matière de défense: «Pour bloquer un assaillant, mets en place le plus de lignes de défense possible».

(2) Les aspects ayant trait à la sécurité des données, de l'information et de l'exploitation sont pris en compte de manière exhaustive et approfondie. Voilà des années que ce concept constitue un standard de facto des TIC commerciales. Adapté à la commande de processus, il peut également être appliqué dans un environnement industriel.

(3) La sécurité des TIC dans l'économie industrielle, c'est-à-dire celle des technologies IT opérationnelles (OT) ou de processus (PI), se différencie toutefois quelque peu, à certains égards, de la sécurité des TIC commerciales:

(4) Toute stratégie de sécurité d'une organisation doit protéger les valeurs déterminantes pour la réussite de cette dernière. Ces valeurs diffèrent selon l'entreprise et la branche industrielle. Dans le secteur

commercial, la sécurité des TIC porte principalement sur la confidentialité; dans le secteur industriel, elle est davantage axée sur la protection de la vie, de l'intégrité corporelle et de l'environnement, et donc sur la disponibilité adéquate des TIC.

(5) La défense en profondeur, c'est-à-dire la juxtaposition de lignes défensives, inclut également la surveillance, la détection et la réaction à des événements particuliers. Il n'est pas possible d'éviter les cyberattaques – c'est pourquoi l'objectif consiste à les identifier rapidement, à les isoler, à les contrer et à réduire les conséquences de l'atteinte (résilience).

(6) La défense en profondeur est un concept; les différentes technologies et applications logicielles sont importantes et constituent un moyen d'atteindre le but fixé. Une «approche globale en profondeur» regroupe toutes les ressources et leurs interactions fournissant des lignes défensives efficaces à des fins de protection, de surveillance et de réaction aux cybermenaces.

(7) Un concept de défense en profondeur doit aborder les grands thèmes ci-dessous:

Figure 4 Planification de la défense en profondeur

(8) En matière de mise en application des concepts de défense en profondeur, il existe des disparités importantes entre l'environnement informatique traditionnel et un ICS. Les principales différences sont récapitulées dans le tableau ci-dessous.

Aspect sécuritaire	Business IT (IT)	Operational Technology/technologies opérationnelles (OT)
Données/informations critiques	Données commerciales (y compris financières) Données personnelles	Données du système de contrôle-commande (signaux de contrôle) Données provenant de capteurs (données «smart meter»)
Intégrité	Critique selon le contexte	Critique (conséquences possibles sur la vie, sur l'intégrité corporelle et sur l'environnement)
Disponibilité	Généralement pendant les heures de bureau	Élevée, en temps réel (365 jours par an, 24 heures sur 24)
Confidentialité	Élevée pour les données financières et personnelles	Peu critique
Durée de vie de la technologie	2 à 3 ans; nombreux fournisseurs; compléments permanents	10 à 20 ans; habituellement, même fournisseur au fil du temps; la fin de vie du produit suscite de nouvelles préoccupations sécuritaires.
Gestion du changement	Régulière et planifiée; coordonnée avec les durées d'utilisation minimales	Planification stratégique; processus à caractère exceptionnel en raison de l'impact sur la production
Gestion des correctifs	Facile à définir; à l'échelle de l'entreprise; à distance et automatisée	Longue période avant l'installation effective des correctifs; spécifique à l'OEM; peut entraver le fonctionnement de l'ICS; les responsabilités doivent être clairement définies pour atteindre un niveau de risque acceptable.
Antivirus	Largement répandus; faciles à mettre en place et à actualiser. Les utilisateurs ont le contrôle sur les adaptations et peuvent être définis pour chaque application ou chaque entreprise.	Les besoins en ressources peuvent impacter l'ICS; cela nécessite en général un répertoire «Exclusions» afin que les programme sans intervention des logiciels à virus (en quarantaine) ne soient pas détériorés.
Procédure de test et d'audit	Emploi de méthodes modernes; systèmes généralement élastiques et robustes vis-à-vis des méthodes d'évaluation	Tests spécifiquement adaptés au système; les méthodes modernes peuvent s'avérer inappropriées; l'appareil peut être sujet à des perturbations pendant les tests.
Classification des installations	Usuelle et réalisée tous les ans; dépenses induites par les résultats	Réalisée uniquement si elle est obligatoire; peu de stocks pour les installations sortant de l'ordinaire; pas de lien entre la valeur des installations et les contre-mesures
Réaction aux incidents et investigation	Faciles à développer et à mettre en œuvre; quelques exigences régulatoires; intégrées à la technologie	Centrées sur les activités visant la restauration du système; procédure d'investigation non mature, au-delà de la reconstitution des événements; nécessite de bonnes relations entre les technologies de l'information (TI) et l'ICS.

Aspect sécuritaire	Business IT (IT)	Operational Technology/technologies opérationnelles (OT)
Sécurité physique et environnementale	De médiocre (systèmes de bureau) à excellente (systèmes informatiques critiques)	Généralement excellente pour les zones critiques; maturité variable en fonction de la criticité/de la culture
Développement sûr du système	Partie intégrante du processus de développement	Historiquement, ne fait pas partie intégrante du processus de développement; les fournisseurs évoluent, mais plus lentement que les TI; solutions ICS clés difficiles à compléter ultérieurement avec des dispositifs de sécurité
Régulation	Différemment marquée selon le secteur et le pays (p. ex. finance et industrie pharmaceutique)	Croissante, selon le pays (forte régulation p. ex.: NERC aux États-Unis, EnWG en Allemagne)

Tableau 1 Différences entre les concepts de défense en profondeur pour l'informatique de gestion et un système ICS

(9) Les stratégies de défense en profondeur appliquées aux systèmes de contrôle-commande dépendent également d'autres réalités commerciales telles que:

- les coûts de sécurisation des anciens systèmes;
- la tendance croissante à connecter les systèmes de contrôle-commande aux réseaux d'entreprise;
- la capacité à permettre à des utilisateurs distants d'accéder aux actifs opérationnels et ICS;
- les problèmes de confiance sur la chaîne d'approvisionnement;
- l'état de la technique quant à la capacité à surveiller et à sécuriser les protocoles spécifiques aux ICS;
- et l'aptitude à se tenir au courant des nouvelles menaces pesant sur les ICS.

(10) La défense en profondeur n'est pas un objet tangible ni une suite logicielle; c'est une combinaison de personnes, de technologies, de processus et de connaissances au sujet de possibles agresseurs. La réflexion et l'action permettent de résoudre les problèmes, et la technologie rend possible cette résolution en fournissant tout un panel d'outils pouvant réduire les risques. La meilleure technologie n'empêchera jamais l'être humain de commettre des erreurs, volontaires ou non. Les organisations doivent en permanence adapter et affiner leurs contre-mesures de sécurité pour se protéger contre les menaces nouvelles ou déjà connues.

(11) La mise en place de lignes défensives multiples dans les environnements ICS renforce la sécurité via l'augmentation des «coûts» d'une attaque, tout en améliorant la probabilité de détecter un cyberpirate et la capacité à se défendre contre lui. Les contre-mesures de sécurité fondées sur des procédures et des normes éprouvées protègent les ressources critiques pour les ICS en superposant plusieurs couches de défenses, et améliorent ainsi la protection de l'exploitation, du personnel et de la technologie.

(12) L'objectif final consiste à bloquer les mouvements latéraux d'un cyberpirate à travers les réseaux et les systèmes et à le contraindre à investir et à dépenser davantage. L'utilisation de plusieurs niveaux permet d'atténuer les attaques directes contre les systèmes critiques et de compliquer les activités

d’identification sur les réseaux et les systèmes ICS, tout en fournissant des zones tout indiquées pour l’introduction de technologies de détection des intrusions.

(13) Comme exposé dans le tableau 2, la présente section traite de certaines des solutions et stratégies disponibles et recommandées pour la sécurité par la défense en profondeur. Il est recommandé aux entreprises de mettre en œuvre ces solutions et ces stratégies en combinaison afin de créer des lignes défensives garantissant la fonctionnalité originelle de leur ICS tout en offrant une protection solide à leurs actifs critiques.

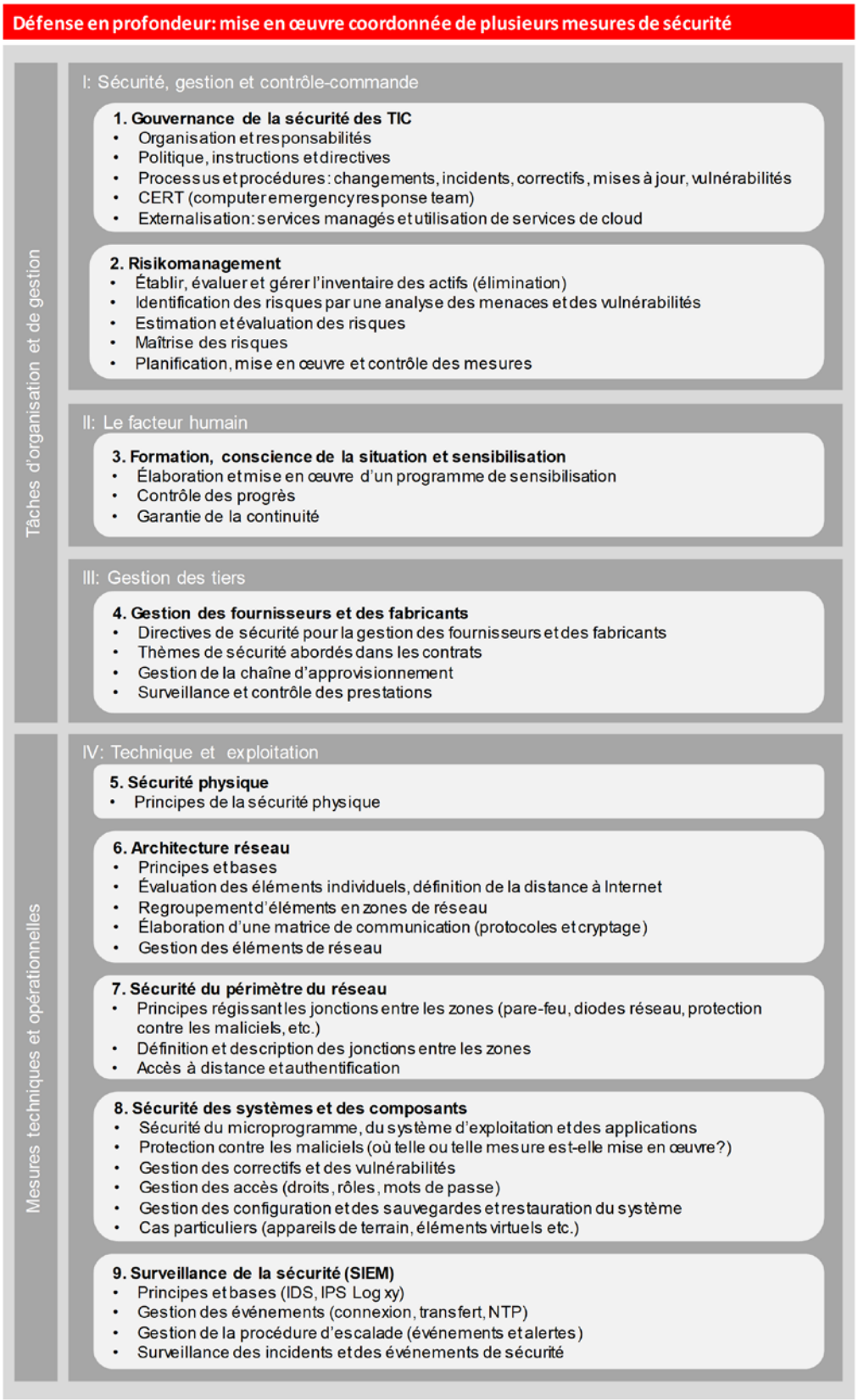

Figure 5 Mise en œuvre coordonnée de plusieurs mesures de sécurité

2. Stratégies de défense en profondeur pour les ICS

(1) Une stratégie de cybersécurité efficace protège les moyens nécessaires à une organisation pour exécuter ses processus d'affaires critiques. Il n'existe pas dans ce domaine de définition des exigences valable dans l'absolu ni de solution applicable de manière générale. La cybersécurité s'entend au contraire comme un processus permanent exigeant une approche en plusieurs strates, appelée «stratégie de défense en profondeur» dans la littérature spécialisée.

(2) Les stratégies de défense en profondeur sont toujours individuelles et doivent s'adapter aux besoins, aux possibilités et aux risques des organisations concernées. L'approche se fonde systématiquement sur les risques et prend en compte les moyens critiques de l'organisation, mais également ses interdépendances et ses dépendances vis-à-vis de processus ou de ressources externes.

(3) Une stratégie de défense en profondeur accepte qu'il ne puisse pas exister de protection complète contre tous les types de cybermenaces. Chacun est au contraire conscient de sa propre vulnérabilité et développe des stratégies et des mesures dans le but d'identifier sa propre exposition aux cyberrisques (IDENTIFY), de s'en protéger de manière optimale (PROTECT), de détecter les atteintes en matière de cybersécurité (DETECT), d'y réagir (RESPOND) et de revenir au plus vite à la normale (RECOVER).

(4) La mise en place d'une stratégie de défense en profondeur pour les systèmes de contrôle-commande industriels (ICS)[2] nécessite, de la part de l'organisation, une connaissance de la totalité des (possibles) vulnérabilités et menaces pesant sur les données, processus et installations qui, ensemble, constitue l'ICS.

2.1 Gouvernance de la sécurité des TIC

(1) La gouvernance de la sécurité jette les bases d'une mise en œuvre réussie et durable de la stratégie de défense en profondeur. Elle crée notamment les conditions permettant d'identifier, d'évaluer et de traiter les menaces pesant sur la commande des processus. La gouvernance offre une structure de niveau supérieur visant à soutenir les objectifs d'affaires en matière de sécurité des TIC sur les plans stratégique, fonctionnel et opérationnel. Le modèle de gouvernance décrit:

- les actions entreprises;
- la façon dont elles sont entreprises;
- qui en porte la responsabilité;
- comment les mesures doivent être effectuées.

(2) La gouvernance définit les règles, les processus, les métriques et les structures organisationnelles nécessaires à une planification et à un pilotage efficaces afin de satisfaire aux exigences métier et d'atteindre les objectifs d'affaires de l'entreprise. Ceux-ci doivent être consignés dans un document stratégique, validés par la direction et communiqués au sein de l'entreprise. Un membre de la direction doit par ailleurs être désigné pour assumer la responsabilité de la sécurité de l'information et

[2] Différents concepts signifiant tous plus ou moins la même chose sont employés dans les milieux spécialisés: ICS (industrial control system, système de contrôle-commande industriel), SCADA (supervisory control and data acquisition, système d'acquisition et de contrôle de données), ou OT (operational technology, technologies opérationnelles).

assurer le soutien managérial requis dans l'élaboration et la mise en œuvre de la stratégie de défense en profondeur. La direction doit être régulièrement informée par l'instance chargée de la sécurité de la maturité, des incidents et des indicateurs clés de performance (key performance indicators, KPI) définis en matière de sécurité.

(3) À cet égard, il est capital de disposer d'un soutien inconditionnel de la part des plus hauts responsables, ainsi que de discuter des moyens, des processus et des ressources nécessaires à une mise en œuvre réussie.

2.2 Instance et responsabilités

(1) L'un des principaux aspects de la gouvernance de la sécurité est une instance en charge de la sécurité établie au sein de l'entreprise et à laquelle sont attribuées des tâches, des responsabilités et des compétences claires. Cette instance est chargée de définir la stratégie de défense en profondeur, de la mettre en œuvre et de la perfectionner. La gestion active des risques revêt dans ce contexte une importance centrale pour identifier les éventuelles menaces pesant sur la sécurité des TIC et pouvoir y faire face à l'aide de mesures. L'instance chargée de la sécurité doit être habilitée par la direction et disposer des ressources nécessaires pour pouvoir exécuter ses tâches de manière efficace et complète. Il est important pour ce faire qu'elle soit solidement ancrée et acceptée dans l'entreprise. Les rôles et les fonctions au sein de l'instance chargée de la sécurité doivent être décrits, indiqués et associés à des compétences claires. Des interfaces avec les autres instances (pertinentes en termes de sécurité) de l'entreprise doivent être définies et consignées, et les éventuels chevauchements de compétences doivent être clarifiés.

(2) Si l'instance chargée de la sécurité a été habilitée par la direction, elle peut mettre en œuvre ses missions clés sans restriction, en collaboration étroite avec les autres secteurs de l'entreprise. Parmi celles-ci figurent notamment les points suivants:

- assurer la direction technique en matière de sécurité de l'information dans le domaine des technologies opérationnelles et fixer les priorités des activités de manière adaptée à la situation;
- veiller à ce que tous les documents de sécurité, instructions et directives nécessaires soient rédigés, si nécessaire actualisés et appliqués de façon systématique;
- faire en sorte que les nouveaux aspects importants pour la sécurité soient identifiés, analysés et, le cas échéant, traités;
- garantir la disponibilité du savoir-faire et des ressources correspondants pour l'ensemble de la gestion de la sécurité;
- veiller à la réalisation de contrôles, d'audits et de tests d'intrusion périodiques;
- faire en sorte que les rapports destinés à la direction soient rédigés de manière correcte quant au contenu, dans le respect des délais et des échelons hiérarchiques et de manière systématique;
- veiller à ce que le processus de sécurité soit intégré méthodiquement et en imbrication avec le processus de gestion des risques de l'entreprise et à ce que les exigences issues de ce dernier soient prises en compte.

2.2.1 Instructions et directives

(1) Dans le domaine de la sécurité de l'information, comme dans d'autres domaines, l'entreprise doit adopter une orientation stratégique. Où veut-elle se situer en la matière d'ici 3 à 5 ans? Dans quelle

mesure est-elle disposée à prendre des risques dans ce domaine? Quelles ressources et quels moyens financiers faut-il investir dans la sécurité de l'information?

(2) Les réponses à ces questions stratégiques doivent être abordées et fournies par une politique de sécurité à l'échelle de l'entreprise. Cette politique doit être établie et mise en vigueur par la direction. La politique de sécurité doit définir les aspects stratégiques ci-dessous, qui constituent ainsi des points d'ancrage pour toutes les activités et exigences relevant de la sécurité de l'information:

- Objectif et champ d'application de la politique de sécurité
- Objectifs de sécurité
- Principes de sécurité
- Propension à prendre des risques
- Coopération avec la branche et les autorités
- Mise en œuvre des normes de sécurité
- Prise en compte de la rentabilité
- Culture de la sécurité
- Dérogations aux directives de sécurité
- Sécurité dans le cadre de projets
- Instance chargée de la sécurité et rôles et fonctions en son sein

(3) Outre la politique de sécurité, dans laquelle entre la sécurité de l'information, l'entreprise doit également se doter, selon sa taille et sa structure, d'autres documents ayant valeur de directive. La figure ci-dessous propose un exemple de hiérarchie des documents liés à la sécurité de l'information dans une entreprise.

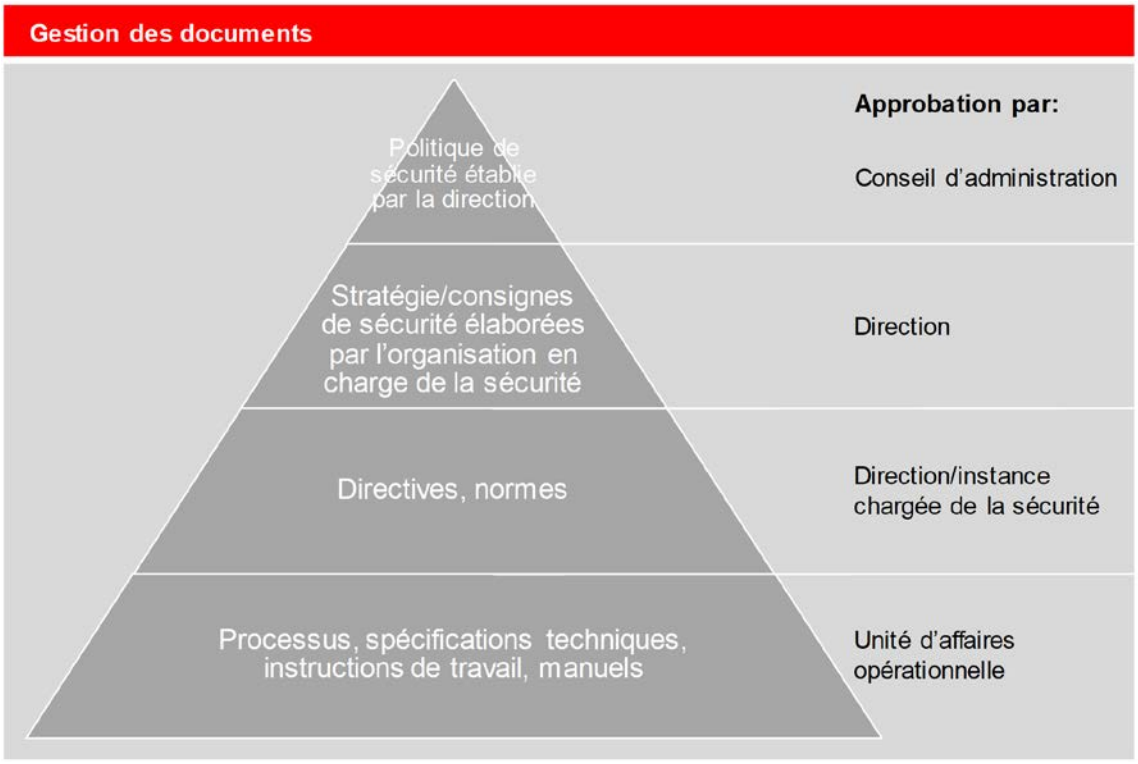

Figure 6 Hiérarchie des documents

(4) Il est important de créer un ensemble de règles à l'échelle de l'entreprise, qui spécifie la façon dont les instructions et les directives doivent être mises en place (propriétaire, validation, diffusion et formation, contrôle régulier de l'actualité des informations) et lesquelles doivent également s'appliquer aux partenaires et aux prestataires externes ou être définies spécifiquement pour ces derniers.

2.2.2 Processus et procédures – gestion du changement

(1) Une organisation se compose de personnes, de processus et de technologies. Elle se différencie des autres par la façon dont elle développe et organise ces trois éléments. Chaque entreprise se définit par son personnel, par les connaissances de celui-ci, par ses tâches, ses fonctions et ses rôles et par ses outils techniques. Chaque organisation IT s'insère également dans un cadre constitué de processus IT, que ceux-ci soient consignés par écrit ou simplement mis en pratique. Les procédures et processus définis ont pour but la transparence et le contrôle et, au final, la réalisation des objectifs. Dans l'idéal, les directives, procédures et processus administratifs sont appliqués pour les tâches et activités pertinentes et utiles pour la réalisation des objectifs.

(2) Un cadre de processus IT sert à mettre en œuvre le plan stratégique en matière d'IT, et doit en conséquence être défini, appliqué et périodiquement adapté. Ce cadre comprend habituellement une cartographie des processus IT indiquant lesquels sont liés les uns aux autres. Certains processus disposent de procédures et de responsabilités définies; les niveaux de maturité souhaités peuvent être mesurés et contribuer à l'amélioration continue. La cartographie des processus IT devrait s'intégrer à la celle des processus de l'entreprise et définir les spécificités des processus IT lorsque ceux-ci diffèrent des processus d'affaires. Globalement, un tel cadre de processus IT sert à normaliser les procédures et doit contribuer à améliorer l'efficacité et l'efficience. ITIL (Information Technology Infrastructure Library, bibliothèque pour l'infrastructure des technologies de l'information) et COBIT (Control Objectives for Information and Related Technology, objectifs de contrôle de l'information et des technologies associées) sont deux exemples de référentiels standard connus pour les processus IT. La gestion du changement y constitue un processus central et joue ici un rôle d'illustration.

Gestion du changement

(3) La gestion du changement revêt une importance décisive pour préserver l'intégrité des systèmes de contrôle-commande de processus. Les logiciels «non patchés» constituent l'une des failles majeures d'un système. Les mises à jour logicielles des systèmes IT, et en particulier les correctifs de sécurité, sont généralement appliqués en temps utile sur la base des directives et des procédures de sécurité appropriées. Ces procédures sont en outre souvent automatisées à l'aide d'outils sur serveur. Les mises à jour logicielles des systèmes ICS ne peuvent pas toujours être déployées en temps voulu. Elles doivent auparavant faire l'objet de tests approfondis et être validées pour l'installation par le fournisseur de l'application de contrôle-commande industrielle et par l'utilisateur final de cette dernière. L'exploitant de l'ICS doit par ailleurs planifier les travaux de maintenance nécessaire des journées, voire des semaines à l'avance. Difficulté supplémentaire, de nombreux ICS font appel à des versions anciennes des systèmes d'exploitation qui ne sont plus prises en charge par l'éditeur, ce qui empêche la prise en compte des correctifs disponibles. La gestion du changement peut également concerner le matériel et les microprogrammes. Appliquée aux ICS, elle nécessite une évaluation minutieuse de la part des fabricants et des exploitants, ainsi qu'une étroite collaboration entre les spécialistes système, réseau et sécurité des deux parties. Les éléments suivants figurent habituellement parmi les caractéristiques obligatoires d'un processus de gestion du changement:

- processus de changement défini, dans l'idéal accompagné d'une documentation écrite permettant de contrôler les modifications de façon répétée sur tous les sites;
- séparation technique et organisationnelle entre le développement, les tests et la production; interface et responsabilités définies entre la production/le développement et l'exploitation;
- définition d'une procédure de validation: répartition des tâches, principe du double contrôle, ségrégation; détermination de critères et de responsables; passerelle de validation;
- traçabilité et reproductibilité: consignation par écrit du changement et documentation de la base de données de configuration, enregistrement, journalisation (logging);
- responsabilités, critères et possibilités de revenir en arrière en cas d'erreur (annulation, procédure de secours);
- acceptation finale par l'utilisateur final (essai d'acceptation par l'utilisateur, EAU).

2.2.3 Gestion des incidents – CERT (computer emergency response team)

(1) Le secteur de l'énergie recourt de plus en plus à des composants informatiques. Ce constat s'applique à l'ensemble de l'organisation, des activités administratives aux éléments de couplage d'une sous-station, en passant par les modèles de calcul du flux d'électricité. Si la mise en réseau ne s'est pas encore entièrement imposée partout, elle deviendra tôt ou tard incontournable. Aujourd'hui, les commutations dans les sous-stations ne sont déjà plus effectuées au niveau local, mais de manière centralisée, depuis un centre de contrôle qui peut en outre assurer à distance la surveillance complète d'une sous-station et lire les valeurs mesurées des flux d'électricité en temps réel.

(2) La production locale d'électricité grâce à des installations photovoltaïques et éoliennes débouche également sur une mise en réseau de plus en plus importante. La possibilité pour chaque exploitant d'une installation ad hoc d'être ainsi raccordé au réseau d'un producteur d'électricité crée un réseau énergétique d'une extrême complexité à l'échelle du pays, les producteurs étant eux aussi reliés les uns aux autres par des processus opérationnels et des interfaces.

(3) L'intégration rapide des technologies informatiques évoluant à une cadence effrénée entraîne la collision de deux univers. De nombreux composants ayant été conçus dans l'optique d'une durée de vie maximale, certains éléments SCADA ont été réalisés à une époque où les fabricants ne se préoccupaient pas encore de cybersécurité. De même, la formation de la plupart des personnels qualifiés ne les sensibilisait pas non plus aux risques actuels. Ces deux facteurs sont à l'origine des difficultés que pose l'intégration de concepts de sécurité et de technologies toujours plus innovants dans un environnement plus ou moins statique.

SOC/CERT

(4) Une approche très prometteuse pour améliorer la sécurité opérationnelle consiste à mettre en place et à faire fonctionner un SOC ou un CERT. Il appartient à l'entreprise de déterminer si elle doit mettre sur pied un tel service, et lequel (SOC ou CERT). Il convient également de se demander si l'entreprise est en mesure de gérer elle-même ces fonctions, ou si elle souhaite les confier à un prestataire externe dans le cadre d'un service managé.

(5) Un CERT ou un CSIRT s'occupe généralement, comme son nom l'indique, «uniquement» des urgences informatiques («computer emergency») ou de la réaction aux incidents de sécurité informatique («computer security incident responses»). Un SOC (security operation center), quant à lui, désigne un centre opérationnel chargé de l'exploitation de l'infrastructure (serveurs, data centers, réseaux), mais également des processus de sécurité et de réaction aux incidents. Son organisation

et sa structure sont fortement inspirées de celles de centres opérationnels similaires, comme p. ex. le centres d'opérations du réseau, aussi appelé centre d'exploitation du réseau («network operation center»). Au fil des années s'est développé un large éventail de types de structures et de gestion pour les centres opérationnels IT, de salles rappelant les salles de contrôle de mission de la NASA aux simples îlots de tables dans un service IT. Les entreprises peuvent soit gérer elles-mêmes leur SOC, soit, de plus en plus, en externaliser la gestion à un MSSP (managed security services provider, fournisseur de services de sécurité managés).

(6) Le but d'un SOC consiste à garantir la sécurité des informations d'une organisation et à s'adapter aux défis fluctuants que posent les menaces nouvelles. Sa présence permet de répondre en partie aux exigences légales et de conformité. Pour cela, le SOC dispose de personnels spécialisés, ainsi que de processus et d'outils établis en conséquence.

(7) Les prestations fournies par un SOC peuvent différer d'un centre à l'autre. Elles doivent en effet être adaptées au cœur de métier, à l'infrastructure et aux processus de l'organisation concernée pour pouvoir garantir la sécurité de ses informations.

Surveillance de la sécurité

(8) Les analystes surveillent en continu les événements relevant de la cybersécurité. Ces derniers sont générés grâce à des **outils** de surveillance comme p. ex. un SIEM, un IDS ou d'autres outils similaires. Les incidents signalés sont en outre surveillés par le biais d'e-mails ou de systèmes de tickets. Les alertes générées sont traitées par des analystes qui mettent alors en œuvre des procédures de gestion des incidents.

Gestion de la sécurité

(9) Les prestations fournies par le SOC font l'objet d'une surveillance concernant leur efficacité et sont perfectionnées en permanence. Les nouvelles prestations du SOC pour d'autres secteurs de l'entreprise sont mises en œuvre par la gestion des services de sécurité.

Ingénierie des services de sécurité

(10) Il s'agit de services de conseil et d'assistance en ingénierie destinés à des outils et des projets relevant de la sécurité des informations. Ils incluent également la mise en place et le perfectionnement d'outils et de plateformes nécessaires au SOC lui-même.

Opérations de sécurité

(11) À la différence de l'ingénierie, les opérations de sécurité sont principalement axées sur l'exploitation stable des plateformes et des outils de sécurité. Les modifications de configuration des systèmes sont effectuées dans le cadre de cette prestation.

Enquête et réaction aux incidents de sécurité

(12) Les événements et les incidents de sécurité sont traités conformément aux procédures établies. Cette prestation est généralement étroitement couplée à la surveillance de la sécurité. Les événements sont analysés et des mesures adaptées sont prises. Cette prestation comprend également le processus de transfert en escalade et d'autres formes d'assistance pour résoudre l'événement. Les activités réalisés dans ce cadre sont souvent aussi qualifiées de «gestion des incidents» dans l'environnement ITIL.

Gestion des journaux de sécurité

(13) Autre aspect étroitement lié à la surveillance de la sécurité, la gestion des journaux de sécurité vise à collecter les données pertinentes de ces journaux, à les normaliser, à les analyser et à les sauvegarder. La collecte porte sur les données de journalisation des systèmes réseau, hôtes et de sécurité ainsi que sur celles des différentes applications. Cette prestation comporte également l'évaluation et l'intégration de nouvelles sources de journaux. Elle est généralement fournie à l'aide d'outils d'analyse automatiques.

Détection des vulnérabilités

(14) Cette prestation vise principalement à identifier les vulnérabilités (points faibles). Elle se distingue de la gestion des vulnérabilités, qui relève généralement d'un processus extérieur au SOC et comprend également la suppression des vulnérabilités repérées. Ces dernières peuvent correspondre à de mauvaises configurations de systèmes, à des failles matérielles ou logicielles, ou encore à des failles de processus.

Analyse des menaces et des vulnérabilités

(15) Des données sont collectées à partir de différentes sources internes ou externes en vue d'établir une vue d'ensemble de la situation actuelle en matière de menaces. Il est possible d'extraire automatiquement les données depuis les sources, mais leur analyse et l'évaluation de leur pertinence doivent être effectuées manuellement.

Analyses et rapports de sécurité

(16) Les informations collectées dans le cadre des différentes prestations fournies sont regroupées et organisées, p. ex. sous forme de rapports permettant leur visualisation. Les informations ainsi obtenues peuvent ensuite être réutilisées dans le cadre des services, afin d'améliorer la qualité et l'efficacité de ces derniers.

Détection des intrusions

(17) Cette prestation pouvant être réalisée par le biais d'une investigation numérique, d'une détection des anomalies et d'analyses rétrospectives consiste à examiner les signes indiquant des atteintes à la sécurité actuelles ou passées. Étroitement associée à la prestation d'enquête et de réaction aux incidents de sécurité, elle se concentre principalement sur l'analyse approfondie des systèmes IT en vue d'identifier les éventuels systèmes compromis et d'en évaluer les conséquences.

(18) Outre les services décrits plus haut, un SOC englobe également les processus ITIL classiques suivants:

- Gestion des événements
- Gestion des incidents
- Gestion des problèmes

(19) Un SOC s'occupe principalement des opérations et de la réaction aux incidents dans un cadre plus restreint, tandis qu'un CERT (computer emergency response team) se situe à un niveau supérieur de l'organisation. Pour accroître la sécurité, on analyse la sécurité des ordinateurs et du réseau. Parmi les prestations fournies figurent la publication d'avertissements et de messages d'alerte, la mise en réseau d'organisations, des analyses approfondies, ainsi que la réaction aux incidents. Les CERT proposent fréquemment leurs services non seulement à leur entreprise propre, mais également à un cercle de clients présentant des conditions et intérêts communs (p. ex. dans la branche de l'énergie).

Il est clair que le secteur énergétique a besoin d'une organisation centrale capable de mettre à disposition des connaissances techniques approfondies et d'apporter son aide dans la coordination et la résolution des incidents.

(20) Les prestations fournies par un CERT peuvent grosso modo être réparties dans les catégories suivantes:

- Services proactifs
- Services réactifs
- Services de gestion de la qualité de la sécurité

(21) Les catégories mentionnées ci-dessus sont décrites ici:

Services proactifs

(22) Ces services visent à atténuer et à prévenir les incidents de cybersécurité. Cet objectif peut être atteint et relevé grâce à une amélioration permanente des infrastructures et de la collaboration.

Services réactifs

(23) Ces services visent à apporter une assistance après la survenue d'incidents de cybersécurité. Variables selon le client, ils peuvent être fournis sur mandat d'un client ou s'inscrire dans le cadre des responsabilités confiées au CERT.

Services de gestion de la qualité de la sécurité

(24) Outre les prestations techniques directement liées aux incidents, des services visant à accroître la sécurité générale d'une organisation peuvent également être fournis.

Services réactifs	Services proactifs	Services de gestion de la qualité de la sécurité
Alertes et avertissements Gestion des incidents - Analyse des incidents - Réaction aux incidents sur site - Aide à la réaction aux incidents - Coordination de la réaction aux incidents Gestion des vulnérabilités - Analyse des vulnérabilités - Réaction aux vulnérabilités Coordination de la réaction aux vulnérabilités	Annonces Veille technologique Audits ou évaluations de sécurité Configuration et maintenance des outils, applications et infrastructures de sécurité Développement d'outils de sécurité Services de détection des intrusions Diffusion d'informations liées à la sécurité	Analyse des risques Planification de la continuité des activités et de la reprise après sinistre Conseil en sécurité Sensibilisation Formation initiale/continue Évaluation ou certification de produits

Tableau 2 Les services que peut proposer un CERT

Alertes et avertissements

(25) Diffusion d'informations sur les attaques, les intrusions, les failles de sécurité, les alertes anti-intrusion, les virus informatiques ou encore les fausses alertes, ainsi que d'indications concernant les mesures d'atténuation pouvant être mises rapidement en œuvre. Les alertes et les avertissements sont communiqués en réaction à un incident.

Analyse des incidents

(26) L'analyse des incidents peut porter sur différents niveaux et différentes sous-prestations. Elle consiste essentiellement à analyser toutes les informations disponibles au sujet d'un incident. L'objectif est de restreindre la portée de celui-ci, d'évaluer les dommages provoqués et d'identifier les stratégies potentielles permettant de le contrer. L'analyse consiste également à mettre en corrélation différentes informations, comme p. ex. les tendances, les signatures et les activités.

Réaction aux incidents sur site

(27) Ce service consiste à apporter une aide pour résoudre les incidents sur site. Les systèmes et infrastructures concernés sont analysés directement par l'équipe elle-même, qui prend également directement les mesures correctrices et de sécurisation.

Aide à la réaction aux incidents

(28) Au lieu de résoudre directement les incidents sur place, l'équipe propose simplement une assistance à la résolution de ces derniers, le plus souvent à distance. Contrairement à la «réaction aux incidents sur site», il n'y a pas d'interaction directe avec les systèmes concernés.

Coordination de la réaction aux incidents

(29) Lors d'incidents concernant plusieurs organisations, le CERT assure la coordination des mesures. Il peut s'agir ici de collaboration avec les victimes d'une attaque, ou encore de coopération avec les autorités de poursuite pénale ou d'autres administrations. Parmi les autres tâches incluses dans ce service figurent la collecte de statistiques, la transmission des informations aux organisations potentiellement impliquées, l'échange de renseignements et la réalisation d'analyses.

Analyse des vulnérabilités

(30) Ce service consistant à réaliser des analyses techniques et à rechercher les failles matérielles et logicielles inclut également la confirmation des points faibles éventuels et l'analyse des possibilités offertes par ces derniers.

Réaction aux vulnérabilités

(31) Analyse des possibles mesures d'atténuation correspondant aux points faibles identifiés et communication de ces mesures aux partenaires et aux clients.

Coordination de la réaction aux vulnérabilités

(32) Le CERT informe les partenaires et les clients des points faibles, des risques associés et des mesures d'atténuation, et peut vérifier les mesures prises. Parmi les activités incluses dans ce service figurent la communication avec les fabricants, les clients, les partenaires, mais également les spécialistes des domaines respectifs, ainsi que la rédaction de rapports et la coordination de la publication des correctifs.

Annonces

(33) Les annonces englobent les alertes, les avertissements relatifs aux points faibles, les conseils, etc. Elles informent également des conséquences à moyen et à long terme des nouvelles vulnérabilités ou menaces.

Veille technologique

(34) Le CERT surveille les nouvelles évolutions de la technologie, la cartographie actuelle des menaces ainsi que les tendances. Les thèmes abordés peuvent également porter sur des aspects juridiques ou politiques. Ces activités s'effectuent par le biais d'une surveillance des listes de diffusion, des sites Internet, des articles et de la presse. Elles peuvent déboucher sur des annonces, des directives ou des recommandations.

Audits ou évaluations de sécurité

(35) Les audits et les évaluations permettent de vérifier si l'infrastructure du client satisfait aux normes ou aux exigences. Ils peuvent comporter une analyse des processus en plus de celle des systèmes techniques.

Configuration et maintenance des outils, applications et infrastructures de sécurité

(36) Ce service consiste à apporter une aide à la configuration et à l'exploitation d'outils, d'applications et d'infrastructures de sécurité. Il peut s'agir, outre d'une assistance, de l'exploitation directe des infrastructures.

Développement d'outils de sécurité

(37) Le CERT développe pour ses clients des outils de sécurité spécifiques répondant aux exigences et aux besoins particuliers d'un client ou d'un groupe de clients. Il peut également s'agir de l'extension d'outils existants.

Services de détection des intrusions

(38) Le CERT analyse les messages IDS et prend les mesures correspondantes. Celles-ci, définies en concertation avec le client, peuvent consister à lui signaler un incident ou à interagir directement avec les systèmes.

Diffusion d'informations liées à la sécurité

(39) Un ensemble d'informations utiles et aisément compréhensibles est fourni au client:

- Règles d'établissement des rapports et informations de contact pour le CSIRT
- Archives des alertes, avertissements et autres annonces
- Documentation sur les bonnes pratiques actuelles
- Directives générales concernant la sécurité informatique
- Politiques, procédures et listes de contrôle
- Informations relatives au développement et à la diffusion des correctifs
- Liens vers les fournisseurs
- Statistiques et tendances actuelles en matière de rapports d'incidents

Analyse des risques

(40) Grâce à leurs connaissances techniques, les CERT apportent une plus-value à l'analyse des risques de leurs clients. Ce service peut consister en partie à réaliser des analyses ou des évaluations de l'infrastructure ou des processus, ou à fournir une assistance pour celles-ci.

Planification de la continuité des activités et de la reprise après sinistre

(41) Les incidents et les tendances de sécurité exercent une influence toujours plus importante sur l'activité et les processus des organisations. Les CERT peuvent apporter une aide précieuse à la reprise ou à la poursuite de l'activité en cas d'incident.

Conseil en sécurité

(42) Le CERT peut proposer une assistance et des conseils pour la mise en œuvre d'infrastructures et de processus de sécurité. L'expérience issue de prestations réalisées pour d'autres clients permet de réutiliser sans cesse les connaissances acquises par ce biais, et de les mettre ainsi à la disposition des autres clients afin d'améliorer leur sécurité en permanence.

Sensibilisation

(43) Un soutien à la sensibilisation peut également être proposé parallèlement à l'assistance technique et dans le cadre des processus. La sensibilisation accroît la sécurité dans les tâches quotidiennes et améliore la compréhension fondamentale. Elle peut s'effectuer via la rédaction d'articles, de newsletters, d'affiches et d'autres moyens similaires.

Formation initiale/continue

(44) Des séminaires, des ateliers, des cours et des guides sont proposés en vue d'accroître les connaissances techniques des clients en matière de sécurité. Les prestations sont conçues en fonction des besoins de ces derniers.

Évaluation ou certification de produits

(45) Le CERT évalue les nouveaux produits et offre la possibilité de les faire certifier. Il peut s'agir ici de produits libres (open source) ou propriétaires (closed source).

2.2.4 Externalisation: services managés et utilisation de services de cloud

Externalisation/services managés

(1) De nombreuses organisations font appel aux services managés et/ou à l'externalisation pour les fonctions nécessitant des technologies et/ou des compétences hautement spécialisées. Il n'est pas rare que des organisations externalisent de nombreuses fonctions de sécurité IT, telles que la réaction aux incidents, l'investigation, les évaluations de la cybervulnérabilité, la gestion des risques, la gestion de la chaîne d'approvisionnement ou d'autres fonctions qu'elles utilisent rarement ou qui ne mobilisent leur savoir-faire que périodiquement. Pour les entreprises, l'un des principaux avantages de l'externalisation réside dans le fait qu'elle requiert moins de capital et peut s'avérer moins coûteuse. Le recrutement d'un collaborateur à temps complet spécialisé dans l'investigation, par exemple, revient extrêmement cher à l'entreprise en raison de son haut niveau de savoir-faire, mais est indispensable pour effectuer des recherches sur les incidents.

(2) Un SLA (service level agreement, accord sur le niveau de service) offre un outil commun pour convenir des prestations entre l'entreprise externalisante et le prestataire. Si le prestataire ne satisfait pas aux exigences du SLA, le bénéficiaire des prestations se réserve le droit de résilier le contrat. Lorsqu'on fait appel à une entité externe pour des services de sécurité, il est important que les deux parties s'accordent sur les rôles, les responsabilités, la gestion et le signalement des incidents, ainsi que sur la sécurité des interfaces et des directives ou procédures d'accès à distance pouvant être requises par un utilisateur. En plus du SLA, les entreprise doivent définir un MOU/MOA (memorandum of understanding/agreement, protocole d'accord/d'entente) et un ISA (interconnection

security agreement, accord sur la sécurité des interconnexions) décrivant les exigences spécifiques que doivent remplir les prestations en termes de gestion et de technique.

(3) Lorsqu'un prestataire externe effectue ou contrôle les évaluations techniques, toutes les parties devraient définir et accepter des règles de collaboration. Les évaluations de la cybervulnérabilité, par exemple, nécessitent habituellement de procéder à un certain nombre d'analyses ou de tests passifs ou actifs sur les systèmes cibles, ce qui signifie que les auteurs des évaluations y accèdent eux-mêmes ou doivent observer les accès d'autres personnes aux cyberactifs critiques au sein de l'environnement des systèmes à contrôler. L'équipe d'évaluation collabore avec ses homologues au sein de l'organisation afin de s'assurer que les activités de test ne perturbent pas l'activité du client, et de convenir ensemble de mesures de surveillance des protocoles si les activités occasionnent des problèmes quelconques pour l'entreprise. Les RoE (rules of engagement, règles d'engagement) définissent quelles activités ont lieu dans quels systèmes et qui peut les réaliser. Elles précisent également si les tests sont effectués au sein du système de contrôle-commande (de production actif) primaire ou d'un équivalent crédible, comme un système de sauvegarde ou de contrôle secondaire, un réseau d'essai ou un autre système autonome. Les analyses actives de systèmes de production doivent être évitées, car elles peuvent perturbent l'activité ou créer un déni de service. Les activités passives, comme l'écoute passive, peuvent être appropriées. En cas de recours à un système de remplacement, il convient de le comparer au système actif afin de vérifier que leurs fonctionnements sont bien identiques. L'équipe d'évaluation et l'organisation doivent en outre définir ensemble quelles personnes auront «les mains sur le clavier» pendant la phase de tests, en particulier lorsque ceux-ci portent sur des systèmes de contrôle-commande (de production) actifs. Le personnel local devrait réaliser tous les tests sur un système de contrôle-commande actif selon les instructions de l'équipe d'évaluation.

Utilisation de services de cloud

(1) Lorsque des organisations utilisent des services de cloud pour le stockage de données (transfert, stockage, traitement), elles doivent tenir compte des aspects correspondants en matière de sécurité et de risque. Pour des raisons de sécurité, chaque élément d'une architecture ICS hébergée de façon externe doit fournir un niveau de durcissement de la sécurité conforme au degré de criticité de la fonction qu'il héberge. En outre, l'entreprise doit exiger de son prestataire de cloud la prise en compte de l'intégrité, de la disponibilité et de la confidentialité des informations ICS, ainsi que des détails fonctionnels et opérationnels associés à la restauration, à la gestion des événements et des perturbations, au basculement en cas de panne, à l'assistance en matière d'investigation, à la surveillance et à d'autres processus opérationnels. Parmi les autres aspects à prendre en compte pour la délocalisation de ressources dans le cloud figurent la dépendance vis-à-vis des connexions au FAI (fournisseur d'accès à Internet) et les possibles augmentations de bande passante susceptibles de survenir. Les instruments juridiques et le recours aux SLA sont importants, car toutes les exigences en matière d'assistance opérationnelle doivent être explicitement identifiées en vue de garantir que les attentes vis-à-vis du fournisseur de cloud, de la disponibilité du FAI et de la capacité de la bande passante sont pleinement satisfaites, afin d'éviter les surprises ultérieures en cas de problème opérationnel. D'autres aspects doivent également être pris en compte, y compris les effets de la répartition de charge et les autres conséquences possibles lorsqu'un fournisseur de cloud est confronté à un accroissement de l'utilisation des ressources disponibles.

(2) Les mesures suivantes doivent être prises lorsque des infrastructures systèmes ou des processus sont externalisés (externalisation, services managés, services de cloud comme SaaS, IaaS, etc.):

- Documents tels que contrat de prestation de services, SLA, accord de non-divulgation, MOU/MOA, ISA, RoE, etc.
- Établissement d'instructions et de directives internes pour une utilisation sûre des services externalisés (p. ex. respect de la législation locale dans le cadre d'accords sur le niveau de service entre pays différents, stockage de données, etc.)
- Surveillance de la fourniture de la prestation et du SLA, échange périodique entre le prestataire et le bénéficiaire du service au niveau du management et de la direction opérationnelle en vue de contrôler la fourniture des prestations/le respect du SLA
- Contrôle de la fourniture de la prestation par le bénéficiaire auprès du prestataire – audit dit «de seconde partie»
- Contrôle de la fourniture de la prestation par un tiers indépendant auprès du prestataire – audit «dit de tierce partie», rapports SOC (service organization control) encadrés par la norme ISAE (International Standard on Assurance Engagements) 3402
- Benchmarking périodique des prix et/ou des prestations

2.3 Gestion des risques

(1) L'amélioration du statut de cybersécurité via la mise en œuvre d'une stratégie de défense en profondeur ICS commence par une prise de conscience des risques qui sont liés à la cybersécurité ICS pour l'entreprise, car ce risque doit en fin de compte être maîtrisé dans le cadre de la propension générale au risque de l'entreprise.

(2) Il importe ici que les fonctions de l'entreprise chargées de l'exploitation et de la maintenance des systèmes de processus et de contrôle-commande connaissent les méthodes d'identification et d'évaluation des risques pour la sécurité des TIC, et qu'elles sachent les appliquer dans leur environnement système spécifique en coopération avec les responsables de la sécurité. Les principales étapes du processus de gestion des risques TIC sont listées et décrites ci-dessous.

(3) Le processus de gestion des risques TIC permet d'identifier les menaces pouvant peser sur les systèmes TIC, les applications et les données à protéger, de les évaluer et de les traiter à l'aide de stratégies adaptées en matière de risques. Il s'agit ici principalement de réduire les risques repérés de manière appropriée et à l'aide de mesures adéquates, en tenant compte de la rentabilité. La sécurité ne pourra jamais être garantie à 100%. La direction doit par conséquent définir la propension de l'entreprise à prendre des risques. Tous les risques situés au-delà de cette limite doivent être activement traités. Les risques résiduels, eux, doivent être indiqués et acceptés par la direction.

(4) Le processus de gestion des risques se décompose en trois activités principales: l'analyse des risques, l'évaluation des risques et la maîtrise des risques. Un examen des risques est effectué et fait l'objet d'un rapport dans le cadre d'une étape continue de surveillance des risques, afin de contrôler l'efficacité des mesures.

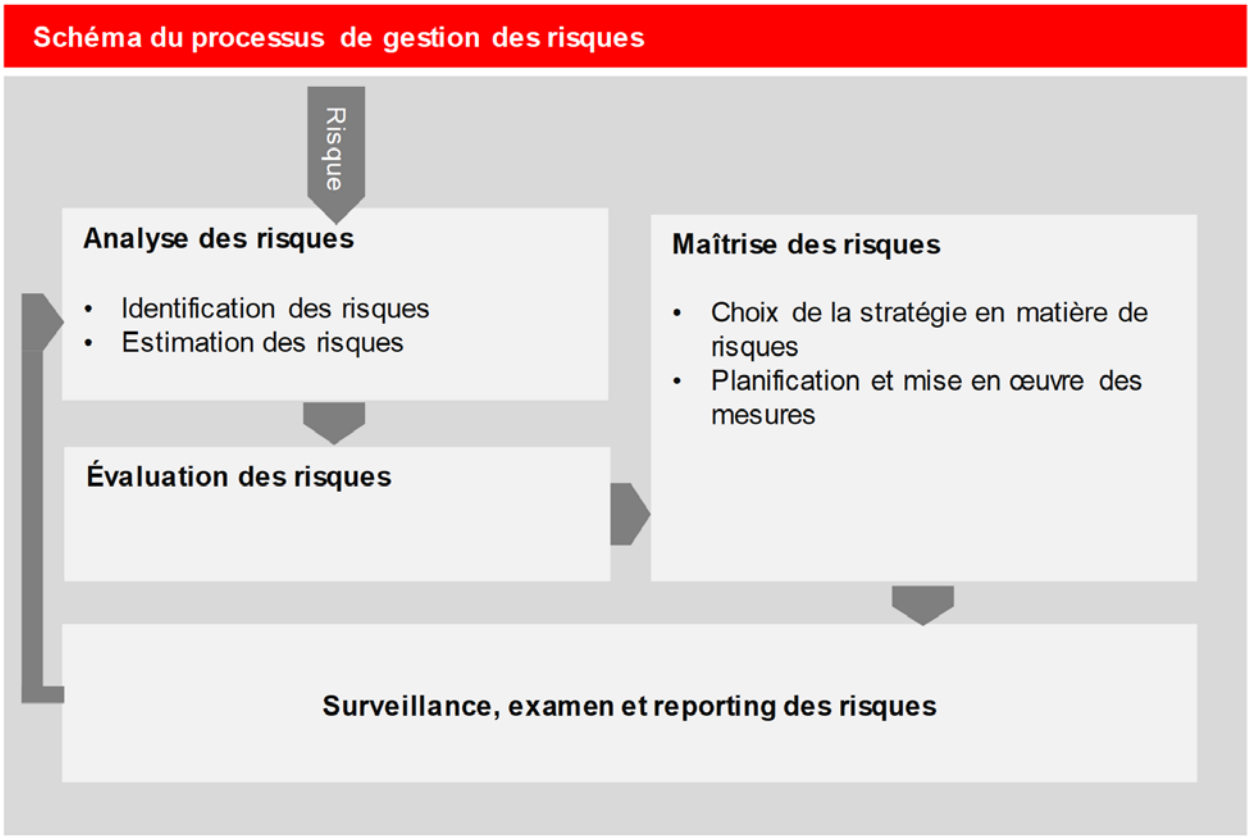

Figure 7 Représentation schématique du processus de gestion des risques

2.3.1 Dresser un inventaire des actifs, l'évaluer et le gérer

(1) Pour pouvoir évaluer les risques, il convient dans un premier temps de définir et d'inventorier les valeurs et les actifs de l'entreprise à protéger. Seule cette approche garantit la réalisation d'une analyse complète et adéquate des menaces.

(2) Il convient en outre de constituer un registre central des actifs permettant de représenter l'ensemble du cycle de vie de ces derniers. Outre les informations nécessaires pour exploiter les actifs de manière intègre, le registre doit également contenir une évaluation de ces derniers au regard des critères de sécurité que constituent la confidentialité, la disponibilité et l'intégrité. Chaque actif doit posséder un propriétaire responsable de la mise en œuvre de son cycle de vie.

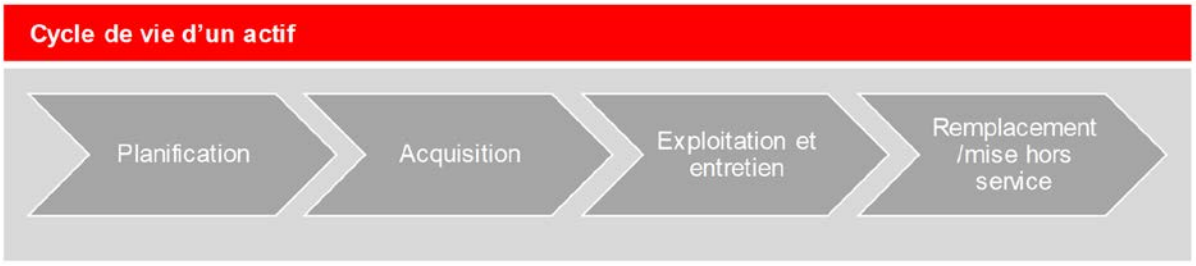

Figure 8 Schéma du cycle de vie d'un actif

L'inventaire doit porter au minimum sur les actifs suivants:
Les actifs suivants doivent être inventoriés: a) Tous les composants physiques et virtuels des systèmes TIC (p. ex. routeurs, points d'accès WLAN, PC, terminaux mobiles, serveurs, appareils de commande et de protection, etc.) b) Bases de données c) Applications d) Zones
Les attributs suivants leur seront affectés: a) Responsable (selon le contexte, responsable de l'application, de l'exploitation ou de l'information) b) Classification c) Version d) Site

Tableau 3 Inventaire des actifs

2.3.2 Analyse des risques

(1) L'analyse des risques constitue la première étape du processus, une fois établi le contexte en matière de risques (domaine, système et objet sur lesquels porte la gestion des risques). Elle se compose de deux activités principales: l'identification des risques et leur estimation. L'identification des risques consiste à examiner de la façon la plus systématique possible tous les facteurs susceptibles d'influer sur le contexte des risques. Pour ce faire, on met en place une analyse permanente des menaces, coordonnée avec l'inventaire des actifs établi et reliée à celui-ci. Cette analyse identifie les menaces potentielles et leurs acteurs et les met en relation avec les mesures de protection et/ou les points faibles existants pour les actifs.

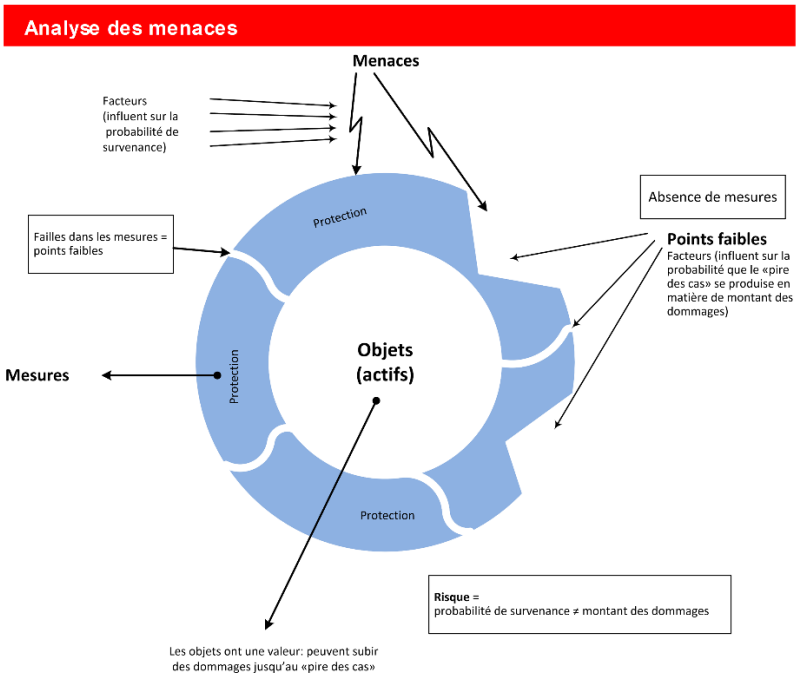

Figure 9 Analyse des risques

(2) L'Office fédéral allemand de la sécurité des technologies de l'information (Bundesamt für Sicherheit in der Informationstechnik, BSI) a publié les dix menaces principales ci-après pesant sur les systèmes de production et d'automatisation des processus:[3]

N°	Menace
1	Ingénierie sociale, ou subversion psychologique («social engineering») et hameçonnage («phishing»)
2	Introduction de logiciels malveillants via Internet et Intranet
3	Infection par des logiciels malveillants via Internet et Intranet
4	Intrusion via des opérations de téléassistance
5	Erreurs humaines et sabotage
6	Composants de contrôle-commande reliés à Internet
7	Erreurs techniques et cas de force majeure
8	Compromission d'Extranet et de composants du cloud
9	Attaques par déni de service (distribué) ou (D)DoS
10	Compromission de smartphones dans l'environnement de production

Tableau 4 Les 10 principales menaces d'après le BSI (instantané)

(3) Lorsque des menaces identifiées rencontrent un point faible (faille), un risque apparaît pour l'actif à protéger. Cette faille peut être comblée par des mesures de protection, ou l'entreprise peut au contraire accepter le risque (traitement des risques). Les menaces émanent de divers acteurs disposant de différents niveaux de savoir-faire, ressources et motivations. Il est impossible pour une entreprise de se prémunir contre tous les acteurs et donc d'atténuer activement tous les risques. L'entreprise doit faire état de certains risques résiduels et les accepter.

[3] Rapport disponible en ligne, à l'adresse suivante:
Industrial Control Systems Top 10 Bedrohungen und Gegenmassnahmen («Les 10 principales menaces des ICS et leurs contre-mesures»; uniquement en allemand)

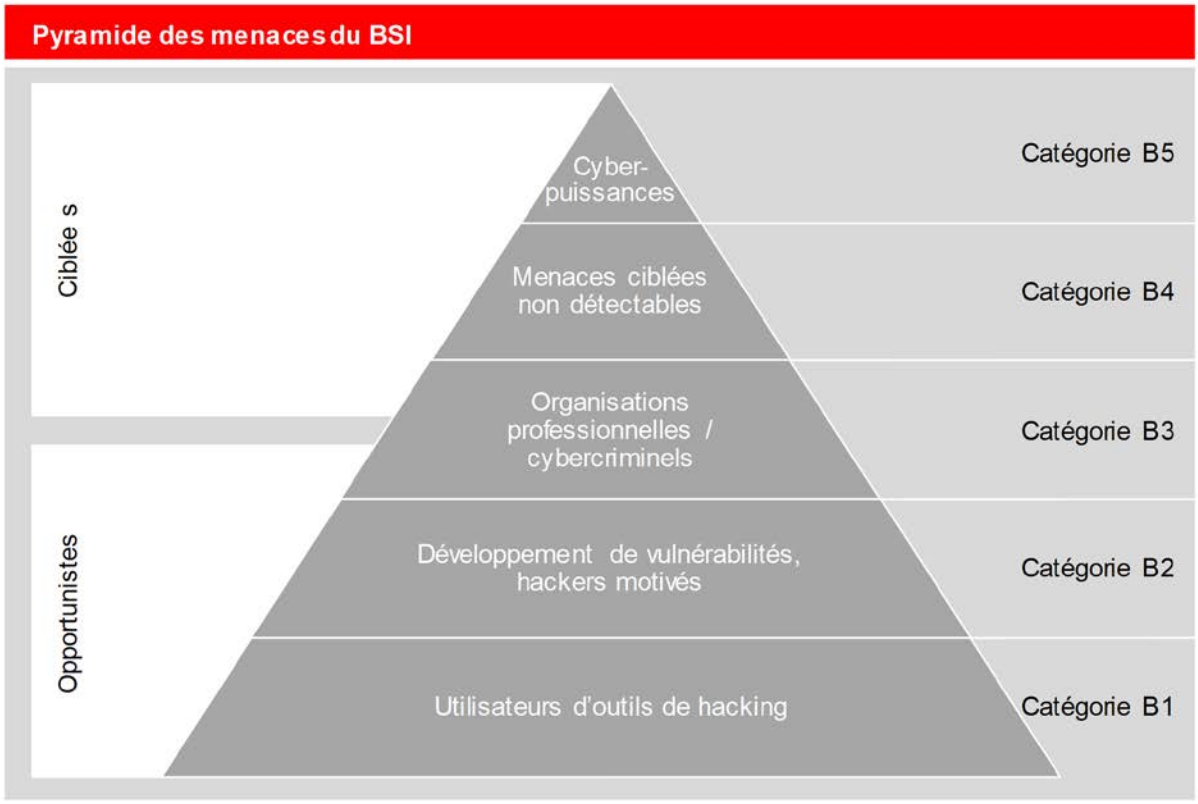

Figure 10 Pyramide des menaces du BSI

N°		Menace	
B1	Pirates débutants	Les «script kiddies» possèdent souvent des connaissances très approfondies. Ils envisagent les attaques sur des infrastructures davantage comme des défis sportifs et recourent pour ce faire à des logiciels courants et à des guides qu'ils peuvent trouver sur Internet. Ils utilisent les logiciels malveillants sans comprendre les détails de ce qui se passe vraiment.	Faible à moyenne
B2	Hackers motivés	Ces personnes sont impliquées à titre professionnel dans la recherche et le développement de méthodes d'attaque. Elles vendent leur savoir et leurs services sur les marchés clandestins du cyberespace, ou mettent leurs connaissances au service d'objectifs politiques ou idéologiques («hacktivistes»).	Très élevée
B3	Organisations professionnelles et cybercriminels	Criminels développant des modèles d'affaires visant à faire de l'espionnage ou à gagner de l'argent par le biais de cyberattaques et des technologies associées. S'ils agissaient auparavant seuls, ils sont aujourd'hui bien organisés et se procurent le savoir-faire qui leur manque et les logiciels malveillants sur les marchés clandestins. La catégorie B3 est aujourd'hui celle qui présente le potentiel de nuisance le plus élevé.	Très élevée

N°		Menace	
B4	Menaces persistantes avancées (advanced persistent threats, APT)	Outils ayant une action ciblée et quasiment indétectable. Ils s'introduisent dans les systèmes protégés (éventuellement en exploitant les erreurs commises par des collaborateurs) et tentent de rester invisibles le plus longtemps possible pour voler d'autres informations (p. ex. des mots de passe) dans le système ou y placer des «bombes à retardement»/portes dérobées.	Très élevée
B5	Cyberpuissances	États-Unis/Chine/Russie/Royaume-Uni/Israël: Le niveau de menace le plus élevé émane d'acteurs soutenus par l'État et issus de ces 5 pays. Ils disposent d'un accès réglementaire et physique aux fabricants de matériel et de logiciels de référence, et peuvent ainsi faire en sorte, p. ex., que des produits déjà pourvus de portes dérobées soient livrés.	Très élevée

Tableau 5 Pyramide des menaces du BSI

(4) Une fois les risques identifiés, il convient de les estimer en fonction de leur probabilité de survenance et de l'étendue des dommages qu'ils peuvent occasionner. Dans le domaine de la sécurité des TIC, on prendra en compte les dommages financiers, mais également l'impact sur la sécurité d'approvisionnement, sur l'intégrité, la confidentialité et la disponibilité des informations, ou encore sur la réputation de l'entreprise. L'estimation des risques peut être effectuée à l'aide d'une matrice des risques.

Matrice des risques (exemple)

Probabilité de survenance							
Probable	L'événement peut survenir avec une probabilité élevée 1 à 3 mois (trimestre)	E4	Moyen	Élevé	Catastrophique	Catastrophique
Possible	L'événement peut survenir 1 an (budget)	E3	Moyen	Moyen	Élevé	Catastrophique
Rare	L'événement peut survenir 1 à 3 ans (PMT)	E2	Faible	Moyen	Moyen	Élevé
Improbable	L'événement peut survenir uniquement dans de très rares circonstances 3 à 10 ans	E1	Faible	Faible	Moyen	Moyen
			S1	S2	S3	S4
			Faible	Modéré	Significatif	Catastrophique
Évaluation financière EAT = résultat d'exploitation de l'entreprise CP = Capitaux propres			Moins de 500 000 CHF Moins de 1% de l'EAT Moins de 0,07% des CP	Entre 500 000 CHF et 5 mio. de CHF Plus de 1% de l'EAT Plus de 0,07% des CP	Entre 5 et 25 mio. de CHF Plus de 10% de l'EAT Plus de 0,7% des CP	Plus de 25 mio. de CHF Plus de 30% de l'EAT Plus de 5% des CP
Réputation - Perception par les médias - Image - Débat politique - Attractivité en tant qu'employeur			Sélective, unique et à court terme Couverture médiatique < 1 semaine Médias régionaux et presse écrite	Couverture médiatique nationale < 1 semaine Campagne dans les médias et/ou grands médias	Couverture médiatique nationale > 1 semaine Campagne dans les médias et/ou grands médias: prise de conscience dans la population grâce à des exemples concrets (perturbations de fonctionnement)	Couverture médiatique nationale > 3 mois, évocation au moins 1 fois/semaine Au moins 1 région linguistique Alliance des médias et des politiques pour remettre le système en question
Sécurité d'approvisionnement			Perturbation régionale	Perturbation importante	Perturbation générale	Blackout sur tout le territoire
Stratégie			Retard dans la mise en œuvre d'éléments essentiels < 1 mois	Retard dans la mise en œuvre d'éléments essentiels < 3 mois	Retard dans la mise en œuvre d'éléments essentiels < 6 mois	Mise en œuvre d'éléments essentiels menacée
			Étendue des dommages			

Figure 11 Matrice des risques (exemple)

2.3.3 Évaluation des risques

(1) Les risques identifiés dans le cadre de l'analyse des risques, ainsi que leurs valeurs en termes d'étendue des dommages, de probabilité de survenance et de risque, nécessitent une évaluation supplémentaire portant sur le contexte de l'objet de l'étude. Il convient notamment de déterminer s'il faut réduire la probabilité de survenance, l'étendue des dommages ou les deux, et d'analyser les interdépendances entre risques et opportunités. Une approche consistant à éviter aveuglément les risques pourrait fermer autant d'opportunités à l'entreprise. À cette étape du processus, l'appréciation prend également en compte les prescriptions externes, comme les obligations légales ou les accords contractuels contraignants.

(2) À ce stade du processus de gestion des risques, le management de l'entreprise doit être informé à l'aide de rapports sur la cartographie des risques (liste de tous les risques identifiés, assortis d'une évaluation). Le management est en devoir de vérifier et de confirmer cette cartographie au regard de la stratégie de la direction de l'entreprise.

(3) Les résultats de cette évaluation sont ensuite intégrés à l'étape suivante (maîtrise des risques) en tant qu'«attributs», et doivent être pris en compte dans l'élaboration des mesures.

2.3.4 Maîtrise des risques

(1) Cette étape du processus de gestion des risques consiste à définir, à planifier et à mettre en œuvre des mesures conformément à l'évaluation des risques, avec pour objectif principal de réduire le profil de risque de l'entreprise à un niveau acceptable (acceptation du risque).

(2) Les mesures de sécurité seront définies de manière à respecter le droit, à offrir un rapport coût-utilité optimal et à correspondre à l'état de la technique, aux avancées technologiques et à la situation en matière de menaces. Il convient de vérifier dans quelle mesure un rapport coût-utilité optimal est adapté au besoin de protection requis pour les infrastructures critiques nationales. On peut partir du principe que certaines mesures de sécurité inadéquates du point de vue économique nécessitent d'être mises en place pour ces infrastructures critiques nationales si l'on souhaite pouvoir garantir le niveau de protection voulu.

(3) Parmi les activités de préparation en vue de la maîtrise des risques figurent un examen de faisabilité des mesures en termes de délais et de coûts et compte tenu des exigences relevées lors de l'étape précédente.

(4) La réduction des risques peut s'effectuer à l'aide des stratégies de maîtrise suivantes:

- Éviter les risques
- P. ex. en renonçant aux processus et aux activités risqués, ou en délocalisant les activités dans des environnements à faible risque.
- Réduire les risques
- La réduction des risques passe par la mise en œuvre de mesures limitant soit l'étendue des dégâts, soit la probabilité de survenance des risques. Cet objectif peut être atteint grâce à des mesures techniques, des processus ou la formation des collaborateurs.
- Transférer les risques
- Il s'agit ici plus particulièrement de répercuter les préjudices financiers sur les assurances.
- Accepter les risques

- Les risques ou les risques résiduels sont volontairement supportés, p. ex. pour pouvoir exploiter les éventuelles opportunités s'offrant à l'entreprise, ou parce qu'il est impossible, d'un point de vue économique, d'assumer toute la charge de l'atténuation du risque.

(5) Le choix d'une stratégie de maîtrise, et donc d'une mesure, s'effectue en fonction des effets de cette dernière sur le risque d'origine. Il est possible de réaliser à nouveau une estimation et une évaluation des risques afin d'obtenir un rapport utilité-coût optimal. Il se peut qu'il faille mener ce processus d'optimisation à plusieurs reprises pour atteindre l'objectif.

(6) Les mesures ainsi définies doivent faire l'objet d'un plan de mise en œuvre à fixer et à communiquer en tenant compte des «attributs» déterminés lors de l'évaluation des risques, p. ex. quant à l'urgence de la mesure.

(7) Les mesures définies doivent impérativement se voir affecter un propriétaire des mesures responsable de leur mise en œuvre et chargé de signaler au propriétaire du risque les éventuelles divergences par rapport au plan de mise en œuvre. Dans ce contexte, la sécurité des technologies de l'information ne constitue pas un état final, mais un processus continu. Les évolutions techniques, en particulier, génèrent sans cesse de nouvelles menaces et/ou de nouveaux vecteurs d'attaque. L'étendue des dommages d'un risque déterminé antérieurement peut aussi se modifier avec le temps. Toutes les tâches relevant de la maîtrise des risques doivent par conséquent être revérifiées à intervalles réguliers et, le cas échéant, adaptées et exécutées.

2.4 Le facteur humain

(1) Les êtres humains sont par essence des «systèmes» sujets aux erreurs. En conséquence, les entreprises sont confrontées à de nombreux défis dès lors qu'il s'agit de gérer le facteur humain dans le cadre de la sécurité des TIC. Les systèmes complexes et de grande envergure peuvent être affectés par les erreurs commises par un personnel inexpérimenté ou peu exercé et par les activités de menaces d'initiés malveillants. Le cas le plus fréquent n'est cependant pas le fait d'un collaborateur malintentionné, mais d'un collaborateur étourdi ou négligent. Par ignorance, inattention ou facilité, les collaborateurs ont tendance à se comporter tôt ou tard de manière inadaptée. Un scénario typique, par exemple, consiste à gérer les mots de passe avec légèreté, p. ex. en choisissant des mots de passe faciles à deviner ou en les inscrivant sur un post-it près de l'appareil. Autre scénario réaliste: le collaborateur clique sur un lien contenu dans un e-mail et visant par exemple à détourner des données d'accès ou à installer un maliciel. L'emploi d'appareils (qui peuvent ne pas être autorisés) et de support de données privés (clés USB, disques durs externes) ou encore l'échange de fichiers via des services de messagerie ou de cloud non autorisés (dépôt de documents commerciaux sur Dropbox, etc.) se rencontrent également régulièrement. Ces comportements inadaptés peuvent nuire aux activités de l'entreprise concernée, même si les collaborateurs ne nourrissent généralement pas d'intentions criminelles lorsqu'ils commettent les actions des exemples cités.

(2) La menace augmente en même temps que l'intention criminelle, qui peut différer selon les cas. Des collaborateurs peuvent chercher à s'enrichir pour des raisons financières, ou agir par frustration personnelle et chercher à nuire à leur employeur. Le scénario le plus dangereux réside dans une action planifiée dans laquelle les collaborateurs sont victimes de chantage ou de corruption dans le but, p. ex., d'installer des logiciels malveillants ou de dévoiler des données d'accès.

(3) Il est impératif que les entreprises sensibilisent leurs collaborateurs à ces multiples risques et les forme régulièrement à une utilisation des outils TIC conforme aux prescriptions en vigueur.

2.4.1 Directives

(1) Des mesures claires et applicables sont nécessaires pour définir le cadre de contrôles stricts visant à sécuriser les technologies ICS et à mettre en place la gouvernance requise pour maîtriser le facteur humain. Les politiques fixent le cadre de procédures détaillées ainsi que les attentes de l'organisation vis-à-vis des activités menées. Les directives exposent les règles de sécurisation des ICS en indiquant les règles de comportement à suivre et les contrôles nécessaires. Les politiques décrivent ce qui doit et ce qui ne doit pas arriver et les sanctions en cas de non-respect.

2.4.2 Procédures

(1) Historiquement, la gestion de la sécurité a toujours été confiée à l'instance chargée de la sécurité IT, laquelle, généralement guidée par des directives, des processus opérationnels et des procédures, protège les données et informations importantes de l'entreprise. Les systèmes de contrôle-commande industriels faisant aujourd'hui partie de réseaux et d'architectures interdépendants de plus grande envergure, les procédures et les mécanismes de sécurité doivent être adaptés en conséquence pour pouvoir inclure également la commande de processus interconnectée.

(2) Les procédures doivent définir la manière d'exécuter certains processus ou de configurer certains systèmes en vue de garantir un fonctionnement standard, sûr, compréhensible et reproductible des systèmes de contrôle-commande. Des procédures définies, documentées et standardisées permettent également de former les nouveaux collaborateurs de façon simple et rapide et de veiller ainsi à ce que l'ensemble du personnel applique de manière homogène les prescriptions et les normes requises dans tout l'environnement OT. Les procédures de sécurité des ICS guident les opérateurs ICS lorsqu'ils doivent prendre des mesures dans les situations d'urgence, comme p. ex. en cas d'intrusion de logiciels malveillants ou d'autres interruptions d'activité imprévues. Des procédures de sécurité standardisées sont particulièrement importantes dans l'environnement ICS, en raison des exigences élevées de disponibilité et de fonctionnement en temps réel. L'utilisation de protocoles spécifiques au fabricant et la longévité des systèmes hérités peuvent en effet entraver les efforts visant à protéger les systèmes critiques pour l'entreprise, et en particulier les infrastructures critiques. Des indicateurs et des points de mesure peuvent être fixés et mesurés dans le cadre de procédures standard définies et documentées, ce qui favorise ainsi la performance globale et permet de réaliser des benchmarkings sur une plus longue période ou des comparaisons. Enfin, des procédures standardisées reproductibles et des indicateurs mesurés autorisent également un contrôle continu et une amélioration permanente de l'efficacité et de l'efficience. Il est difficile d'améliorer une procédure lorsqu'elle est exécutée différemment à chaque passage et que l'on ignore ce qu'apporterait une amélioration.

2.4.3 Formation et sensibilisation

(1) De nombreuses organisations négligent plus fréquemment les formations à la sécurité et les activités de sensibilisation que beaucoup d'autres aspects de l'exploitation des ICS. Les propriétaires et les exploitants OT se fient à leur connaissance intime du système et des processus pour garantir le bon fonctionnement de celui-ci, et n'allouent généralement que du temps et des ressources à cet objectif. Les ICS étant de plus en plus interconnectés et les cybermenaces et les vulnérabilités prenant toujours plus d'ampleur, il est primordial pour les entreprises d'exiger et de favoriser des formations

spécifiquement consacrées à la sécurité des ICS. Les responsables de la mise en œuvre IT et les exploitants OT devraient savoir comment se présentent les indicateurs d'éventuelles compromissions et quelles mesures ils devraient prendre pour garantir la réussite d'une cyberenquête. Le management IT et ICS devrait également savoir quelles actions il peut entreprendre pour améliorer la sécurité du système, afin de pouvoir prendre des décisions judicieuses en termes de rapport coût-utilité des mesures de protection mises en place.

2.5 Gestion des fournisseurs et des fabricants

2.5.1 Directives de sécurité pour la gestion des fournisseurs et des fabricants

(1) Ces dernières années, les fournisseurs ont pris conscience de l'importance de la cybersécurité dans les solutions de contrôle-commande industrielles, principalement après que les cybervulnérabilités liées à des exploits comme Stuxnet, SQL Slammer ou autres ont été rendues publiques.

(2) Afin de répondre aux exigences du nouveau marché, de nombreux fabricants – pas tous, mais la plupart des leaders du marché – ont intégré des composants de sécurité au cycle de vie de leurs produits.

(3) Partir du principe que les fournisseurs intègrent systématiquement des mesures de sécurité strictes au cycle de vie de leurs produits est une erreur. Il est par conséquent indispensable de prendre en compte les exigences de sécurité de manière précoce lors de l'acquisition du système de contrôle-commande. Cette démarche s'avère non seulement avantageuse pour le propriétaire de l'installation, mais permet aussi au fournisseur de disposer d'instructions spécifiques quant aux fonctionnalités requises.

(4) Il convient de tenir compte des points suivants:

- Vérifier le cycle de vie/développement du produit et les éléments de sécurité qui sont garantis par le fournisseur/fabricant.
- S'assurer auprès du fournisseur/fabricant que le système intégré ne contient pas de composants manipulés, falsifiés ou échangés.
- S'assurer que le système intégré est conforme aux spécifications et qu'aucune fonction cachée n'a été mise en place lors de la fabrication.
- Vérifier quelles exigences du fournisseur/fabricant sont remplies en termes de maintenance/service après-vente de ses produits (gestion/périodicité/accès aux correctifs), et/ou contrôler si le fabricant respecte les exigences/règles internes.
- Élaborer un catalogue des exigences minimales pour les fournisseurs/fabricants.

2.5.2 La sécurité dans les appels d'offres et les contrats

(1) Il ne faut pas négliger les aspects liés à la sécurité en cas d'appels d'offres ou de contrats avec des tiers. Les appels d'offres doivent préciser les normes de sécurité applicables et les consignes de sécurité régissant la mise en place et/ou l'exploitation d'un système. Il est tout aussi important de définir des accords de confidentialité, ainsi que des conventions sur les processus permettant d'effectuer des modifications au sein du système de production. Ces mesures visent à empêcher formellement toute fuite d'information depuis l'entreprise et à établir clairement qui peut procéder à quelles modifications.

(2) La liste ci-dessous présente les contenus contractuels possibles en matière de sécurité:

Informations/données

- Quelles informations sont classées confidentielles/secrètes et comment doivent-elles être traitées?
- Quel canal de communication et quel procédé cryptographique employer pour chiffrer les données?
- À quel endroit le stockage des données secrètes/confidentielles est-il autorisé? En cas de sauvegarde sur des systèmes externes, il convient de définir comment et quand les données peuvent être durablement supprimées. On accordera une attention particulière aux supports de sauvegarde et aux éventuels sites de stockage en cloud.
- Il sera fait en sorte que toutes les informations et données communiquées au prestataire ou générées dans le cadre de son activité soient traitées ou stockées uniquement chez ce prestataire. Si le stockage et/ou le traitement sont effectués par des tiers, on veillera à ce que ces derniers respectent les exigences des directives de sécurité applicables.

Composants et systèmes TIC

- Lorsque des systèmes et des composants TIC sont mis en réparation ou au rebut, la préservation de la confidentialité doit être garantie tout au long du processus.
- Destruction de données/de configurations sur les composants TIC et/ou des composants TIC eux-mêmes.

Protection de base/interfaces

- Par quelles dispositions contractuelles les collaborateurs du fournisseur/fabricant sont-ils tenus de garantir la protection de base des technologies de l'information ou un niveau de protection comparable?
- Toutes les interfaces entre les parties au contrat sont-elles identifiées de façon à permettre de fixer en conséquence les exigences en matière de sécurité?
- Les droits (d'accès physique ou informatique) que le mandant doit octroyer au fournisseur/fabricant sont-ils définis?
- Comment est identifié et enregistré le personnel du fournisseur/fabricant?
- Les obligations/exigences légales et les droits de propriété intellectuelle sont-ils respectés par le fournisseur/fabricant et comment ce point est-il garanti?
- La forme sous laquelle le fournisseur/fabricant est autorisé à recourir à la sous-traitance est-elle définie, et des mécanismes de contrôle sont-ils établis?

2.5.3 Gestion de la chaîne d'approvisionnement

(1) La chaîne d'approvisionnement représente un risque considérable pour les systèmes ICS. Les fabricants d'ICS et les éditeurs de logiciels créent leurs produits en de nombreux endroits du globe. Les circuits et les puces sont souvent décrits sur le plan fonctionnel et physiquement produits par des organisations différentes. Les sociétés dites «fabless» (sans usine de fabrication), qui développent des circuits et des puces mais ne les produisent pas elles-mêmes, peuvent être aussi bien des fabricants renommés de puces électroniques que des petites entreprises hautement spécialisées. La fabrication est confiée à des sociétés spécialisées, appelées «fonderies de silicium», réparties dans le monde entier mais principalement hors d'Europe. Les puces ainsi fabriquées sont livrées depuis l'usine directement au client ou au grossiste. Les distributeurs réputés sont également répartis dans le monde entier.

(2) Il est par conséquent impossible, pour la plupart des exploitants d'ICS, de garantir la sécurité du système ou de l'application pendant toute la durée du cycle de développement. L'achat de produits standard du commerce (technologies COTS[4]) accroît la probabilité de recevoir des appareils qui ne sont pas d'origine. Le CERT de l'ICS a par ailleurs connaissance de rapports faisant état d'appareils associés à un code intégré non autorisé au sein de son microprogramme ou du système d'exploitation, ce qui ménage une «porte dérobée» dans les appareils ou permet au programme, une fois installé, de communiquer avec l'extérieur. Pour atténuer ces menaces, les propriétaires d'actifs doivent prêter une grande attention aux contrats d'achat, au contrôle qualité et à la validation de la performance en fonction des processus de spécification. Un contrôle complet, y compris une analyse des points faibles, constitue par ailleurs une tâche importante avant d'installer des systèmes dans des environnements de production.

(3) En cas de besoin de protection accru, il faudra accorder aux fabricants et à leurs sous-traitants fiables un agrément pour produire des matériels ou des logiciels. La preuve doit en être consignée. Cette certification des fabricants doit être renouvelée régulièrement.

(4) Exemples rencontrés ces dernières années dans des environnements ICS/IT:

- matériel réseau ou informatique installé avec un maliciel;
- logiciel ou matériel infecté par un maliciel par différents moyens;
- points faibles dans les applications et les réseaux logiciels au sein de la chaîne d'approvisionnement;
- infection par téléchargement de pilotes depuis Internet;
- matériel informatique falsifié.

2.5.4 Surveillance et contrôle des prestations

(1) Lorsque des prestataires externes sont impliqués dans le projet, par exemple pour l'hébergement, la mise en place, l'installation, le développement logiciel ou la livraison de logiciels standard, il convient de les engager par contrat à respecter la sécurité IT. La surveillance des prestations consiste alors à assurer le suivi des règles contractuelles et à vérifier qu'elles sont bien respectées, l'objectif étant d'empêcher toute violation des critères de sécurité définis dans le cadre du déroulement du projet/de la prestation de service.

2.5.5 Surveillance et contrôle des accès à distance

(1) Le recours aux services d'un prestataire nécessite souvent un accès à distance aux systèmes en vue de leur maintenance. Ce type d'accès constitue l'une des principales menaces en matière de sécurité des systèmes. Le défi consiste à limiter autant que possible l'accès et à enregistrer les opérations réalisées par le prestataire de manière compréhensible. L'identité de l'intervenant, ainsi que les moments, les règles et les systèmes concernés par l'intervention doivent être clairement définis.

(2) La liste ci-dessous énumère les exigences en matière d'accès à distance à des fins de maintenance:

- Chaque accès à distance s'effectue exclusivement via un compte personnalisé autorisant l'accès uniquement aux systèmes requis.

[4] COTS: Commercial off-the-shelf

- L’accès à distance n’est possible qu’après autorisation par le personnel d’exploitation. Toute session non séparée le sera automatiquement à l’issue d’un délai défini. Une fois la session séparée, la connexion aux systèmes s’effectuera de manière distincte sur le plan logique et, dans la mesure du possible, physique.
- La maintenance réalisée sur place par le prestataire constitue un risque de sécurité à prendre au sérieux. On évitera que le mandataire connecte son propre matériel au réseau de processus (p. ex. ordinateurs portables pour effectuer la maintenance, mais aussi périphériques de stockage tels que clés USB). Si cela s’avère cependant nécessaire, ce matériel devra être soumis à une sécurisation spéciale, approuvé par le mandataire et faire l’objet d’une recherche de maliciels dans les meilleurs délais. Le prestataire est tenu d’attester de l’application de directives de sécurité internes adaptées pour fournir cette prestation.
- Enregistrement des accès à distance (*session recording*).

2.6 Sécurité physique

(1) Les mesures de sécurité physique réduisent le risque de pertes ou de dommages involontaires ou intentionnels affectant les actifs d’une organisation ou l’environnement. Parmi les actifs d’une entreprise figurent notamment les actifs matériels, comme les appareils et les installations, l’environnement et la propriété intellectuelle, y compris les données propriétaires comme les paramétrages de processus et les informations clients.

(2) Les contrôles de sécurité physique doivent fréquemment répondre à des exigences environnementales, sécuritaires, régulatoires, juridiques et autres, souvent spécifiques à un environnement donné. Les mesures de sécurité physique devraient être adaptées aux exigences supérieures de la protection globale.

(3) Les entreprises doivent traiter la protection physique des cybercomposants et données associés à l’ICS comme un élément de la sécurité globale de l’environnement ICS. La sécurité de nombreux équipements ICS est étroitement liée à la sécurité des installations, l’objectif premier étant d’éviter aux personnes de se retrouver dans des situations dangereuses, sans pour autant les gêner dans leur travail. Les contrôles de sécurité physique sont des mesures physiques, actives ou passives, restreignant l’accès physique à tous les actifs d’information présents dans l’environnement ICS. Ces mesures sont mises en œuvre par les entreprises pour éviter les conséquences indésirables sur les systèmes, notamment les suivantes:

- accès physique non autorisé à des sites sensibles;
- modification, manipulation, vol ou autre soustraction ou destruction physique de systèmes, infrastructures, interfaces de communication, personnel ou sites physiques existants;
- consultation illicite d’informations sensibles et d’actifs par observation visuelle, prise de notes, photographie ou d’autres moyens;
- introduction illicite de nouveaux systèmes, infrastructures, interfaces de communication ou autres matériels;
- introduction illicite d’appareils développés intentionnellement pour réaliser des manipulations matérielles, des écoutes ou d’autres activités nuisibles par le biais de dispositifs de stockage USB, de points d’accès sans fil, du Bluetooth ou d’autres technologies mobiles.

2.6.1 Principes de la sécurité physique

(1) L'accès physique aux composants des systèmes de contrôle et de commande implique fréquemment un accès logique au système de contrôle-commande de processus. L'accès physique permet à un éventuel délinquant d'obtenir un contrôle logique grâce à des mesures physiques, p. ex. lorsque les ordinateurs sont aisément accessibles et équipés de lecteurs de médias mobiles (lecteurs de disquettes, lecteurs CD/DVD/Blu-ray, disques durs externes ou ports USB). Les entreprises peuvent doter ces lecteurs de cadenas, les éloigner des ordinateurs ou désactiver les ports USB. Selon les besoins et les risques en matière de sécurité, il est également possible de désactiver les boutons d'alimentation ou de les protéger physiquement pour empêcher leur actionnement par des personnes non autorisées. Pour une sécurité maximale, les serveurs sont implantés dans des zones fermées à clé et protégés par des mécanismes d'authentification (p. ex. double authentification, ou authentification à deux facteurs). Les dispositifs réseau au sein du réseau ICS, y compris les switchs, routeurs, prises réseau, serveurs, stations de travail et contrôleurs, doivent être accessibles uniquement pour un cercle de personnes autorisées et dans une zone sécurisée. Cette dernière devrait en outre être compatible avec les exigences de protection environnementale (p. ex. installations d'extinction au halon).

(2) La sécurité physique traditionnelle est généralement constituée d'une architecture de mesures physiques échelonnées en cercles concentriques. Ce périmètre de sécurité se matérialise sous la forme de barrières physiques successives, aussi bien actives que passives, autour des bâtiments, installations, locaux, appareils ou autres actifs d'information. Les contrôles de sécurité physique incluent des clôtures, des fossés, des talus, des murs, des barricades renforcées, des portails ou d'autres mesures. Dans la plupart des entreprises, la première mesure de défense consiste en un accès protégé aux installations, comme p. ex. des clôtures, des gardiens, des portails et des portes fermées à clé.

(3) Les systèmes de contrôle physique des accès visent à garantir que seules les personnes autorisées ont accès aux espaces contrôlés. Ils doivent en outre se montrer flexibles. Les accès nécessaires peuvent en effet varier selon la période de la journée, de la semaine ou de l'année, le niveau de formation, le statut professionnel, la tâche, l'état des installations ou d'innombrables autres facteurs. Le système doit s'assurer que les personnes bénéficiant de l'accès sont effectivement celles qu'elles affirment être; il recourt généralement pour ce faire à un objet en possession de la personne (carte d'accès ou clé), à une information qu'elle détient (code PIN) ou à un élément la caractérisant (caractéristique biométrique). Les systèmes de contrôle d'accès devraient offrir une excellente fiabilité sans pour autant entraver les tâches habituelles ou les procédures d'urgence du personnel de l'installation. Leur intégration à l'ensemble du système de processus permet de bénéficier d'une vue d'ensemble plus large par rapport aux accès simplement sécurisés; elle autorise un suivi physique, peut écourter les temps de réaction, notamment dans les situations d'urgence, et améliore la productivité globale. Il ne faudrait autoriser l'accès aux armoires et aux ordinateurs réseau qu'aux personnes devant exécuter des tâches. Tous les ordinateurs et les périphériques réseau doivent être installés dans des racks sécurisés. Le raccordement à ces derniers s'effectuera par le biais d'un terminal distant ou d'une interface homme-machine (IHM) distante.

(4) Les systèmes de surveillance des accès sont composés de caméras fixes, de caméras vidéo, de capteurs et de différents types de systèmes d'identification. Ces appareils n'empêchent pas expressément l'accès à un site particulier, mais ils y enregistrent la présence ou l'absence physique. Selon le type de dispositif de surveillance employé, on veillera à un éclairage suffisant.

(5) Les systèmes visant à limiter les accès peuvent faire appel à une combinaison d'appareils pour contrôler ou empêcher l'accès physique à des ressources protégées. Il peut s'agir de dispositifs aussi bien actifs que passifs, comme des clôtures, des portes, des coffres-forts ou des portails, souvent associés à des systèmes d'identification ou de surveillance, dans le but d'autoriser l'accès à certaines personnes ou groupes de personnes en fonction de leurs rôles.

(6) La localisation des personnes et des véhicules dans une grande installation est importante non seulement au regard de la sécurité de l'information, mais aussi de la sécurité au travail et d'exploitation (qui correspond à l'anglais «safety», c.-à-d. la vie et l'intégrité corporelle des personnes). Les technologies de localisation peuvent suivre les mouvements des personnes et des véhicules au sein de l'installation afin de veiller à ce qu'ils restent dans les zones autorisées, ou fournir au personnel l'aide et le soutien nécessaires en cas d'urgence.

(7) Les besoins de sécurité d'un système et de ses données doivent toujours être traités en tenant compte de l'environnement, p. ex. avec des filtres à air dans un environnement poussiéreux. Cet aspect revêt une importance particulière en présence de poussière conductrice ou magnétique ou dans les environnements contenant des systèmes et des supports nécessitant une température ou une humidité stable. Le système de contrôle-commande de processus devrait déclencher une alarme lorsque les valeurs prescrites pour l'environnement, comme la température ou l'humidité, dépassent certains seuils.

(8) Les systèmes de chauffage, de ventilation et de climatisation (CVC, en anglais «heating, ventilation and air conditioning», HVAC) doivent impérativement protéger le personnel d'exploitation en conditions normales et en cas d'urgence, ce qui peut libérer des substances toxiques dans l'atmosphère. Il faudrait que les entreprises utilisent avec précaution les systèmes d'extinction des incendies afin d'éviter de générer des dommages plus importants encore. Les systèmes HVAC et de protection contre les incendies doivent également être protégés contre d'éventuelles cyberattaques (en 2014, des hackers ont réussi à s'infiltrer dans le système financier de la société commerciale américaine TARGET via le HVAC; cet exemple est demeuré célèbre).

(9) Un approvisionnement fiable en électricité revêt une importance capitale, ce qui rend indispensable une alimentation sans interruption (uninterrupted power supply, UPS) pour les systèmes de contrôle-commande. En présence d'un générateur de secours, la batterie UPS ne doit fournir de l'électricité que durant quelques secondes; au contraire, lorsqu'on est tributaire d'une alimentation externe, la batterie UPS peut être sollicitée durant plusieurs heures. Elle doit donc être paramétrée de façon à permettre au moins un arrêt du système en toute sécurité.

(10) La sécurité physique du centre ou de la salle de contrôle réduit l'impact de nombreuses menaces. Les centres et les salles de contrôle abritent fréquemment des consoles connectées en permanence, avec un accès continu aux serveurs primaires de contrôle-commande; la rapidité de réaction et la visibilité permanente sur l'installation jouent ici un rôle de premier plan. Ces zones abritent également souvent les serveurs eux-mêmes ainsi que d'autres nœuds informatiques et systèmes de contrôle-commande critiques. Les responsables des actifs doivent autoriser leur accès uniquement à des utilisateurs habilités, et recourir pour cela à des méthodes d'authentification telles que les cartes d'identité intelligentes ou magnétiques ou les appareils biométriques. Dans de nombreux cas, il est nécessaire de prévoir une centrale d'urgence/un poste de conduite hors site afin de pouvoir garantir le contrôle lorsque le poste primaire devient inutilisable.

(11) Les ordinateurs et les appareils commandés par ordinateur et servant aux fonctions de l'ICS (comme p. ex. les automates programmables industriels, API) ne devraient pas quitter la zone de l'ICS. Les ordinateurs portables, les ordinateurs portatifs destinés au paramétrage ou à la téléconduite et les terminaux mobiles devraient faire l'objet d'une sécurisation stricte et ne pas être utilisés en-dehors du réseau ICS.

(12) Il faudrait que les entreprises sécurisent également la conception de leurs câblages et leur mise en place pour le réseau de contrôle-commande. Les câbles de communication torsadés non blindés, acceptables dans un environnement de bureau, ne conviennent généralement pas aux installations, en raison de leur sensibilité aux perturbations provoquées par les champs magnétiques, les ondes radio, les températures extrêmes, l'humidité, la poussière et les vibrations. Les câbles optiques ou coaxiaux constituent souvent une meilleure solution pour le câblage du réseau de contrôle-commande, car ils résistent à de nombreuses conditions caractéristiques de ce type d'environnements, y compris aux interférences électriques et radioélectriques, fréquentes dans les environnements de contrôle-commande industriels. Les codes couleur, les câbles étiquetés et les connecteurs réduisent le potentiel d'erreurs de connexion involontaires. L'installation des câblages dans des armoires verrouillables limite leur accès au personnel autorisé.

(13) Pour résumer, les mesures minimales de sécurité physique peuvent être définies comme suit:

- Définition de différentes zones de sécurité, chacune associée à des exigences spécifiques en matière de sécurité physique. Répartition des composants sur des sites décentralisés, en particulier pour les systèmes de transport et de distribution de l'énergie et dans le domaine de la production décentralisée. Implantation de l'équipement dans les locaux techniques et les salles de contrôle, dans le bâtiment ou sur des sites décentralisés. L'appareil peut parfois se trouver chez des prestataires ou au sein d'environnements publics. Il est habituellement impossible de garantir une protection physique complète pour les sites périphériques, qui sont parfois inoccupés; le risque résiduel doit par conséquent, le cas échéant, faire l'objet de mesures complémentaires et de contrôles compensatoires.
- Définition de contrôles minimaux de sécurité physique à des fins de prévention et de détection pour les différentes zones de sécurité.
- Contrôle physique du périmètre: mise en œuvre de mesures de sécurité visant à protéger les zones de sécurité contenant des informations ou des installations de traitement sensibles ou critiques.
- Contrôle des accès: les zones sécurisées sont protégées par des contrôles d'accès ad hoc et accessibles uniquement au personnel autorisé.
- Bureaux et locaux d'exploitation: la sécurité physique des bureaux et autres locaux importants, comme les postes de conduite, est définie et mise en œuvre.
- Protection contre les menaces externes et environnementales: la protection physique contre les attaques naturelles et malveillantes est définie et mise en œuvre.
- Définition, délimitation et sécurisation physique de zones sûres.
- Définition, isolement et protection physique correspondante des points d'accès (p. ex. zones de livraison ou de chargement).
- Centres de contrôle: il convient d'élaborer, de développer et d'appliquer des mesures visant à garantir la sécurité physique des centres de contrôle abritant des systèmes de contrôle-commande centraux (p. ex. serveurs de commande, interfaces homme-machine et systèmes de support).

- Locaux techniques, d'appareillage et périphériques: des mesures de sécurité physique doivent être définies et mises en œuvre selon le degré de criticité et le niveau de danger.

(14) Nous attirons également l'attention sur le fait qu'il existe une recommandation distincte de la branche[5] sur la sécurité physique, émanant de l'AES.

2.7 Architectures réseau ICS

(1) Une architecture réseau ICS sûre et robuste constitue l'un des principaux piliers d'une protection efficace contre les attaques. Chaque interface, chaque jonction et chaque connexion représente un danger potentiel. C'est pourquoi il est indispensable que tous les processus survenant sur les différents réseaux et installations soient connus et dûment traités. Pour ce faire, un regroupement et une segmentation appropriés sont essentiels.

2.7.1 Principes et fondements

(1) Par le passé, les systèmes ICS fonctionnaient de manière strictement isolée du monde extérieur et cloisonnée. Les exigences actuelles en matière d'échange d'informations et d'automatisation entre les systèmes ICS et les applications métier nécessitent l'établissement de liaisons et/ou d'interconnexions entre les différents systèmes. Une autre difficulté réside dans les systèmes dédiés à des fonctions spécifiques, comme p. ex. la surveillance des bâtiments, la conduite du réseau ou le contrôle-commande de la production, qui doivent fréquemment être regroupés en un seul réseau. Ainsi, chaque liaison ou interconnexion entre ces sous-systèmes crée une jonction susceptible de générer un risque de sécurité potentiel. De plus, l'emploi de composants informatiques (matériels et logiciels) standard devant en permanence être corrigés et mis à jour rend nécessaires des accès supplémentaires aux moyens requis. Les systèmes modernes sont donc confrontés aux problèmes suivants:

- Chaque interface, connexion ou jonction représente un risque potentiel.
- La distance par rapport aux réseaux publics «non sécurisés», comme Internet, ne cesse de diminuer, car les systèmes sont de plus en plus fréquemment et de plus en plus interconnectés.
- De nombreux systèmes sont aujourd'hui «dépendants» d'Internet, ce qui accroît considérablement les cybermenaces.
- L'environnement TIC fait appel à des technologies dont les points faibles sont connus, ce qui génère des cybermenaces indésirables.
- Absence de modèles d'affaires valables ou compréhension insuffisante des exigences, des procédures et des processus propres à l'environnement ICS.

(2) Auparavant, les environnements ICS étaient isolés des réseaux externes (historiquement non fiables), ce qui permettait de réduire le niveau de protection garanti par la sécurité ICS pour une menace donnée; celle-ci se restreignait pratiquement à l'accès physique à un équipement ou à une installation. La plupart des transferts de données dans l'environnement ICS nécessitaient une surveillance limitée des autorisations ou de la sécurité, car les commandes d'exploitation, les instructions et la saisie des données étaient effectués dans un environnement fermé, via des processus de communication de données fiables. Lorsqu'on envoie une commande ou une instruction via le réseau, on part généralement du principe qu'elle arrivera et exécutera une fonction autorisée, puisque seuls les utilisateurs autorisés ont accès au système.

[5] Ce document de la branche devrait paraître au printemps 2019

(3) L'association d'une architecture IT moderne et d'un environnement ICS isolé susceptible de ne comporter aucune mesure de protection contre les cybermenaces représente un défi de taille. Une simple mise en réseau (c.-à-d. avec des routeurs et des switchs) constitue un moyen évident d'interconnecter des éléments ou des composants au sein de réseaux. L'accès d'une personne non autorisée est toutefois susceptible de déboucher sur un accès illimité à l'ensemble de l'environnement ICS.

(4) Une autre difficulté majeure réside dans l'emploi de moyens IT standard dans l'environnement ICS. Auparavant, la gestion des correctifs s'effectuait uniquement en fonction du fournisseur, et les correctifs n'étaient appliqués aux systèmes qu'en cas d'absolue nécessité. Les moyens IT standard requièrent un «entretien» permanent de la part des prestataires, qui mettent leurs services de correctifs à disposition sur Internet ou dans un cloud. La distance avec les réseaux publics et/ou Internet ne cesse ainsi de s'amenuiser, ce qui accroît la probabilité de voir des logiciels malveillants s'introduire dans l'environnement ICS.

a) Les différents domaines de sécurité (aires, zones et secteurs) de l'environnement ICS

(1) Pour une meilleure compréhension des différents processus, procédures, fonctions et compétences, l'environnement ICS ainsi que les systèmes avoisinants et autres environnements opérationnels impliqués doivent être répartis en différents domaines (aires, zones et secteurs), auxquels sont associées des responsabilités, des compétences et des exigences spécifiques. Une sécurité harmonisée dans les différents domaines ainsi qu'une compréhension mutuelle de leurs fonctions, processus, exigences et interfaces sont impératives pour pouvoir créer un environnement sûr.

(2) La mise en réseau requise et l'échange de données nécessaire entre les différents éléments rendent indispensables une définition et une connaissance claires des principes et des exigences régissant tous les éléments. Il est par conséquent impératif de porter un regard global sur l'ensemble de l'environnement ICS ainsi que sur les environnements voisins, afin d'identifier et de décrire avec précision les frontières de chacun et les jonctions nécessaires. C'est le seul moyen de garantir une protection de l'environnement ICS complète et adaptée aux besoins.

b) Des zones communes structurées

(1) La mise en place d'une stratégie de défense en plusieurs strates nécessite une bonne compréhension de la façon dont les environnements et leurs éléments périphériques s'imbriquent les uns dans les autres et dont ils sont interconnectés. La répartition en différents secteurs des architectures communes de systèmes de contrôle peut aider l'entreprise à établir des limites claires en vue de mettre effectivement en œuvre sa stratégie de défense sur plusieurs niveaux. Les modes possibles de segmentation du réseau et de constitution d'interfaces à définir doivent être limpides. Il est indispensable pour cela de déterminer une structure d'aires, de zones et de secteurs.

(2) L'environnement dans son ensemble peut en principe être divisé en trois domaines administratifs/aires administratives de sécurité:

Domaines de sécurité/aires	Explication/description
I. Aire de sécurité externe (external security area)	Aire de sécurité des partenaires et environnements de travail externes. Elles sont soumises aux exigences et aux directives de sécurité des différentes parties concernées.

Domaines de sécurité/aires	Explication/description
II. Aire de sécurité de l'entreprise (enterprise business security area)	L'aire de sécurité de l'entreprise contient les connexions à Internet, aux sites de l'entreprise, aux installations de sauvegarde ou distantes (DMZ Internet, secteur E5), aux réseaux d'entreprise, aux communications de l'entreprise, aux serveurs de messagerie électronique, aux serveurs DNS (Domain Name System) et aux systèmes d'affaires IT (secteur E4). Le nombre important de systèmes et de connexions génère une multiplicité de risques dans cette zone, qui doit donc être considérée comme non fiable au regard de la sécurité de l'environnement ICS.
III. Aire de sécurité des processus de production (process manufacturing security area)	Aire de sécurité de la zone de production et de contrôle-commande, regroupant les technologies opérationnelles (OT). Cette zone rassemble l'environnement ICS et les infrastructures critiques en matière d'approvisionnement, telles que les installations de distribution (postes de transformation, installations de couplage, sous-stations) et de production (centrales électriques).

Tableau 6 Vue d'ensemble des trois domaines administratifs/aires administratives de sécurité

(3) L'aire dédiée à la production et au contrôle-commande (process manufacturing area) est divisée en une zone centrale et une zone décentralisée.

Sous-domaines/zones	Explication/description
Zone de sécurité SCADA /centre de contrôle	Cette zone de sécurité répond aux exigences de sécurité des systèmes de contrôle centralisé SCADA. Les secteurs correspondants (P2, 1 et E2) contiennent la zone des connexions, dans laquelle se déroulent une large majorité des opérations de surveillance et de contrôle sur l'ensemble des commandes de production et de réseau. Cette zone revêt une importance critique pour la continuité et l'administration d'un réseau de contrôle. Elle accueille également des appareils de soutien opérationnel et de gestion en ingénierie, ainsi que des serveurs de collecte et des archives de données. Son degré de criticité est très élevé. Les risques et les dangers résultent de sa connexion directe à des systèmes ou réseaux externes.
Zone de sécurité critique en matière d'approvisionnement	Cette zone de sécurité est associée aux installations critiques en matière d'approvisionnement (centrales électriques, postes de transformation, etc.). Elle contient des systèmes servant à la commande locale ou distante de domaines et d'installations comme des appareils de contrôle-commande de terrain, des éléments de commande IHM locaux, des contrôleurs locaux et leurs éléments de commande, et des dispositifs d'entrée/sortie de base, comme des actionneurs ou des capteurs. Le degré de criticité de cette zone est élevé, car elle pilote les terminaux physiques. Dans le réseau d'un système de contrôle-commande moderne, ces composants sont interconnectés grâce au protocole TCP/IP (Transmission Control Protocol/Internet Protocol) ou d'autres protocoles courants. Cette zone abrite également des systèmes de protection (SIS), qui doivent être connectés à d'autres systèmes de protection d'autres installations. Dans l'idéal, les appareils de protection sont isolés sur un réseau séparé afin de préserver les fonctions de protection en cas d'intervention sur le réseau ICS primaire. Les compromis sur ce point sont cependant fréquents.

Tableau 7 Sous-domaines centralisé et décentralisé de l'aire dédiée aux processus de production (process manufacturing area)

(4) Chacune de ces zones nécessite une approche ciblée spécifique en matière de sécurité. Une analyse par couches successives permet d'établir qu'un intrus cherchera en premier lieu à atteindre les éléments centraux des secteurs 1, P2, P3, P4 et P5 (voir tableau 12), car c'est là qu'il pourrait provoquer les dommages les plus importants. Ces secteurs doivent donc se voir attribuer le degré de criticité le plus élevé et/ou requièrent une protection maximale. En général, les tentatives visent à prendre le contrôle total des services centraux et de la commande des installations correspondantes. Une manipulation des ressources en informations de l'ICS pourrait menacer l'existence d'une entreprise lorsque cette zone critique est compromise.

(5) Dans un scénario d'attaque, l'intrusion commence à n'importe quel moment à l'extérieur des secteurs clés ou de contrôle. Le cyberpirate tente, par différents moyens, de s'introduire toujours plus profondément dans l'architecture. Les architectures étagées à plusieurs niveaux disposant de jonctions et d'interfaces contrôlées peuvent compliquer considérablement les intrusions dans les secteurs clés, voire les empêcher complètement. Les jonctions surveillées et contrôlées offrent aux administrateurs système des possibilités supplémentaires pour contrôler les informations et les ressources. Il est en outre possible de mettre en place des contre-mesures automatisées qui n'entravent pas obligatoirement l'activité de l'entreprise.

(6) La prise en compte des spécificités du lieu est à mettre en relation directe avec la protection physique des éléments. L'organisation de cette dernière, y compris la protection de l'accès aux différents éléments, influe directement sur les mesures à prendre. Une délimitation parfaite et une protection maximale permettent de réduire considérablement les mesures supplémentaires de protection et de durcissement dans ce domaine. L'approche consistant à viser une protection de base maximale est celle adoptée par le NERC. Cette protection doit donc se voir accorder une importance majeure dans l'évaluation du degré de criticité.

c) Segmentation horizontale en secteurs fonctionnels

(1) Les différents secteurs constituant la cartographie des systèmes permettent d'établir des délimitations par fonction/fonctionnalité et tâches. La cartographie des secteurs peut ainsi être subdivisée de la façon suivante:

Secteur	Description
Externe	Postes de travail externes et systèmes des fournisseurs, des fabricants et des personnes en charge du support IT. Inclut également le bureau à domicile et les accès à distance par Internet, ainsi que les services de cloud.
Internet	Internet, réseaux publics ainsi que leurs fournisseurs/prestataires de services et leurs composants. L'accent est mis sur la transmission pure de données via Internet.
DMZ Internet	Zone démilitarisée permettant de séparer les différents réseaux de façon sûre.
Activité de l'entreprise	Secteur abritant l'ensemble des applications et des services métier, comme p. ex. les applications bureautiques et les systèmes GIS, ERP ou de gestion de l'énergie.
DMZ OT/IT du SCADA	La zone démilitarisée joue un rôle de tampon entre les univers IT et OT, et permet un échange sécurisé d'informations selon des règles clairement définies.
SCADA/ centre de contrôle	Regroupe tous les systèmes centraux nécessaires à la commande et à la surveillance centralisées du réseau électrique et de la production.

Secteur	Description
DMZ frontale du SCADA	Zone démilitarisée permettant de séparer les différents réseaux de façon sûre, sur laquelle débouchent les connexions entre installations et passerelles. Il s'agit habituellement de systèmes front-end ou de systèmes de couplage de processus.
WAN (wide area network)	Réseau étendu: switchs, routeurs et multiplexeurs de données permettant la transmission des signaux de données entre les différents sites. Comprend également le support physique (fibre optique, cuivre ou ondes radio).
IHM locale	Interface homme-machine permettant l'utilisation protégée de toute l'installation locale critique en matière d'approvisionnement. La connexion à la passerelle ou à l'installation s'effectue habituellement via la norme CEI 60870-5-104 et/ou la norme CEI 61850.
Contrôleurs	Contrôleurs de terrain destinés aux technologies de processus et de protection, reliés ensemble par une interface TCP/IP. Actionneurs et capteurs directement connectés à un contrôleur de terrain via une interface TCP/IP. Passerelle du contrôle-commande de la station. Habituellement, norme CEI 60870-5-104 et/ou norme CEI 61850.
Appareils de terrain	Actionneurs et capteurs raccordés au contrôleur de terrain à l'aide d'un bus de terrain local, d'un bus spécifique au fabricant ou d'autres bus similaires. Connexion sans IP.
Activité extérieure	Applications métier connexes dans les installations critiques en matière d'approvisionnement.

Tableau 8 Segmentation horizontale par secteurs fonctionnels

d) Évaluation des différents éléments/détermination de la distance à Internet

(1) En raison des exigences accrues en matière de mise en réseau et de la complexité grandissante, il est impératif de définir, d'évaluer, de rassembler et/ou de regrouper les différents éléments au sein de la cartographie des systèmes, ce qui permet de représenter la complexité de l'ensemble de manière schématique et logique. L'évaluation des différents éléments nécessite en outre une classification supplémentaire de ces derniers.

(2) Il importe de considérer la cartographie des systèmes dans sa totalité. Il faut prendre en compte tous les éléments qui, d'une manière ou d'une autre, communiquent avec un élément de l'environnement ICS ou qui peuvent y être rattachés. Cela concerne également les serveurs de correctifs et de mises à jour des fournisseurs, les accès à distance des collaborateurs et des fournisseurs, etc. Le graphique ci-dessous présente une configuration idéale.

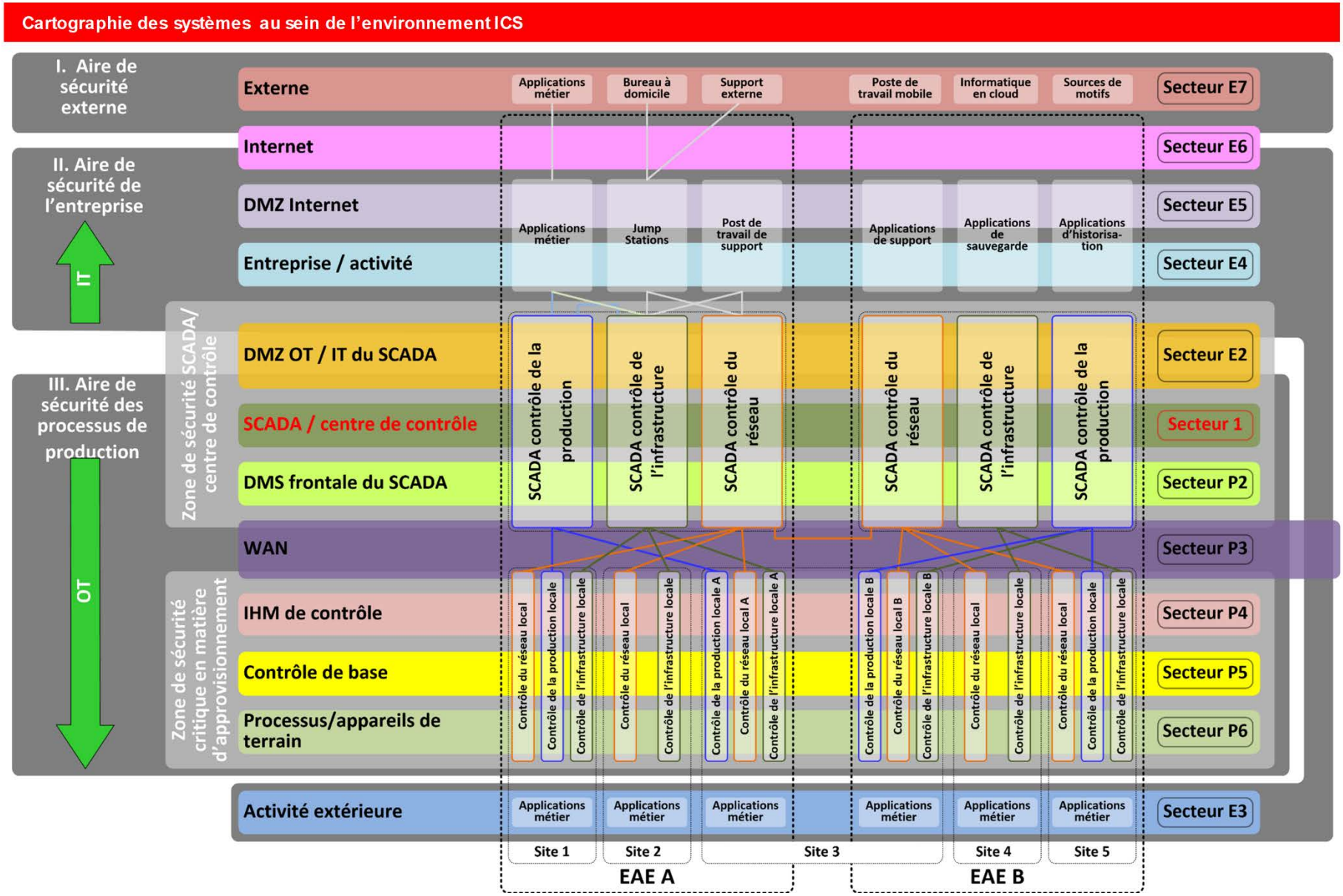

Figure 12 Cartographie des systèmes au sein de l'environnement ICS

e) Description des différents secteurs de sécurité et attribution d'un degré de criticité/distance à Internet requise

Secteur	Désignation	Degré de criticité	Distance à Internet requise
E7	Externe	Non concerné	La distance et/ou l'isolation par rapport à Internet est définie par l'organisation externe. Ce secteur doit être considéré comme non sûr pour l'environnement ICS, même si des connexions durcies et cryptées ont été établies entre eux.
E6	Internet	Non concerné	Internet est considéré comme la plus importante source de risques d'attaques potentielles pour l'environnement ICS. Aucune connexion directe n'est donc autorisée dans ce secteur, qui ne doit accueillir aucun élément disposant d'un accès direct à l'environnement ICS. Les connexions établies par le biais de ce secteur nécessitent obligatoirement une protection (disponibilité, confidentialité et intégrité des informations).
E5	DMZ Internet	Non concerné	La DMZ Internet de l'informatique d'entreprise/de la Business IT marque la fin de toutes les connexions entrantes et sortantes à Internet. Elle fait appel à des systèmes proxy et des passerelles de la couche application. Les transferts de données doivent en outre déboucher sur une DMZ de données. Ce secteur doit être le lieu du premier contrôle visant à détecter les maliciels ou autres logiciels malveillants. La définition et l'ampleur de ce contrôle sont soumises aux prescriptions des IT opérationnelles et de leurs systèmes.
E4	Activité de l'entreprise	Non concerné	Ce secteur est soumis aux directives et aux exigences relatives à la sécurité et à la protection de l'informatique d'entreprise/de la Business IT. Il doit cependant être considéré comme non sûr pour l'environnement ICS, car il se rapproche toujours plus d'Internet. L'intégration de services de cloud, les correctifs permanents, mais également les connexions directes à Internet via un navigateur confèrent à ce secteur un niveau d'insécurité très élevé pour l'ICS. Il fait également office de vecteur de nombreuses attaques visant l'environnement ICS, car il peut servir de maillon intermédiaire pour accéder à ce dernier.
E2	DMZ OT/IT du SCADA	3	Ce secteur constitue une jonction sûre entre les environnements non sécurisés des applications informatiques d'entreprise/métier, et assure également les connexions nécessaires à des tiers via Internet ou directement à Internet. Toutes les connexions possibles doivent donc déboucher sur ce secteur. Les transferts de fichiers nécessaires doivent y aboutir et il doit accueillir les contrôles requis contre les risques potentiels. Ce secteur constitue ainsi la dernière possibilité de contrer une attaque potentielle ou l'intrusion d'un logiciel malveillant.

Secteur	Désignation	Degré de criticité	Distance à Internet requise
1	Centre de contrôle SCADA	5	Secteur comportant le plus d'éléments à protéger. Les connexions qui peuvent y être établies doivent obligatoirement déboucher sur la DMZ correspondante ou être interrompues par cette dernière. Dans tous les cas, l'importation de fichiers ou l'échange automatique de données ne peuvent s'effectuer que par les voies prédéterminées et avec les contrôles et les terminaisons définis. Ce secteur doit observer la plus grande distance possible avec Internet.
P2	SCADA	4	Ce secteur accueille la connexion des installations critiques en matière d'approvisionnement au système SCADA. Les systèmes front-end ou de couplage de processus font ici office de séparation entre les deux zones de sécurité. Le principal défi dans ce secteur réside dans la jonction protégée entre les installations critiques en matière d'approvisionnement et le système SCADA: celle-ci doit impérativement être dotée de restrictions et avoir subi un durcissement adéquat. Tout doit avoir été mis en œuvre pour empêcher un éventuel cyberpirate de s'introduire dans le SCADA central via cette connexion. Une isolation entre les connexions servant au raccordement des différentes installations critiques en matière d'approvisionnement doit par ailleurs avoir été mise en place. Il faut veiller à ce qu'une connexion ne puisse être établie entre ces installations via ce secteur.
P3	WAN	4	Ce secteur requiert une isolation importante des connexions. Celle-ci peut être mise en place sans grandes difficultés sur les WAN classiques. Les connexions à prendre en charge doivent être cryptées. Il est recommandé de chiffrer tous les transferts de données de manière globale, la gestion des éléments étant elle aussi transmise de manière cryptée. Les jonctions entre les différentes connexions doivent être évitées, ce qui implique d'envisager l'isolation sur l'ensemble du WAN.
P4	IHM locale	3	Au sein d'une installation critique en matière d'approvisionnement, ce secteur pose des exigences spécifiques en termes de protection des éléments, car le facteur humain exerce une influence importante sur l'ensemble du système. La création d'un secteur dédié et la mise en place des jonctions nécessaires permettent de surveiller, de contrôler et, le cas échéant, de bloquer les processus.

Secteur	Désignation	Degré de criticité	Distance à Internet requise
P5	Contrôleurs	3	Ce secteur abrite le réseau de processus local et les contrôleurs correspondants. Dans l'idéal, il propose une segmentation par fonction. Les connexions à d'autres réseaux doivent être restreintes et paramétrées de façon à pouvoir être surveillées, contrôlées et, si nécessaire, bloquées.
P6	Appareils de terrain	2	Ce secteur peut accueillir des éléments disposant d'une protection physique inadaptée ou insuffisante (poste en plein air, coffret extérieur, etc.). Les raccordements aux contrôleurs ou aux technologies de processus locales doivent donc s'effectuer par le biais de connexions qui ne sont pas directement reliées au réseau de processus local (connexions sans IP ou via des réseaux isolés et cloisonnés). Aucune jonction IP avec le réseau de processus n'est autorisée.
E3	Activité extérieure	Non concerné	Ce secteur accueille des applications métier connexes dans les installations critiques en matière d'approvisionnement. Son fonctionnement doit être isolé des autres secteurs. L'interface ou la jonction doit s'effectuer via le secteur P3 «WAN» vers le secteur E4 «Activité de l'entreprise». Les connexions nécessaires doivent toujours emprunter le biais du secteur E4. Les exigences de sécurité dans ce domaine relèvent de la responsabilité de l'informatique d'entreprise.

Tableau 9 Degré de criticité des différents secteurs de sécurité

(3) Comme pour le degré de criticité, on distingue les niveaux suivants, conformément à la norme CEI 62443-3-2:

Appréciation du degré de criticité selon la norme CEI 62443-3-2				
Insignifiant	Insignifiant	Insignifiant	Insignifiant	Insignifiant
1 ●	1 ●	1 ●	1 ●	1 ●

Tableau 10 Appréciation du degré de criticité selon la norme CEI 62443-3-2

(4) Compte tenu de ces éléments, le secteur 1 est celui qui nécessite le niveau de protection de plus élevé (voir colonne Degré de criticité, tableau 9).

f) Regroupement vertical par sites, compétences, fonctions et processus

(1) Les installations critiques en matière d'approvisionnement étant contrôlées et surveillées par divers systèmes spécifiques à leurs fonctions et à leurs processus et dont la responsabilité est confiée à différents domaines de l'entreprise ou à différentes entreprises, il s'avère nécessaire de procéder à un regroupement vertical de la cartographie des systèmes.

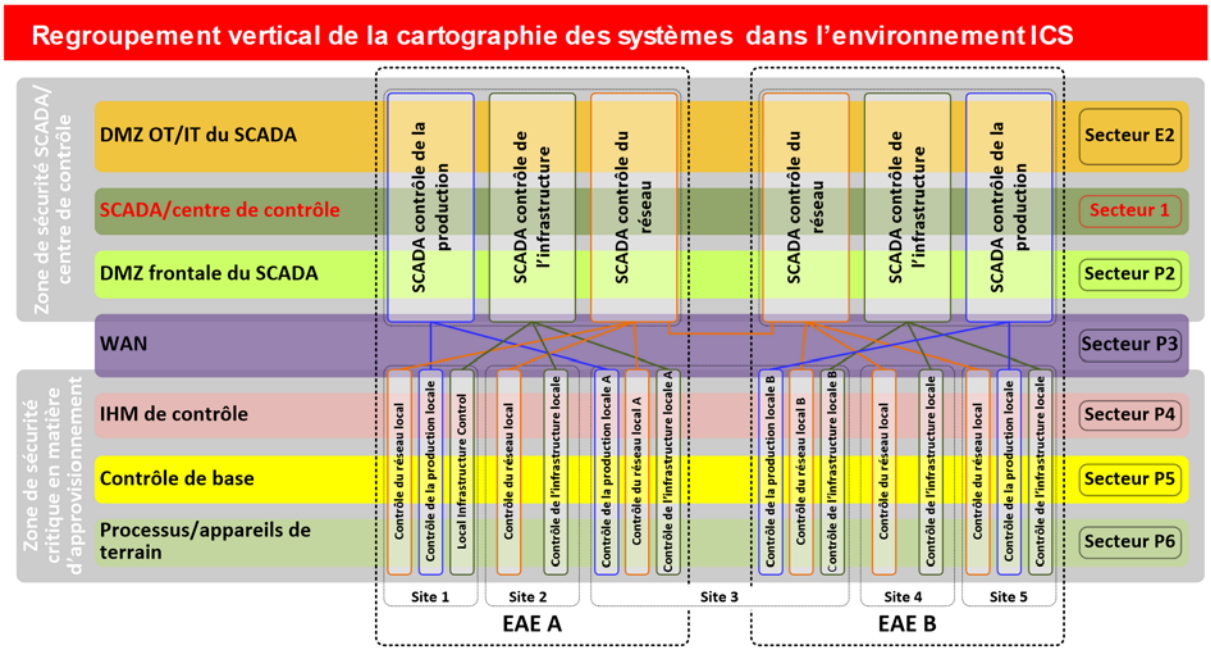

Figure 13 Regroupement vertical de la cartographie des systèmes dans l'environnement ICS

(2) Comme on le voit sur l'illustration ci-dessus, il est nécessaire de regrouper et de délimiter clairement les différents éléments fonctionnels et organisationnels. La mise en réseau des différents éléments peut générer un risque accru et une vulnérabilité importante. Les jonctions entre les différents éléments doivent être définies et dotées de la protection nécessaire. Il suffit d'une seule jonction non protégée pour connecter deux réseaux fonctionnels et ainsi les affaiblir.

2.7.2 Regroupement d'éléments en zones de réseau

(1) Chaque élément de l'environnement ICS doit en principe être étudié et examiné plus en détail. Il convient notamment d'identifier quels éléments doivent échanger leurs données avec quels autres éléments. Il convient à cet effet de procéder à un examen global, c.-à-d. que toutes les connexions possibles depuis et vers un élément doivent être connues. Chacun des éléments doit pour cela faire l'objet d'un inventaire. Une matrice permet enfin de déterminer comment les différents éléments doivent être regroupés, segmentés ou isolés. On tiendra compte pour ce faire de la protection physique dont dispose l'élément concerné, des types d'interfaces de communication existantes (p. ex. Ethernet, série, sans fil, etc.) et de la façon dont sont gérés ces systèmes (application des mises à jour, lecture des fichiers journaux, modification des configurations). Tous les éléments de l'environnement ICS doivent en premier lieu faire l'objet d'un durcissement ciblé

selon les connaissances et les besoins (pour de plus amples informations, veuillez vous reporter à la section «Sécurité des systèmes et des composants»).

(2) Le regroupement et la segmentation doivent être effectués selon les facteurs et les caractéristiques suivantes:

- Quels éléments offrent quelle protection physique; lesquels disposent d'une bonne protection physique permettant d'empêcher tout accès physique non autorisé au système?
- Quels éléments possèdent une fonction centrale; à quel niveau les éventuels cyberpirates ou logiciels malveillants peuvent-ils provoquer les dégâts les plus importants?
- Quels éléments ont subi un durcissement; de quelle protection dispose-t-on contre les erreurs de manipulation potentielles et l'intrusion de logiciels malveillants?
- Quels éléments doivent pouvoir établir des connexions avec quels autres éléments dans le cadre de leur fonctionnement?
- Où est-il pertinent de créer des jonctions entre éléments de façon à permettre les contrôles de sécurité, les isolations et les restrictions?
- Quels éléments peuvent être dotés d'outils de contrôle, d'isolation et de restriction?
- Quels éléments constituent des points centraux et par conséquent critiques, présentant un risque potentiel de vulnérabilité de l'ensemble du système?
- Quel cycle de correctifs et de mises à jour s'applique à quels éléments?

a) Regroupements dans la zone de sécurité SCADA/centre de contrôle et établissement d'une matrice de connexion interne

(1) La zone de sécurité SCADA/centre de contrôle est celle qui pose les exigences les plus élevées en termes de sécurité. C'est celle où l'intrusion d'un cyberpirate ou d'un logiciel malveillant peut entraîner les conséquences les plus lourdes. Différents facteurs doivent être pris en compte pour la mise en place de regroupements et de segmentations. Il importe de considérer l'environnement de cette zone dans sa totalité.

(2) Le regroupement et la segmentation peuvent être effectués comme dans la figure 12, fournie à titre d'exemple. Les rubriques peuvent bien entendu varier, et doivent être définies en fonction des prescriptions et des analyses applicables.

(3) Une fois le regroupement et la segmentation effectués, il est judicieux d'établir pour chaque secteur une matrice de connexion locale prenant en compte toutes les connexions rencontrées dans les différents groupes et segments.

Exemple de matrice de connexion interne pour le secteur E2 DMZ OT/IT du SCADA

De \ Vers	Serveur de fichiers 1	Serveur de fichiers 2	Jump server 1	Jump server 2	Serveur d'historisation	Serveur d'antivirus et de correctifs	Serveur de fichiers sécurisé
Serveur de fichiers 1	x	TCP/22 TCP/443	TCP/22 TCP/443	TCP/22 TCP/443	Non	Non	Non
Serveur de fichiers 2	TCP/22 TCP/443	x	TCP/22 TCP/443	TCP/22 TCP/443	Non	Non	Non
Jump server 1	TCP/22 TCP/443	TCP/22 TCP/443	x	TCP/22 TCP/443	TCP/22 TCP/443	TCP/22 TCP/443	TCP/22 TCP/443
Jump server 2	TCP/22 TCP/443	TCP/22 TCP/443	TCP/22 TCP/443	x	TCP/22 TCP/443	TCP/22 TCP/443	TCP/22 TCP/443
Serveur d'historisation	TCP/22 TCP/443	TCP/22 TCP/443	Non	Non	x	TCP/22 TCP/443	Non
Serveur d'antivirus et de correctifs	Non	Non	Non	Non	Non	x	Non
Serveur de fichiers sécurisé	Non	Non	Non	Non	Non	Non	x

Figure 14 Exemple de matrice de connexion interne pour le secteur E2 DMZ OT/IT du SCAD

(4) Comme le montre l'exemple ci-dessus, il faut dresser un inventaire des connexions requises entre les différents éléments d'un secteur donné. Chacune des connexions doit être décrite et son fonctionnement doit être connu. Il convient à cet égard de veiller impérativement à l'emploi systématique de protocoles sécurisés. On recourra en outre à des protocoles et à des structures de données pouvant être interrompus par ou déboucher sur les composants de contrôle et de surveillance nécessaires, comme un pare-feu de la couche application (application layer firewall, ALF) ou une passerelle de la couche application (application layer gateway, ALG), et permettant de vérifier le contenu des données à transmettre. Cette matrice de connexion doit bien entendu correspondre à la structure horizontale de chaque environnement ICS, comme le contrôle du réseau, le contrôle de la production et le contrôle de l'infrastructure. Les connexions entre secteurs ne sont volontairement pas encore abordées dans la présente section.

b) Regroupements au sein d'installations critiques en matière d'approvisionnement

(1) Comme décrit au point précédent, une matrice de connexion décrivant les connexions nécessaires doit également être créée par secteur pour les installations critiques en matière d'approvisionnement. Chaque matrice se limitera au secteur concerné. La matrice de connexion devra non seulement mentionner les connexions TCP/IP ou UDP/IP, mais également décrire et recenser les connexions sans IP et celles respectant des normes spécifiques (p. ex. GOOSE dans le cas de la norme CEI 61850). Seule cette procédure permet une prise en compte définitive et intégrale des éléments du secteur.

Matrice de connexion interne pour le secteur P5 «Contrôle de base» dans une installation critique en matière d'approvisionnement

De \ vers	Passerelle vers terrain	Passerelle vers protection	Passerelle vers IHM	Appareil de terrain 1 vers terrain	Appareil de terrain 2 vers terrain	Contrôleur de terrain 1 vers terrain	Contrôleur de terrain 2 vers terrain	Capteur de terrain 1 vers terrain	Capteur de protection 1 vers protection	Capteur de protection 2 vers protection	Protection Field Controller 1 vers protection	Protection Field Controller 2 vers protection	IHM locale vers IHM
Passerelle vers terrain	x	Non	Non	TCP/102 UDP/123	TCP/102 UDP/123	TCP/102 UDP/123	TCP/102 UDP/123	TCP/102 UDP/123	Non	Non	Non	Non	Non
Passerelle vers protection	Non	x	Non	Non	Non	Non	Non	Non	TCP/102 UDP/123	TCP/102 UDP/123	TCP/102 UDP/123	TCP/102 UDP/123	Non
Passerelle vers IHM	Non	Non	x	Non	Non	Non	Non	Non	Non	Non	Non	Non	TCP/102 UDP/123
Appareil de terrain 1 vers terrain	TCP/102 UDP/123	Non	Non	x	TCP/102 UDP/123	TCP/102 UDP/123	TCP/102 UDP/123	TCP/102 UDP/123	Non	Non	Non	Non	Non
Appareil de terrain 2 vers terrain	TCP/102 UDP/123	Non	Non	TCP/102 UDP/123	x	TCP/102 UDP/123	TCP/102 UDP/123	TCP/102 UDP/123	Non	Non	Non	Non	Non
Contrôleur de terrain 1 vers terrain	TCP/102 UDP/123	Non	Non	TCP/102 UDP/123	TCP/102 UDP/123	x	TCP/102 UDP/123	TCP/102 UDP/123	Non	Non	Non	Non	Non
Contrôleur de terrain 2 vers terrain	TCP/102 UDP/123	Non	Non	TCP/102 UDP/123	TCP/102 UDP/123	TCP/102 UDP/123	x	TCP/102 UDP/123	Non	Non	Non	Non	Non
Capteur de terrain 1 vers terrain	TCP/102 UDP/123	Non	Non	TCP/102 UDP/123	TCP/102 UDP/123	TCP/102 UDP/123	TCP/102 UDP/123	x	Non	Non	Non	Non	Non
Capteur de protection 1 vers protection	Non	TCP/102 UDP/123	Non	Non	Non	Non	Non	Non	x	TCP/102 GOOSE	TCP/102 GOOSE	TCP/102 GOOSE	Non
Capteur de protection 2 vers protection	Non	TCP/102 UDP/123	Non	Non	Non	Non	Non	Non	TCP/102 GOOSE	x	TCP/102 GOOSE	TCP/102 GOOSE	Non
Protection Field Controller 1 vers protection	Non	TCP/102 UDP/123	Non	Non	Non	Non	Non	Non	TCP/102 GOOSE	TCP/102 GOOSE	x	TCP/102 GOOSE	Non
Protection Field Controller 2 vers protection	Non	TCP/102 UDP/123	Non	Non	Non	Non	Non	Non	TCP/102 GOOSE	TCP/102 GOOSE	TCP/102 GOOSE	x	Non
IHM locale vers IHM	Non	Non	TCP/102 UDP/123	Non	Non	Non	Non	Non	Non	Non	Non	Non	x

Figure 15 Matrice de connexion pour le secteur P5 dans une installation critique en matière d'approvisionnement

2.7.3 Gestion de réseau, inventaire et performances

(1) La gestion de réseau – également appelée administration de réseau – constitue un préalable indispensable au fonctionnement sûr et fiable d'un réseau. En raison de la complexité des réseaux de grande envergure, le système de gestion doit prendre en charge diverses fonctions de contrôle, de surveillance et de configuration des chemins. Parmi les tâches relevant de la gestion de réseau figurent ainsi, entre autres, la collecte d'informations sur l'utilisation du réseau par les éléments qui y sont raccordés, l'établissement de rapports et de statistiques à des fins de planification, d'exploitation, de réparation et de maintenance, la configuration du réseau et les modifications de configuration qui en découlent, et la surveillance des performances, des événements et des erreurs. L'Organisation internationale de normalisation (ISO) a défini cinq domaines fonctionnels relevant de la gestion de réseau et associés à la communication ouverte: la gestion des erreurs, la gestion des performances, la gestion de la configuration, la gestion de la comptabilité et la gestion de la sécurité.

- La gestion des erreurs regroupe toutes les fonctions pouvant servir à prévenir, à détecter et à résoudre les erreurs sur le réseau.
- La gestion de la configuration rassemble les outils et les fonctions servant à la planification, à l'extension et à la modification de la configuration, ainsi qu'à la gestion des informations de configuration.
- La gestion des performances fournit des outils et des instruments permettant de mesurer et d'améliorer les performances du réseau, ce qu'on appelle la «mise au point» («tuning») du réseau.
- La gestion de la comptabilité propose des moyens en vue du traitement conforme aux dispositions légales de l'utilisation du réseau, comme la gestion des accès, le contrôle des utilisateurs, des aides à la facturation et des services d'information.
- La gestion de la sécurité est chargée de surveiller les autorisations d'accès aux réseaux, aux segments de réseaux locaux, aux éléments, aux services et à d'autres ressources.

Inventaire du réseau

(1) Avant d'«administrer» le réseau, il convient de recenser au préalable l'ensemble de ses éléments et composants. Cette tâche peut être effectuée de manière automatique par un logiciel dit «d'inventaire», qui enregistre non seulement l'existence de divers appareils à l'aide des adresses IP actives via la commande PING, mais consigne aussi différentes informations concernant chaque élément dans une base de données. Pour un ordinateur client, il peut s'agir par exemple de données sur le matériel, sur le système d'exploitation, mais également sur les logiciels installés. Une vue d'ensemble complète des programmes installés revêt une importance déterminante pour une parfaite gestion des licences.

(2) Si l'inventaire des éléments du réseau et des terminaux raccordés est essentiel, il convient aussi de recenser et d'inventorier les connexions possibles et nécessaires (p. ex. connexions TCP/IP) sur l'ensemble du réseau entre les différents éléments de ce dernier. Seule cette procédure permet de garantir une bonne compréhension du fonctionnement d'un réseau. Ces inventaires constituent également la base des éléments de sécurité requis. Les inventaires uniques d'un réseau sont intéressants en ce qu'ils proposent un état des lieux, mais ils ne constituent qu'un aperçu momentané. Il est donc recommandé d'inventorier le réseau en permanence ou de maintenir à jour les inventaires du réseau existants.

Garantie des performances

(1) Sur les réseaux modernes utilisés pour le trafic de données pur, mais également souvent pour la communication vocale (VoIP) ou pour des vidéoconférences, il n'est pas toujours aisé de fournir à tout moment les performances requises. Comparé à d'autres applications du réseau, le VoIP réagit avec une extrême sensibilité aux retards et aux pertes de paquets. Il est par conséquent nécessaire d'examiner les paramètres spécifiques au VoIP avant même l'installation pour pouvoir obtenir en pratique les valeurs voulues. Toutefois, pour pouvoir mesurer la performance VoIP d'un réseau d'entreprise, il faut impérativement vérifier la pertinence de celui-ci avant d'acquérir et d'installer des composants VoIP/UC tels que des téléphones, des serveurs et des passerelles. Cette opération peut être effectuée à l'aide de simulateurs et d'analyseurs VoIP capables d'imiter des milliers d'utilisateurs et leurs comportements en matière de téléphonie, et pouvant être intégrés progressivement au réseau.

(2) Les applications des systèmes SCADA et des infrastructures critiques dépendent souvent de données en temps réel. Les performances du réseau doivent donc être dimensionnées ou adaptées spécifiquement pour ces applications. Des facteurs, tels que la gigue et les temps d'exécution, jouent également un rôle important. Il convient par conséquent de veiller impérativement à ce que les paramètres requis en termes de temps réel, de gigue et de temps d'exécution soient respectés à tout moment, même lorsque le réseau est fortement sollicité par d'autres applications comme de la vidéo ou du VoIP. S'il existe une possibilité que le réseau existant soit confronté à des congestions, l'établissement de priorités peut constituer une bonne solution.

(3) L'évolutivité est aujourd'hui l'une des principales caractéristiques d'une infrastructure IT. Elle promet, par exemple, de garantir la disponibilité des applications et des services même si le trafic sur le réseau augmente sensiblement. Il est toutefois extrêmement complexe de déterminer le degré d'évolutivité d'un réseau existant, ou même tout simplement d'identifier où se situe le goulot d'étranglement en cas de forte sollicitation. Dans la pratique, les responsables IT recourent pour ce faire à des tests de sollicitation réalisés à l'aide d'outils qui créent une sollicitation artificielle sur le réseau local. Il ne suffit cependant pas d'injecter des volumes invraisemblables de données sur le réseau; les résultats de ces tests ne sont véritablement probants que s'ils sont associés aux mesures organisationnelles appropriées au sein de l'environnement.

Surveillance du réseau

(1) La surveillance du réseau et de ses différents composants, qui revêt une importance déterminante pour la détection et la résolution des erreurs, s'effectue le plus souvent par le biais des protocoles SNMP (Simple Network Management Protocol) ou WMI (Windows Management Instrumentation). La surveillance par des agents logiciels constitue une autre méthode très répandue pour se faire une idée de l'état de composants du réseau. Outre la gestion et la surveillance des composants, l'administration de réseau consiste également à contrôler les serveurs et les services fournis (serveurs web, serveurs de messagerie, etc.).

(2) Les administrateurs recourent souvent à des logiciels spécifiques pour la surveillance du réseau. Parmi les solutions open source les plus courantes figure Nagios, un programme Unix encore très largement répandu, mais qui n'est quasiment plus développé. De plus, bon nombre de ses fonctions sont disponibles uniquement grâce à des plug-ins; les outils relativement récents OpenNMS et Shinken sont donc de plus en plus fréquemment employés. Shinken s'appuie sur Nagios et définit ses fonctions de surveillance, tout comme son modèle, à l'aide de divers fichiers

de configuration. OpenNMS adopte au contraire une approche plus globale et propose un paramétrage de nombreuses tâches dès les réglages de base. Parmi les autres logiciels libres de gestion de réseau, on peut également citer Cacti, MRTG ou Zabbix.

(3) Divers produits commerciaux de surveillance de réseau sont en outre disponibles sur le marché, par exemple HP Open View, IBM Tivoli ou Microsoft Operations Manager, proposés par les principaux fournisseurs de solutions IT. Mais de petites entreprises, comme Ipswitch ou Paessler, ont elles aussi développé leurs propres produits, avec WhatsUp Gold et PRTG Network Monitor.

(4) Il importe d'appliquer les fonctions et exigences nécessaires en matière de sécurité, y compris dans la surveillance de réseau. Pour les cyberpirates potentiels, une gestion du réseau non dissociée de ce dernier offre une possibilité idéale d'entreprendre des manipulations et des actions dans les installations critiques en matière d'approvisionnement. La mise en œuvre du protocole SNMPv3 (Simple Network Management Protocol Version 3) et de connexions SSH est impérative. En cas d'emploi de protocoles propriétaires différents, on veillera impérativement à ce que l'intégrité et la protection des données soient garanties. Des techniques de cryptage et d'autres méthodes de protection doivent obligatoirement être utilisées.

VLAN et VPN

(1) La gestion d'un réseau doit s'effectuer sur des réseaux dédiés cloisonnés. Pour la faciliter, on peut créer un VLAN (virtual local area network, réseau local virtuel), qui répartit les appareils d'un réseau local en groupes entre lesquels les connexions sont en principe impossibles, mais peuvent être autorisées de manière ciblée par un pare-feu ou une passerelle de la couche application (ALG). Le VPN (virtual private network, réseau privé virtuel) est utilisé systématiquement lorsqu'un réseau protégé contre les accès extérieurs doit être rendu accessible de façon sûre via des réseaux étrangers ou non fiables.

2.8 Sécurité du périmètre du réseau

(1) Dès lors qu'une entreprise a conçu et mis en place une architecture réseau solide, l'architecture de sécurité doit également être mise en œuvre pour le réseau et les systèmes. L'architecture de sécurité comprend les contrôles spécifiques et le positionnement stratégique de détecteurs et de sondes à l'intérieur du réseau ou des systèmes en vue de mettre en place les différentes strates de la défense en profondeur. Des diagrammes du réseau, des matrices de connexion et des diagrammes portant sur les flux d'information, qui permettent de mettre en relation tous les systèmes et leurs connexions avec l'inventaire physique, sont indispensables pour comprendre le fonctionnement des flux d'information et des connexions nécessaires au sein du réseau. La création d'aires, de zones et de secteurs et la superposition des niveaux de sécurité pour chaque système ou sous-système affecté durant l'inventaire permettent de déterminer les éléments de contrôle-commande et de surveillance mis en place pour protéger le système sans amoindrir les performances.

(2) Les administrateurs système doivent prendre en compte la mise en œuvre de contrôles de sécurité au niveau des couches réseau, système, application et physique pour pouvoir garantir la sécurité de l'information, ce qui inclut la gestion des directives et de la sécurité, la sécurité des applications, la sécurité des données, la sécurité des plateformes, la sécurité des réseaux et des périmètres, la sécurité physique et la sécurité des utilisateurs. L'architecture de sécurité consiste en un rassemblement de tous les mécanismes et contrôles de défense et en leur superposition à l'architecture du réseau. L'architecture de sécurité définit les situations où des mesures de défense

en profondeur doivent être appliquées dans l'ensemble de l'entreprise. Le document NIST 800-82 *Guide to Industrial Control Systems (ICS) Security* («Guide de la sécurité des systèmes de contrôle-commande industriels (ICS)») propose à cet égard une superposition des contrôles de sécurité des ICS à l'échelle de l'entreprise, en s'appuyant sur la norme NIST 800-53 *Security and Privacy Controls for Federal Information Systems and Organizations* («Contrôles de sécurité et protection de la vie privée pour les systèmes d'information et entreprises fédéraux»).

2.8.1 Principes pour la sécurisation des accès au réseau et des jonctions entre zones

(1) Au sein de l'environnement ICS, les architectures intégrées et l'interconnexion avec d'autres environnements créent des possibilités d'accès aux systèmes critiques. De par leurs propriétés, ces architectures nécessitent des échanges de données provenant de sources d'information différentes, ce qui peut être mis à profit par des intrus potentiels. La norme CEI 62443-3-2 «Sécurité des systèmes d'automatisation et de commande industriels – Évaluation des risques de sécurité et conception des systèmes» décrit cette problématique.

(2) Il convient d'appliquer les principes suivants:

- Un regroupement et une segmentation seront systématiquement effectués lorsque les connexions entre les éléments OT présentent un besoin de protection ou un niveau de criticité accru ou lorsqu'un contrôle s'avère nécessaire. Le regroupement et la segmentation visent à créer ainsi des jonctions et des interfaces vérifiables et contrôlables.
- On veillera à ce que toute connexion dans l'environnement OT soit établie à partir du secteur ou de l'élément présentant un besoin de protection ou un niveau de criticité supérieur.
- Dans la mesure du possible, des protocoles sécurisés seront mis en œuvre à l'intérieur des secteurs également.
- L'authentification MAC sera appliquée aux composants du réseau OT (switchs et routeurs).
- Le contrôle des flux et/ou la validation des connexions au niveau des couches 3 et 4 seront appliqués aux composants du réseau à l'aide de listes de contrôle d'accès.
- Les accès et tentatives d'accès non autorisés seront détectés et enregistrés et généreront un processus d'alerte et de transfert en escalade.
- Les ports non utilisés (accès et trunk) seront désactivés sur tous les éléments OT (réseau et hôtes).
- Les serveurs RADIUS et les serveurs de contrôle des systèmes de l'environnement OT destinés aux infrastructures critiques d'approvisionnement en électricité peuvent représenter un risque majeur. Leur mise en place et leur utilisation seront donc contrôlées avec précision et soumises à d'importantes restrictions. On évitera de les connecter au système de l'environnement IT.
- Les accès physiques seront contrôlés par une suppression des câbles de raccordement à la console ou par la mise en place d'une console protégée uniquement par mot de passe ou d'un accès virtuel au terminal soumis à des restrictions de temps et d'accès.
- On emploiera des liaisons 1-1 entre les sous-réseaux et les VLAN, ce qui nécessite la mise en place d'un pare-feu, d'un routeur ou de switchs multicouches pour connecter plusieurs VLAN. Bon nombre de routeurs et de pare-feux prennent en charge les cadres balisés, ce qui peut déboucher sur la création d'une interface physique unique entre plusieurs réseaux logiques.
- Il est recommandé de contrôler les accès aux VLAN à l'aide d'un pare-feu. On créera des comptes utilisateur basés sur les rôles pour tous les VLAN. On dressera une liste d'accès en vue de restreindre les accès de certains réseaux et hôtes à Telnet et à Secure Shell (SSH).

- On établira et on utilisera des listes de contrôle d'accès (ACL) de couche 2 (L2) et des ACL virtuelles permettant de bloquer la communication directe entre un cyberpirate potentiel et l'appareil attaqué au niveau de la couche 2. On mettra en œuvre davantage d'intelligence dans le réseau OT de façon à permettre la vérification de l'identité et de l'exactitude des paquets ARP (Address Resolution Protocol) transférés.
- On aura recours à des VLAN privés pour protéger les réseaux contre les accès indésirables d'appareils non fiables.
- On sécurisera les ports dans les éléments du réseau OT.
- Des contrôles des flux broadcast et multicast et des restrictions aux ports concernés des éléments du réseau OT seront mis en place.
- On isolera la gestion des composants du réseau OT au sein d'un VLAN isolé, ou on mettra en œuvre une administration «out of band» en lieu et place de l'administration «in band».
- Le nombre d'adresses MAC (media access control) employées par un seul et même port sera limité de façon à associer directement l'identification d'un appareil et le port d'origine. Les ports non utilisés seront désactivés, et les ports désactivés seront affectés à un VLAN non utilisé.
- On créera et on appliquera des ACL de couche 3 selon l'adresse IP (recommandée pour la plupart des réseaux filaires statiques), le filtrage de l'adresse MAC, l'affectation de ports, l'assignation dynamique (recommandée pour la plupart des réseaux sans fil et des réseaux de ports de commutateurs partagés), les protocoles et les applications. Par défaut, seuls les ports connus et fiables seront traités comme tels; tous les autres ports seront configurés comme non fiables, ce qui permet d'éviter les manipulations inadaptées des valeurs de qualité de service par les appareils connectés.
- Les protocoles VTP (VLAN Trunking Protocol) / MVRP (Multiple VLAN Registration Protocol) et DTP (Dynamic Trunking Protocol) seront désactivés sur tous les ports non fiables. Cette méthode éprouvée permet d'utiliser les VLAN à l'intérieur des réseaux OT, car elle peut restreindre (voire bloquer) les éventuelles interactions de protocole indésirables au sein des configurations VLAN à l'échelle du réseau. Cette mesure de précaution peut également limiter ou contrer le risque qu'une erreur de l'administrateur se propage à l'ensemble du réseau.

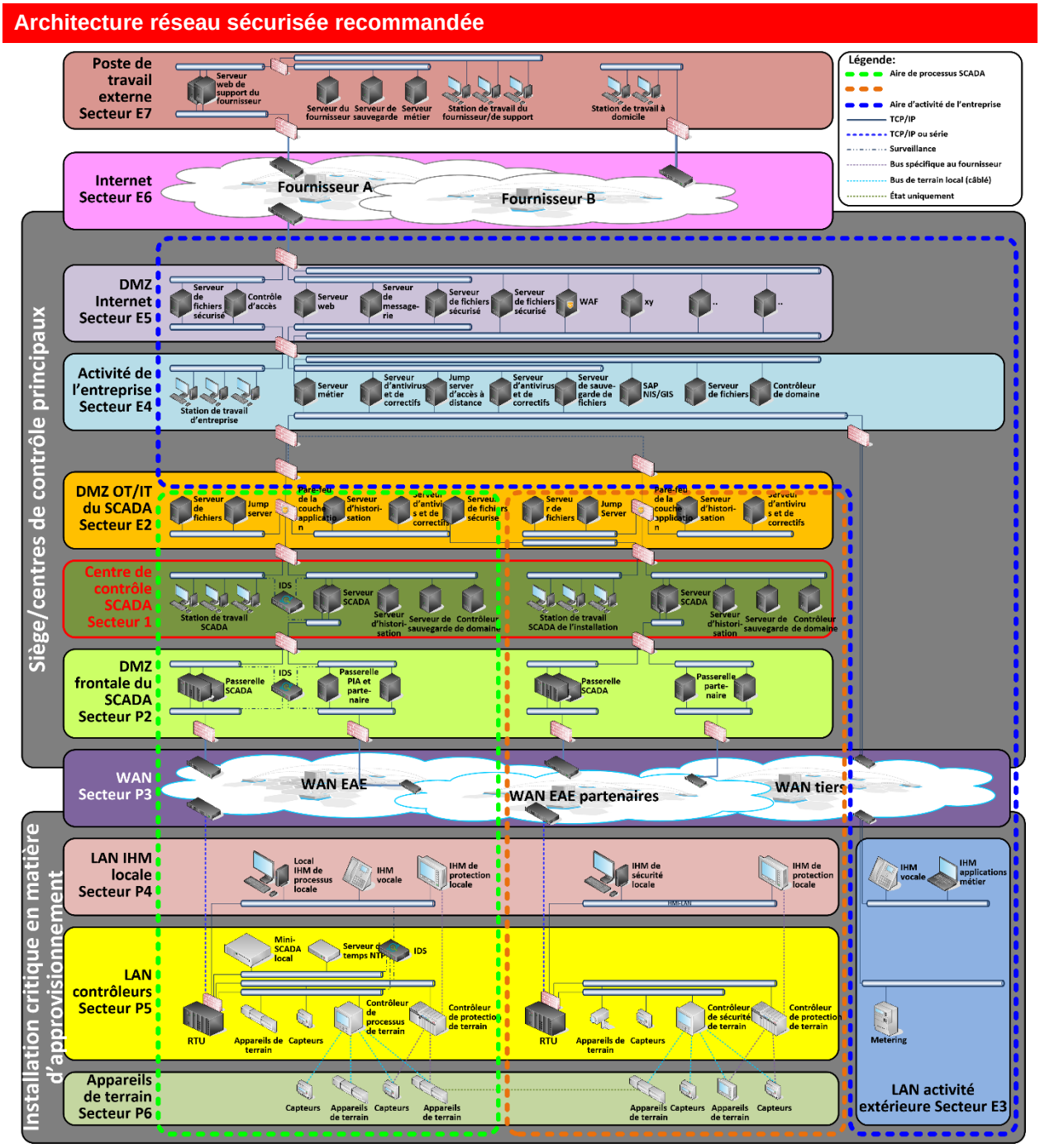

Figure 16 Architecture réseau sécurisée recommandée

(3) La sécurité du périmètre ICS inclut des contrôles de sécurité physique et logique visant à protéger les infrastructures présentes dans ce périmètre. À cet égard, il convient en premier lieu de définir où se situe la limite des communications. Pour cela, on procédera à une évaluation destinée à déterminer les points où les cybercriminels pourraient utiliser des vecteurs d'intrusion potentiels pour infiltrer le système ICS. La sécurité logique englobe des contrôles tels que des mécanismes d'authentification, des ACL à l'intérieur des composants du réseau, des signatures IDS/IPS (voir

tableau 11), des outils de surveillance et d'autres moyens visant à protéger les systèmes sur le plan logique. La sécurité physique du périmètre comprend tous les moyens visant à protéger les infrastructures physiques, comme p. ex. les cartes-clés servant à ouvrir les portes, les détecteurs de mouvement et les caméras ou les forces de sécurité.
Pour pouvoir mettre en place des réseaux sûrs, il est important de connaître les opérations, connexions, classes de protection et jonctions requises ainsi que les technologies utilisables. Les procédés techniques suivants permettent de créer des réseaux sécurisés:

Procédé	Description
Network access control	Le network access control (NAC, contrôle d'accès au réseau) est une technologie permettant de bloquer les accès non autorisés au réseau. Au moment de leur authentification, les terminaux font l'objet d'une vérification visant à établir leur conformité avec les directives. De nombreux appareils de réseau disposent de fonctionnalités NAC. Aujourd'hui, on recourt le plus souvent au contrôle des adresses MAC et IP. Les systèmes modernes font appel à des contrôles d'accès basés sur des certificats.
Segmentation du réseau Constitution de sous-réseaux	Le regroupement et la segmentation de réseaux commencent par la constitution de réseaux ou de sous-réseaux les plus petits possibles. Un segment de réseau doit conserver une envergure réduite, de façon à répondre uniquement aux exigences fonctionnelles nécessaires. Les réseaux de grande taille contenant de nombreux éléments accroissent le risque de propagation des maliciels, et offrent une marge de manœuvre accrue aux cyberpirates potentiels. Il convient de constituer de petits réseaux et sous-réseaux afin de créer des jonctions contrôlables.
LAN virtuels VLAN	Un VLAN (virtual local area network, réseau local virtuel) est un sous-réseau logique au sein d'un switch ou d'un réseau physique entier. Il peut s'étendre sur un ou plusieurs switchs. Un VLAN sépare des réseaux physiques en sous-réseaux en faisant en sorte que les switchs compatibles VLAN ne transmettent pas les trames (paquets de données) d'un VLAN à un autre VLAN (même si les sous-réseaux peuvent être raccordés à des switchs communs). Il est ainsi possible de réaliser une segmentation et un regroupement sur un réseau commun. Les VLAN débouchent sur des pare-feux ou des routeurs, lesquels établissent des jonctions contrôlées avec d'autres VLAN.
Routage	Le routage définit l'ensemble du trajet qu'emprunte un flux d'informations à travers le réseau; le réacheminement désigne en revanche le processus de décision par lequel un nœud donné choisit auquel de ses voisins il doit transférer un message. Le réacheminement et le routage sont toutefois fréquemment amalgamés sous la désignation de «routage»; ce concept désigne alors de manière générale la transmission de messages via les réseaux de communication. Contrairement aux répartiteurs (hubs et switchs), le routage fonctionne sans restriction, y compris sur les réseaux maillés. En technique de transmission, le terme de «gestion du trafic» désigne le choix des tronçons de route lors de l'établissement des liaisons de communication, choix qui peut s'effectuer en prenant en compte certains critères, comme p. ex. la plus courte distance. S'il s'agit d'une connexion par commutation de circuits, un canal de transmission est sélectionné pour toute la durée de la connexion, et toutes les informations sont transmises par le même chemin. S'il s'agit en revanche d'un transfert de données par paquets, chaque nœud du réseau redéfinit le trajet emprunté par chaque paquet.

Procédé	Description
Pare-feu	Un pare-feu est en principe mis en place entre deux segments de réseau. Il contrôle uniquement les connexions réseau entrantes et sortantes selon certaines règles et bloque les tentatives de communication jugées dangereuses. On emploie aussi parfois le terme de «filtre de paquets», car les données sont transmises sous forme de «paquets de données» sur le réseau. Les pare-feux opèrent une distinction en fonction de «zones» déterminées. Ainsi, le réseau local ou d'une entreprise peut être défini comme une «zone» sûre et/ou fiable, où les informations peuvent circuler librement, tandis qu'Internet est considéré comme une zone non sûre. Les pare-feux peuvent également traiter différemment certains programmes ou services. Dans ce cas, les programmes légitimes considérés comme sûrs sont autorisés à communiquer sans restriction avec les autres éléments du réseau, contrairement aux programmes inconnus susceptibles d'entrer dans la catégorie des logiciels malveillants. Certains serveurs – identifiables à leur adresse IP – peuvent eux aussi être définis comme sûrs ou non sûrs dans le pare-feu.
Zones démilitarisées (DMZ)	Une zone démilitarisée (parfois également appelée réseau de périmètre) est un sous-réseau physique et logique faisant office d'intermédiaire pour les dispositifs de sécurité raccordés, de façon à ce que ces derniers puissent être connectés à un réseau de plus grande envergure et non fiable, généralement le réseau de l'entreprise ou Internet. La DMZ ajoute une couche de sécurité supplémentaire au réseau local d'une entreprise. Ainsi, un intrus externe ne peut accéder directement qu'aux appareils situés à l'intérieur de la DMZ, et non aux autres parties du réseau, quelles qu'elles soient.
Cryptage, signatures et certificats	Pour sécuriser une connexion entre deux éléments, on recourt à des techniques de cryptage telles que le SSH (Secure Shell). SSH désigne aussi bien un protocole réseau que les programmes correspondants permettant d'établir en toute sécurité une connexion réseau cryptée avec un équipement distant. Une autre méthode, SSL/TLS, consiste à crypter les données à transmettre.
Diodes réseau	Les diodes réseau sont des éléments pouvant être branchés entre deux réseaux ou sous-réseaux afin de n'autoriser le transfert de données que dans une seule direction. Les données peuvent ainsi être transmises de façon sûre et fiable depuis des réseaux sécurisés vers des réseaux non sécurisés, sans nécessiter de canal retour susceptible de constituer une faille dans le réseau.
Convertisseur de protocole	Une méthode efficace pour sécuriser le transfert de données consiste à employer des convertisseurs de protocole. Un flux de données sur port est alors mis en œuvre de telle sorte que seules les données utiles réelles sont transmises. Le composant TCP-IP est supprimé en totalité, ce qui élimine par la même occasion les éventuelles vulnérabilités.

a) Contrôles d'accès au réseau

(1) Il existe des moyens simples permettant de limiter l'accès à un réseau ICS. L'authentification des adresses MAC peut déjà s'opérer sur les appareils L2 (encore appelés de couche 2). À cet effet, l'accès est accordé uniquement à des composants enregistrés et saisis. En outre, les contrôles d'accès et de flux de données peuvent être mis en œuvre dans les composants du réseau à l'aide de listes de contrôle d'accès (ACL ou DACL). Cette mise en œuvre est aisée étant donné que les réseaux ICS sont souvent statiques. Dans les réseaux classiques, les contrôles d'accès s'effectuent selon le protocole IEEE802.1x. Au sein de ces réseaux, on recourt fréquemment à des systèmes centraux, tels que des serveurs RADIUS et de contrôle, pour contrôler l'accès. Vu que l'on vise une segmentation et une délimitation claires entre les différents secteurs des réseaux ICS et que les serveurs RADIUS et de contrôle locaux y sont souvent dénués de sens, il faut se demander dans quelle mesure l'utilisation du protocole IEEE802.1x avec toutes les fonctions s'avère judicieuse. Il est de plus en plus fréquent que la connexion au réseau soit établie par le biais de certificats délivrés par les fabricants, ce qui offre un moyen supplémentaire de surveiller et de contrôler les accès.

(2) Les équipements réseau L2 actuels disposent de plusieurs fonctions capables de commander et de réguler l'accès au réseau. Étant donné que l'environnement ICS est plutôt statique et subsiste pendant une période relativement longue, les entrées et listes locales peuvent être tout à fait pertinentes sur les terminaux réseau respectifs. Il est ainsi possible d'éliminer également la vulnérabilité par le biais de serveurs RADIUS et de contrôle centraux.

(3) Les accès aux réseaux ICS doivent être enregistrés. Il faut de surcroît identifier et faire remonter les tentatives d'accès non autorisées. En cas de recours à un SIEM (security information and event management) central, on doit disposer de l'interface et de la connexion requises.

b) Segmentation du réseau / constitution de sous-réseaux

(1) Comme décrit dans les chapitres précédents, la bonne segmentation du réseau et la constitution de sous-réseaux constituent un acte fondamental et décisif. Les éventuelles connexions et communications entre les différents éléments de réseau ne doivent être autorisées que lorsque cela s'avère nécessaire. En outre, il faut répartir l'ensemble des réseaux en aires, zones et secteurs et créer les jonctions requises entre ces zones pour pouvoir procéder aux contrôles et vérifications qui s'imposent. Quoi qu'il en soit, il est impératif que toutes les connexions et communications possibles et nécessaires entre les divers éléments du réseau ICS soient connues et décrites.

c) LAN virtuels

(1) Un LAN virtuel (VLAN) divise les réseaux physiques en réseaux logiques plus petits constitués d'un seul domaine de broadcast qui isole la circulation des données des autres VLAN. L'utilisation de VLAN restreint le trafic de broadcast et permet aux sous-réseaux logiques d'englober plusieurs sites physiques.

(2) S'il semble opportun pour les professionnels de la sécurité d'être toujours au courant des dernières avancées techniques, on peut également leur conseiller de se pencher à nouveau sur les fondements de la sécurité des réseaux. Ou plus concrètement: les professionnels de la sécurité devraient envisager d'étoffer leurs connaissances sur des concepts tels que les local area networks virtuels (VLAN). Car il est parfaitement concevable que dans certaines situations, un VLAN

correctement configuré constitue le seul et unique obstacle entre l'environnement ICS et un intrus ayant jeté son dévolu sur ce dernier.

(3) Les VLAN existent depuis presque aussi longtemps que les commutateurs Ethernet. Dans une configuration VLAN type, chaque nœud d'un réseau est relié physiquement à un commutateur (ou switch) Ethernet. L'administrateur réseau configure le commutateur de façon à ce que certains ports soient segmentés pour des groupes déterminés. Chacun de ces groupements est appelé VLAN. Tous les membres d'un même VLAN peuvent communiquer entre eux sans devoir passer par d'autres équipements réseau, sauf dans les cas spécifiques où un VLAN s'étend sur au moins deux sites géographiques. Les réflexions qui sous-tendent cette segmentation de couche 2 varient. En matière de sécurité, elle offre à l'administrateur un moyen d'isoler son réseau des attaques d'initiés redoutées.

(4) Les VLAN présentent donc certains avantages en termes de sécurité, mais ne sont pas dénués de risques. Les professionnels de la sécurité devraient garder à l'esprit ce que l'on appelle le VLAN hopping. Comme son nom l'indique, il s'agit de la communication illicite d'utilisateurs finaux avec un VLAN dont ils ne font pas partie. Cette attaque est la plus facile à réaliser lorsqu'un VLAN comporte plusieurs commutateurs. C'est souvent le cas dans les entreprises dotées de VLAN par groupes, car un ou plusieurs groupes deviennent trop grands pour une connexion via un seul commutateur. Dans ce cas, on peut recourir à un concept baptisé VLAN trunking. Dans ce contexte, un ou plusieurs ports d'un commutateur Ethernet sont configurés de manière à n'accepter et à ne transmettre que le trafic de données VLAN d'un autre switch physique. En cas d'attaque éventuelle, un cyberpirate mal intentionné insère un deuxième en-tête 802.1Q dans une trame Ethernet de sorte que celui-ci peut être relayé dans un VLAN non autorisé. Cela est possible car le premier commutateur analyse la trame, en retire le premier des deux en-têtes, puis transmet le reste des trames. Or le deuxième en-tête 802.1Q se trouve toujours dans la trame, ce qui entraîne une erreur logique susceptible de perturber fortement un réseau. Pour se défendre contre de telles attaques, les administrateurs doivent prêter une grande attention à leurs journaux de réseau. Un mécanisme d'alerte peut en outre être mis en œuvre au niveau de la couche 3.

(5) Il faut sécuriser explicitement les VLAN des environnements ICS, étant donné que les configurations et configurations réseau standard ne sont intrinsèquement pas sûres. Lors de l'utilisation de VLAN, il convient de désactiver le DTP (Dynamic Trunking Protocol) sur les éléments de réseau. Les ports doivent par conséquent être configurés comme des ports d'accès statiques, ce qui permet d'éviter les switch spoofing exploits. Qui plus est, les ports de commutateur non utilisés doivent être désactivés, ce qui empêche tout accès non autorisé au réseau.

(6) Les éléments de réseau sont par défaut conçus avec le VLAN 1, dont il ne faut jamais se servir.

d) Pare-feux (ou firewalls)

(1) La sécurité des réseaux dépend de plusieurs composantes remplissant chacune un rôle spécifique. Au sein d'un environnement réseau sûr, les pare-feux constituent un élément essentiel permettant d'empêcher l'intrusion d'éventuels attaquants. Pour pouvoir intégrer des pare-feux à des environnements réseau, il faut au préalable segmenter et regrouper les réseaux dans l'environnement ICS. On crée par conséquent des jonctions où il est possible d'utiliser des firewalls.

(2) Les pare-feux font office de sentinelles ou de gardiens entre les zones. S'ils sont correctement configurés, seules les connexions souhaitées et nécessaires sont autorisées et établies. Les règles

de pare-feu permettent de surveiller le trafic réseau et activent un chemin fiable vers les utilisateurs et un canal – fiable lui aussi – vers d'autres appareils. L'efficacité des firewalls dépend de l'efficience des règles avec lesquelles ils sont configurés Au sein d'un pare-feu, on définit des règles qui sont exécutées de manière séquentielle. Toutes les possibilités de connexion doivent ainsi être configurées de façon explicite et séquentielle. La règle d'or du pare-feu énonce que «ce qui n'est pas explicitement permis n'est pas autorisé», ce qui signifie que la dernière règle empêche toujours les «possibilités restantes».

(3) La tâche du pare-feu consiste:

- à isoler les domaines les uns des autres;
- à surveiller (et à consigner) les événements système;
- à authentifier les utilisateurs avant qu'ils bénéficient d'un accès;
- à surveiller le trafic entrant et sortant et à empêcher toute communication non autorisée.

(4) On distingue deux types de pare-feux: le pare-feu de l'ordinateur, ou pare-feu hôte, et le pare-feu réseau. Le pare-feu hôte protège un hôte spécifique. Il peut faire partie du système d'exploitation, ou il peut s'agir d'une application en lien direct avec l'hôte. Le pare-feu utilisé protège le réseau à l'aide de l'une des techniques suivantes:

Filtrage de paquets

(5) Les pare-feux à filtrage de paquets (packet filtering) ou network layer firewalls (couche 3) prennent des décisions sur la base des adresses et ports source et destination contenus dans les paquets IP. Cette forme de base de protection pare-feu n'est en réalité ni plus ni moins qu'un simple algorithme de tri. En général, ces pare-feux vous permettent d'effectuer un certain contrôle en utilisant des listes d'accès. Souvent, le filtrage de paquets peut également être exécuté par d'autres équipements réseau tels que les routeurs. Vous bénéficiez habituellement aussi de ce filtrage lorsque vous téléchargez un logiciel pare-feu gratuit.

(6) Le filtrage de paquets fonctionne bien sur les petits réseaux. Lorsqu'il est utilisé sur des réseaux de plus grande taille, sa configuration peut toutefois s'avérer très complexe. Ce type de pare-feu offrant peu ou pas de possibilité d'enregistrement, il est difficile d'établir si une attaque a eu lieu ou non. Ce type de pare-feu filtre le trafic de données en s'appuyant sur des règles. Celles-ci pilotent le trafic sur la base des trois premiers niveaux du modèle OSI: l'adresse MAC et l'adresse IP avec un filtrage basé sur la couche de transport (numéros de port).

Passerelles de niveau circuit (circuit level gateways)

(7) Les passerelles de niveau circuit (circuit level gateways) travaillent sur la couche session du modèle OSI ou font office de «couche de calage» («shim layer») entre la couche application et la couche transport de la pile TCP/IP. Ces passerelles contrôlent le handshaking TCP entre les paquets pour déterminer si la demande de session est légitime. Les informations qui ont été transmises à un ordinateur distant en transitant par un circuit level gateway s'affichent comme provenant de cette passerelle. Les applications de pare-feu de niveau circuit représentent la technologie de prochaine génération. Cette technologie de pare-feu contrôle le handshaking TCP entre les paquets pour confirmer qu'une session ou une connexion est autorisée. Le trafic du pare-feu est clairement défini sur la base de certaines règles de session et ne peut être piloté que sur les éléments concernés. Les pare-feux de niveau circuit (circuit level firewalls) ne contrôlent et ne vérifient pas le contenu des paquets de données. Ils ne filtrent pas non plus les différents paquets.

Passerelle de proxy, pare-feu de la couche application, passerelle de la couche application (application layer gateway ou ALG)

(8) Ce pare-feu offre un filtrage au niveau de la couche application. En d'autres termes, il limite les types d'applications et de protocoles qui communiquent par-delà les frontières de sécurité, p. ex. le File Transfer Protocol (FTP) ou l'HyperText Transfer Protocol (HTTP).

Inspection d'état (stateful inspection)

(9) Un pare-feu à états (stateful inspection firewall) examine les paquets de données et intègre l'état de la connexion à la décision. Cette technique consiste à analyser les paquets de données (en fait les segments) pendant leur transfert sur la couche réseau (3^{e} couche du modèle OSI) et à les mémoriser dans des tableaux d'état dynamiques. Les décisions relatives au routage des paquets sont prises sur la base de l'état des connexions. Les paquets de données ne respectant pas certains critères ou faisant partie d'une attaque par déni de service (attaque DoS) sont rejetés. C'est pourquoi les pare-feux SPI (aussi appelés pare-feux à filtrage dynamique de paquets) surpassent les pare-feux à simple filtrage de paquets dans les applications touchant à la sécurité.

Inspection approfondie des paquets (deep packet inspection ou DPI)

(10) L'inspection approfondie des paquets, ou DPI, permet d'analyser des informations supplémentaires, qui sont notamment spécifiques à un protocole. Il est ainsi possible d'utiliser des règles basées sur les URL, sur les noms de fichiers, sur le contenu des données (analyse antivirus ou data loss prevention) et sur d'autres éléments similaires. Les possibilités sont analogues à celles d'un proxy ou d'un filtre de contenu, mais de nombreux protocoles sont généralement couverts.

(11) Pour pouvoir également analyser les données de connexion et contenus cryptés, on recourt à l'inspection approfondie des paquets SSL (SSL deep packet inspection), qui termine un cryptage SSL existant, examine les contenus, puis les crypte de nouveau pour le client. À cet effet, il est en général nécessaire d'installer sur le client un certificat racine d'autorité de certification (AC) permettant au pare-feu de générer lui-même les certificats appropriés au cours du fonctionnement. Sur le plan technique, cela correspond à une attaque de l'homme du milieu.

(12) L'emplacement du pare-feu devrait être coordonné, planifié et pensé dans les moindres détails. Son lieu d'utilisation doit être prévu de façon à ce qu'aucun individu ni élément ne puisse contourner la sécurité du pare-feu sur l'ensemble du réseau. Ainsi, un élément comportant deux cartes d'interface réseau (NIC), souvent appelées «dual-homed» host, entraîne un cyberrisque lorsque l'une d'elles est reliée au réseau de l'entreprise et l'autre à l'environnement ICS. Bien que ce type de configuration simplifie la gestion et réduise la complexité, elle contourne effectivement les mécanismes de protection périmétrique et peut engendrer une grande vulnérabilité que les cybercriminels peuvent également exploiter dans les environnements virtuels.

(13) Il faudrait que les administrateurs système spécifient et mettent en place l'ensemble des règles de pare-feu en fonction des besoins, comme le montre la figure ci-dessous. Le principe est le suivant: on fait en sorte qu'à chaque jonction, seul le trafic devant être autorisé spécifiquement à chaque niveau transite par le pare-feu. Il est également essentiel de mettre à jour en permanence les règles de ce dernier, car une modification même minime pourrait réduire l'efficacité contre les vecteurs d'intrusion/failles actuels. Tout changement dans les règles de pare-feu est susceptible d'affecter les autorisations de circulation des données. Testez-le donc toujours afin de vous assurer qu'il ne neutralise pas le système de sécurité. Contrôler périodiquement les emplacements des pare-feux et les règles y afférentes contribue au maintien de la protection requise.

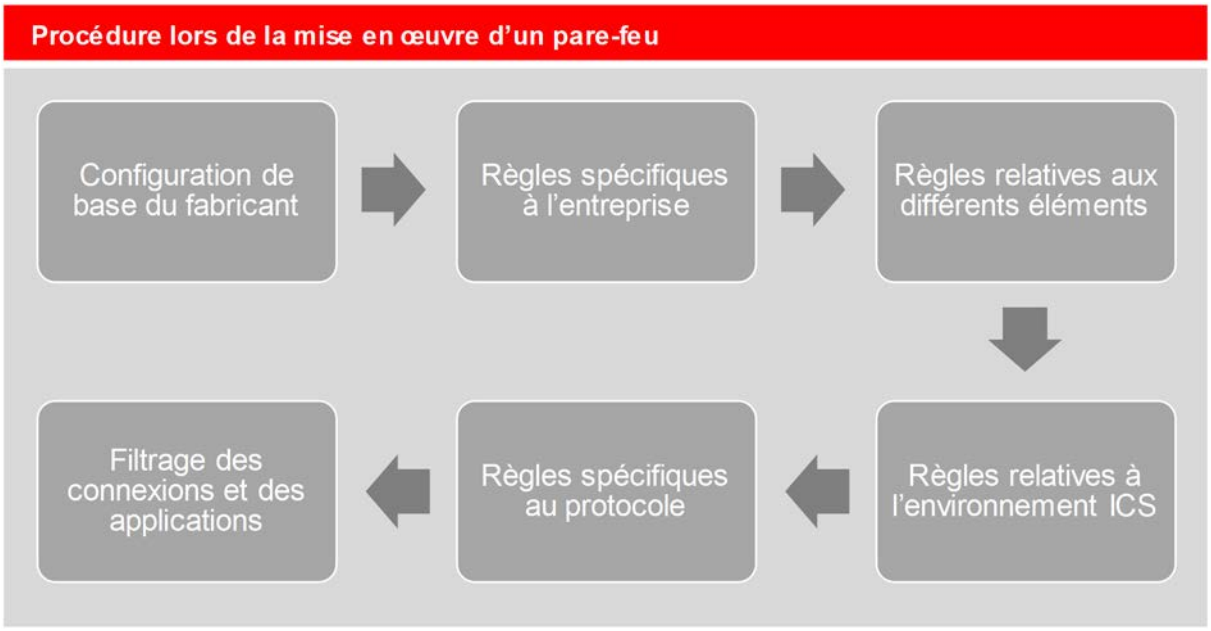

Figure 17 Procédure lors de la mise en œuvre d'un pare-feu

(14) Mal placer un pare-feu risque de diminuer son efficacité. Il n'est pas rare de contourner le firewall, de manière intentionnelle ou non. Les modems ayant un accès direct aux éléments ICS, les VPN des fabricants disposant d'un accès direct à l'environnement ICS, les points d'accès sans fil et l'utilisation d'un dual-NIC host peuvent altérer les performances du pare-feu et, par voie de conséquence, lever la protection nécessaire de l'environnement ICS.

e) Zones démilitarisées

(1) Une zone démilitarisée (demilitarized zone ou DMZ, parfois appelée réseau de périmètre) est un sous-réseau physique et logique faisant office d'intermédiaire pour les dispositifs de sécurité raccordés afin qu'ils ne soient pas exposés à un réseau plus vaste et non fiable, généralement Internet. La DMZ ajoute une couche de sécurité supplémentaire au réseau d'une entreprise. Un intrus externe ne dispose ainsi que d'un accès direct aux appareils situés à l'intérieur de la DMZ, toute autre partie du réseau lui étant inaccessible.

(2) La possibilité d'établir une DMZ entre le réseau de l'entreprise et l'environnement ICS constitue une amélioration significative lors de l'utilisation des pare-feux. La création d'une DMZ exige que le pare-feu offre au moins trois interfaces en lieu et place des interfaces publiques et privées

habituelles. L'une des interfaces se connecte au réseau de l'entreprise, la deuxième à l'environnement ICS et les interfaces restantes aux dispositifs partagés ou non sécurisés, tels que le serveur d'archivage des données, les serveurs de fichiers, etc., sur le réseau de la DMZ.

(3) Placer des éléments spécifiques au sein d'une DMZ rend inutiles les voies de communication directes entre le réseau d'entreprise et l'environnement ICS; l'ensemble des connexions ou chemins aboutissent effectivement au niveau de la DMZ. La plupart des pare-feux sont capables de gérer plusieurs DMZ et de spécifier le type de trafic pouvant être transféré entre ces zones. Le pare-feu peut empêcher n'importe quel paquet provenant du réseau de l'entreprise de passer dans l'environnement ICS et est également à même de réguler le trafic des autres zones du réseau, y compris du réseau de contrôle. Une bonne planification des jeux de règles permet de garantir une séparation claire entre l'environnement ICS et les autres réseaux, avec un trafic faible, voire inexistant entre le réseau de l'entreprise et cet environnement.

(4) Dans ce type d'architecture, le principal risque en matière de sécurité est qu'un cyberpirate compromette un élément au sein de la DMZ et l'utilise pour s'introduire dans l'environnement ICS via un trafic applicatif autorisé par cette dernière. Il est possible de réduire ce risque en renforçant et en corrigeant activement les systèmes dans la DMZ. Cela implique que l'ensemble des règles de pare-feu autorise uniquement les connexions initiées par les équipements réseau SCADA entre le réseau de commande et la DMZ. Parmi les autres problèmes posés par cette architecture, citons la complexité accrue et le surcoût potentiel des pare-feux à plusieurs ports. Pour les systèmes plus critiques, l'amélioration de la sécurité devrait toutefois largement compenser ces inconvénients.

(5) Les solutions à deux zones (pas de DMZ) peuvent à la limite être acceptées, mais ne doivent être utilisées qu'avec une extrême prudence. Les architectures de segmentation du réseau de commande et du réseau d'entreprise les plus sûres, les plus faciles à gérer et les plus évolutives recourent généralement à un système comportant au moins trois secteurs avec une ou plusieurs DMZ.

(6) Il convient de constituer plusieurs DMZ pour des fonctionnalités et autorisations d'accès distinctes comme les connexions de poste à poste, les archives de données, les protocoles de communication ICS, le serveur ICCP dans les systèmes de surveillance et de saisie des données (systèmes SCADA), ainsi que les serveurs de sécurité, de réplication et de développement. Plusieurs DMZ se sont avérées efficaces pour protéger de vastes environnements composés de réseaux faisant intervenir différents exploitants et utilisateurs. Un flux de données sûr au sein et en provenance des divers environnements revêt une importance cruciale pour l'exploitation.

(7) Les exploitants d'installations devraient limiter l'accès à une DMZ ICS aux seuls utilisateurs, applications et services autorisés. Dans la mesure du possible, il faudrait enregistrer et surveiller le trafic entrant dans la DMZ et celui en sortant afin de pouvoir s'en servir pour le filtrage de la source/de la destination/du service, pour un contrôle supplémentaire de la sécurité et pour la détection des anomalies au niveau des données utiles (fonctions IDS et IPS).

(8) L'accès depuis la zone de sécurité supérieure, c'est-à-dire à l'intérieur des niveaux de contrôle ou d'exploitation, s'effectue en général pour transmettre des données («push de données») à l'application DMZ et les mettre ainsi à disposition des utilisateurs autorisés de l'entreprise. L'accès pour l'utilisateur de l'entreprise passe uniquement par le serveur applicatif DMZ, ce qui fournit une séparation supplémentaire. Il est important de créer cette séparation logique afin d'éviter qu'un

cybercriminel puisse exploiter la confiance entre les enclaves de l'entreprise au sein de la DMZ pour «pivoter» de cette dernière dans le système de contrôle-commande.

(9) En cas d'utilisation de solutions DMZ, la prudence est cependant de mise. Il existe là aussi un risque de relier entre eux des domaines qui, sinon, seraient logiquement séparés. Ne partez pas du principe que la mise en œuvre d'une DMZ constitue une panacée permettant d'empêcher les cybercriminels de pénétrer plus profondément dans des environnements critiques. L'exploitation efficace des données de confiance via un périmètre de sécurité est un vecteur d'intrusion plausible. Mais si on développe et utilise une DMZ offrant une sécurité ad hoc, cette contre-mesure complique la tâche du cyberpirate, renforce le contrôle de l'exploitant d'installation et réduit le cyberrisque à certaines installations importantes critiques en matière d'approvisionnement.

f) Cryptages

(1) SSH et SSL/TLS désignent deux procédés de cryptage en matière de connexions réseau. Ces deux méthodes se distinguent nettement de par leur origine et leur finalité. Pour simplifier, SSL sert à crypter les données, tandis que SSH permet de sécuriser la liaison de communication entre un client et un serveur. Mais cette explication ne suffit pas. Il s'agit en substance tout bonnement des deux piliers de la sécurité informatique. D'un côté, SSL vise à empêcher l'usage abusif et l'espionnage de données. De l'autre, en sécurisant l'accès aux ordinateurs centraux, SSH doit éviter les piratages ou les sabotages.

(2) Abréviation de Secure Sockets Layer, SSL est d'ores et déjà un standard obsolète. Il a été remplacé par TLS (actuellement en version 1.2), qui signifie Transport Layer Security. Bien que les différences soient relativement faibles, certaines fonctions supplémentaires rendent TLS encore plus sûr que son prédécesseur SSL. Il s'agit d'un protocole de cryptage dit «hybride», qui combine des procédés asymétriques et symétriques.

Procédé de cryptographie asymétrique, ou cryptographie à clé publique:

(3) On génère tout d'abord une paire de clés constituée d'une clé publique et de la clé privée correspondante. Le texte est chiffré et envoyé en utilisant la clé publique du destinataire, qui doit déchiffrer les données à l'aide de sa clé privée appropriée.

- Avantages: sécurité relativement élevée, moins de clés, aucun problème de distribution de clés
- Inconvénients: beaucoup plus lent, clés très longues, cryptage explicite

Cryptographie symétrique:

(4) Dans ce système cryptographique, l'expéditeur et le destinataire utilisent la même clé.

- Avantages: gestion ordinaire des clés, vitesse élevée
- Inconvénients: une seule et même clé pour le chiffrement et le déchiffrement, nécessité de transporter la clé, grand nombre de clés

(5) Dans le cas de TLS/SSL, on commence par générer une clé de session (session key) symétrique, qui code et envoie ensuite les données sensibles. Une fois arrivée sur le terminal, cette clé réceptionne les données et les déchiffre de manière asymétrique. Ce procédé permet de distribuer des clés uniques asymétriques aux destinataires tout en recourant à la cryptographie symétrique plus rapide pour transporter les données. SSL ou son successeur TLS est notamment mis en

œuvre pour les connexions HTTPS, raison pour laquelle la plupart des serveurs web utilisent TLS avec des algorithmes Camellia ou AES. En clair, cela signifie que TLS est le protocole et qu'il définit les conditions-cadre pour le transfert crypté. AES et Camellia sont les méthodes permettant d'appliquer le chiffrage.

(6) SSH, ou Secure Shell, est le nom d'un protocole de cryptage réseau issu d'une tout autre approche que TLS ou SSL. Il désigne aussi bien un protocole réseau que les programmes correspondants permettant d'établir en toute sécurité une connexion réseau cryptée avec un équipement distant. Cette méthode est souvent employée pour mettre à disposition en local une ligne de commande à distance, c'est-à-dire que les sorties de la console distante s'affichent sur une console locale et les saisies clavier locales sont envoyées à l'ordinateur distant. On peut l'utiliser par exemple pour la télémaintenance d'un serveur situé dans un centre de calcul distant. Baptisée SSH-2, la version plus récente du protocole offre d'autres fonctions telles que le transfert de données par SFTP.

(7) Contrairement à SSL ou à TLS, SSH applique uniquement le principe de la cryptographie asymétrique, ou à clé publique. Pour ce faire, le serveur envoie en premier lieu sa clé publique que le client renvoie chiffrée. Doté de sa clé privée appropriée, le serveur peut désormais autoriser les connexions cryptées avec le client. Le problème se pose lorsqu'un proxy ou un pare-feu se trouve sur le chemin. Dans ce cas, on utilise d'autres protocoles (HTTPS) et certificats perfectionnés, ou on crée un tunnel SSH. Cela permet de transporter des protocoles réseau peu sûrs en les intégrant à un protocole réseau sécurisé et crypté de manière à les protéger contre les interceptions et les manipulations.

Le problème des connexions cryptées

(8) Or les connexions cryptées présentent aussi des risques importants. L'examen de leur contenu pour détecter la présence d'un éventuel logiciel malveillant ou dysfonctionnement n'est pas si simple. En outre, des réseaux entiers peuvent être interconnectés par le biais de connexions SSH sans qu'aucune barrière de sécurité, comme un pare-feu, ne s'en aperçoive. Il faut donc définir très précisément les éléments qui doivent communiquer via une connexion cryptée. Chacune de ces connexions devrait se terminer au niveau du pare-feu, ou ne pas dépasser l'IDS/IPS.

g) Signatures numériques, certificats numériques et infrastructures à clé publique

(1) Les signatures et certificats numériques constituent aujourd'hui le fondement de la confiance sur Internet. De plus en plus de dispositifs sont connectés à Internet, les appareils dits «de l'Internet des objets» (IdO, en anglais Internet of Things ou IoT) et le machine-to-machine (M2M) permettent de communiquer et d'échanger des données en permanence. De véritables flux de big data font rapidement leur apparition, le tout dans une relative insécurité, car la communication n'est généralement pas régie par des certificats numériques.

Signatures numériques

(2) Une signature numérique (à ne pas confondre avec un certificat numérique) désigne une signature électronique permettant à l'expéditeur d'un message ou au signataire d'un document de prouver son identité. Ce procédé garantit le cas échéant que le contenu initial d'un document ou message envoyé n'a pas été altéré. Les signatures numériques sont faciles à transmettre, infalsifiables et horodatées automatiquement. Étant donné qu'il est possible de prouver la réception du message original signé, l'expéditeur ne pourra pas non plus en contester l'envoi ultérieurement.

Certificats numériques

(3) Un certificat numérique désigne une carte d'identité électronique permettant à une personne, un ordinateur ou une organisation d'échanger en toute sécurité des informations par Internet à l'aide de l'infrastructure à clé publique (ICP, en anglais public key infrastructure ou PKI). Il est aussi souvent appelé certificat de clé publique.

(4) À l'instar d'une carte d'identité, un certificat numérique fournit des informations sur l'identité et ne peut pas être falsifié. Il peut en revanche être vérifié car il a été délivré par une institution officielle digne de confiance. Le certificat comporte le nom de son propriétaire, un numéro de série, la date d'expiration, une copie de la clé publique dudit propriétaire (utilisée pour crypter des messages et les signer numériquement) et la signature numérique de l'institution qui l'a délivré, de façon à ce que le destinataire puisse en vérifier l'authenticité.

(5) Les certificats de clé publique conformes à la norme X.509, qui confirment l'identité de leur titulaire et d'autres caractéristiques d'une clé cryptographique publique, sont largement répandus. A contrario, les certificats d'attribut ne contiennent pas de clé publique, mais renvoient à un certificat de clé publique dont ils définissent plus précisément le champ d'application. Dans le contexte des signatures électroniques, le terme de certificat est compris dans une acception plus neutre du point de vue technologique (cf. section «Aspects juridiques» de l'article consacré au certificat de clé publique), de sorte qu'un certificat ne doit pas nécessairement se référer à une clé cryptographique, mais comporte en général des données destinées à vérifier une signature électronique. Dans la pratique, il s'agit pourtant toujours de certificats de clé publique.

(6) Ces certificats signés peuvent être attribués de manière univoque. C'est le seul moyen d'empêcher leur altération, et donc leur falsification. Tous les certificats sont gérés par une autorité de certification (certification authority, CA) qui se charge de leur sécurité et leur confère un statut digne de confiance.

(7) Pour vérifier l'authenticité du certificat dit «de clé publique» – en d'autres termes, pour démontrer que l'origine indiquée correspond bien à l'origine réelle –, d'autres certificats entrent en jeu. Ils constituent des chaînes de certificats connues sous le nom de «chemin de validation» et autorisant le path tracking. Ensemble, les différents chemins de certification forment une infrastructure à clé publique (ICP) solide.

(8) Les cyberpirates recourent la plupart du temps à des attaques de l'homme du milieu. Ainsi, ils interceptent la communication au moyen d'un certificat compromis. Les cybercriminels ont développé quelques milliers de chevaux de Troie qui leur permettent de voler tous les certificats possibles, de les modifier puis de les réintégrer.

(9) De nombreux experts tablent à l'avenir sur une nette augmentation des attaques par le biais de certificats frauduleux, notamment en ce qui concerne l'Internet des objets. Bon nombre de ces nouveaux appareils doivent faciliter la vie de chacun tout en accroissant l'efficacité de la production industrielle. Il faut donc appliquer une approche globale de sécurité, qui vérifie l'authenticité des certificats et met en quarantaine ceux qui ont été falsifiés.

(10) Un certificat numérique est en général valable deux ans, tandis que la durée de vie des composants au sein des installations critiques en matière d'approvisionnement dépasse souvent dix ans. Cela pose un nouveau défi à l'introduction de certificats.

h) Infrastructure à clé publique ou ICP (public key infrastructure ou PKI)

(1) Une infrastructure à clé publique (ICP) offre certains avantages aux utilisateurs d'un réseau public intrinsèquement non sécurisé, comme Internet: un échange sécurisé et confidentiel des données à l'aide d'une paire constituée d'une clé cryptographique publique et d'une clé cryptographique privée. Une autorité digne de confiance se procure celle-ci et la transmet. L'ICP met à disposition un certificat numérique servant à identifier une personne ou une entreprise. Elle offre en outre des services de répertoire pour enregistrer et, le cas échéant, pour révoquer les certificats. Si les éléments requis d'une ICP sont largement compris, de nombreux fournisseurs proposent de nouvelles approches et prestations dans ce domaine.

(2) Qui dit ICP dit procédé de cryptographie à clé publique. Il s'agit de la forme la plus courante d'authentification de l'expéditeur et de cryptage des messages. Lors du cryptage traditionnel, une clé secrète destinée à chiffrer puis à déchiffrer les messages a généralement été créée et transmise. Ce système basé sur une clé secrète ou privée présente toutefois un sérieux inconvénient: si un tiers intercepte ou craque cette clé, il peut décrypter sans problème les messages. C'est la raison pour laquelle, sur Internet, on privilégie l'approche combinant un procédé de cryptographie à clé publique et une ICP. La cryptographie à clé privée est parfois aussi qualifiée de symétrique, tandis qu'on parle de cryptographie asymétrique dans le cas de la terchnique à clé publique.

Une infrastructure à clé publique englobe les éléments suivants:

- Une autorité de certification pour la délivrance et la vérification des certificats numériques
- Un certificat comportant la clé publique ou des informations sur cette dernière
- Une autorité d'enregistrement pour vérifier l'autorité de certification avant qu'elle délivre un certificat numérique au demandeur
- Un ou plusieurs répertoires pour y conserver les certificats (et leurs clés publiques)
- Un système de gestion des certificats

Fonctionnement de la cryptographie à clé publique/à clé privée

(3) Pour la cryptographie à clé publique, une clé publique et une clé privée sont créées simultanément. L'autorité de certification utilise à cet effet le même algorithme (le célèbre RSA étant particulièrement apprécié). La clé privée est remise uniquement au demandeur, tandis que la clé publique est disponible dans un répertoire accessible à toutes les parties (en tant que composante d'un certificat numérique). La clé privée, quant à elle, n'est jamais transmise à des tiers ni envoyée par Internet. Elle vous sert à déchiffrer des messages cryptés avec votre clé publique, que l'expéditeur a obtenue à partir du répertoire accessible au public.

(4) Si on recourt aux certificats numériques avec une ICP pour les installations critiques en matière d'approvisionnement, cette infrastructure doit être mise en place localement au sein de l'entreprise et isolée d'Internet. En cas d'utilisation d'ICP publiques ou externes sur Internet, il faudrait sinon établir des connexions avec ces entités, ce qui créerait une faille de sécurité supplémentaire sur le réseau prétendument sûr. C'est pourquoi l'introduction de certificats numériques en relation avec une ICP doit être mûrement réfléchie et planifiée, d'autant plus que les fournisseurs actuels de composants destinés aux installations critiques en matière d'approvisionnement n'ont pas encore implémenté ni utilisé cette fonction.

i) Diodes réseau

(1) Une diode réseau, également appelée passerelle de sécurité unidirectionnelle, est un équipement réseau ou un dispositif permettant le transfert de données dans un seul sens. On trouve ces diodes le plus souvent dans les environnements de haute sécurité, où elles servent à connecter deux ou plusieurs réseaux de niveaux de sécurité différents. Cette technologie est utilisée aujourd'hui dans les systèmes de contrôle-commande industriels de centrales nucléaires et d'installations productrices d'électricité, p. ex..

(2) De par leur nature physique, les réseaux unidirectionnels autorisent uniquement le transfert de données d'une extrémité à l'autre d'une connexion réseau, et non l'inverse. Les avantages pour les utilisateurs du réseau de priorité critique supérieure (p. ex. d'un segment ICS) résident dans le fait qu'il est possible de transférer les données situées sur un réseau de criticité inférieure (réseau bas), comme p. ex. d'un serveur dans une DMZ, tout en empêchant ce réseau de priorité critique inférieure d'accéder aux informations du réseau ICS. L'interface pilotée, qui englobe les éléments émetteurs et récepteurs d'un réseau unidirectionnel, agit comme une rupture unidirectionnelle du protocole de communication entre les deux domaines réseau interconnectés. Cela n'exclut pas l'utilisation du réseau unidirectionnel pour transférer des protocoles comme TCP, qui nécessitent une communication (confirmations incluses) entre émetteur et récepteur.

(3) Les exploitants d'installations critiques en matière d'approvisionnement recourent de plus en plus aux diodes réseau.

j) Convertisseurs de protocole

(1) Dans l'environnement ICS, les connexions sont souvent utilisées lorsque de petites quantités de données doivent être transférées. Pour une protection efficace, il est donc possible de recourir au transfert de données traditionnel via des ports série. Ces connexions fonctionnent généralement sans fonctionnalité IP et peuvent être considérées comme des liaisons point à point classiques On obtient ainsi des connexions «sans IP». Cette mesure permet d'éliminer une grande partie, voire la totalité des vulnérabilités au sein de l'environnement ICS.

(2) L'exécution de cette fonctionnalité requiert à chaque fois deux éléments, comme le montre la figure ci-dessous:

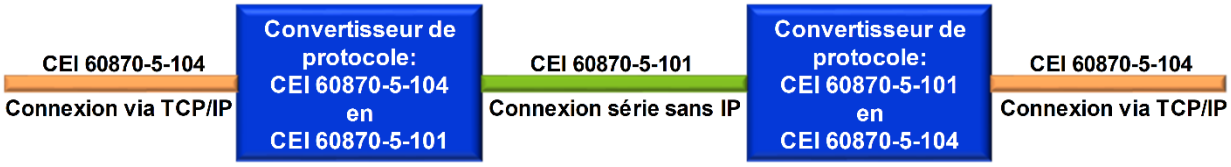

Figure 18 Utilisation de convertisseurs de protocole

(3) Cette méthode peut être utilisée pour opérer une segmentation entre deux secteurs ou segments. Le transfert «sans IP» permet de supprimer de nombreuses vulnérabilités présentées par les réseaux IP classiques.

2.8.2 Définition et description des jonctions entre les zones

(1) Il existe en principe des jonctions horizontales et verticales entre les zones de l'environnement ICS. Les types de jonctions doivent tous être définis et décrits.

a) Jonctions horizontales entre les secteurs et les zones

(1) Dans la mesure où cela est nécessaire, applicable, judicieux et techniquement réalisable, la structure de réseau sous-jacente au système est divisée horizontalement en secteurs et zones indépendants (p. ex. selon les sites et les fonctions), la séparation des secteurs/zones devant être effectuée par des pare-feux, des routeurs filtrants, des passerelles ou via DMZ. Une segmentation doit également être effectuée au sein des différents secteurs et zones. Il faut créer des espaces avec des jonctions contrôlables et pilotables, afin d'empêcher un cyberpirate ou un logiciel malveillant de se déplacer ou de se propager librement. Au niveau des jonctions, on peut mettre en place des éléments de surveillance et de commande qui permettent de superviser, de contrôler et de limiter le trafic.

b) Jonctions verticales entre les secteurs et les zones

(1) Dans la mesure où cela est nécessaire, applicable, judicieux et techniquement réalisable, la structure de réseau sous-jacente au système est divisée verticalement en secteurs et zones remplissant diverses fonctions (contrôle du réseau, de la production et de l'infrastructure) et satisfaisant à des besoins de protection différents. Lorsque cela est techniquement possible, ces zones de réseau sont séparées par des pare-feux, des routeurs filtrants, des passerelles et des DMZ. La communication avec les autres réseaux doit s'effectuer exclusivement par le biais de protocoles de communication autorisés par le mandant et dans le respect des règles de sécurité en vigueur. Les jonctions verticales entre les zones doivent être planifiées et définies avec précision. Dans la mesure du possible, elles ne doivent être réalisées qu'en un point déterminé, ce qui empêche les déviations d'interconnecter les réseaux. Ces jonctions exigent un niveau de protection élevé, car les systèmes de différents fournisseurs et entreprises doivent souvent y être connectés. Or si la protection est insuffisante, une vulnérabilité dans un système peut affecter le système voisin.

c) Élaboration d'une matrice sectorielle et évaluation des connexions et des jonctions

(1) Pour obtenir une vue d'ensemble de toutes les connexions et communications possibles et nécessaires sur le réseau ICS, il est absolument indispensable d'élaborer une matrice de communication globale qui couvre les différents segments et zones. Ainsi, tous les processus peuvent être analysés et évalués. On utilise une matrice de communication pour déterminer les jonctions requises entre les zones, qui peuvent ensuite faire l'objet d'une évaluation. Il est impératif que toutes les connexions et options de communication nécessaires et possibles soient représentées dans cette matrice de communication. Cette méthode permet d'identifier les vulnérabilités ou les jonctions insuffisamment protégées entre les secteurs et les zones.

(2) La matrice de communication couvrant l'ensemble de l'environnement ICS décrit les mécanismes de base des jonctions entre les secteurs et les zones. Il faut établir des exigences et des directives détaillées pour la réalisation technique ou le dimensionnement.

(3) Tous les environnements et systèmes périphériques avec lesquels toute communication ou connexion est possible doivent eux aussi impérativement être répertoriés et décrits dans la matrice de zones couvrant l'ensemble de l'environnement ICS.

Matrice de zones couvrant l'ensemble de l'environnement ICS

de \ vers	Poste de travail externe Secteur E7	DMZ Internet Secteur E5	Activité de l'entreprise Secteur E4	IHM activité de l'entreprise Secteur E3	Metering activité de l'entreprise Secteur E3	Réseau DMZ OT/IT du SCADA Secteur E2	Installation DMZ OT/IT du SCADA Secteur E2	Réseau centre de contrôle SCADA Secteur 1	Installation centre de contrôle SCADA Secteur 1	Réseau DMZ frontale du SCADA Secteur P2	Installation DMZ frontale du SCADA Secteur P2	Partenaire DMZ frontale du SCADA Secteur P2	Réseau LAN IHM locale Secteur P4	Installation LAN IHM locale Secteur P4	Réseau LAN contrôleurs Secteur P5	Installation LAN contrôleurs Secteur P5	Réseau appareils de terrain Secteur P6	Installation appareils de terrain Secteur P6
Poste de travail externe Secteur E7	x	Oui[1]	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non
DMZ Internet Secteur E5	Oui[2]	x	Oui[2]	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non
Activité de l'entreprise Secteur E4	Oui[2]	Oui[1]	x	Oui[1]	Oui[1]	Oui[1]	Oui[1]	Oui[3]	Oui[3]	Non	Non	Non	Non	Non	Non	Non	Non	Non
IHM activité de l'entreprise Secteur E3	Non	Non	Oui[1]	x	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non
Metering activité de l'entreprise Secteur E3	Non	Non	Oui[1]	Non	x	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non
Réseau DMZ OT/IT du SCADA Secteur E2	Non	Non	Oui[1]	Non	Non	x	Non	Oui[2]	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non
Installation DMZ OT/IT du SCADA Secteur E2	Non	Non	Oui[1]	Non	Non	Non	x	Non	Oui[2]	Non	Non	Non	Non	Non	Non	Non	Non	Non
Réseau centre de contrôle SCADA Secteur 1	Non	Non	Oui[3]	Non	Non	Oui[1]	Non	x	Non	Oui[1]	Non	Oui[1]	Oui[3]	Non	Non	Non	Non	Non
Installation centre de contrôle SCADA Secteur 1	Non	Non	Oui[3]	Non	Non	Non	Oui[1]	Non	x	Non	Oui[1]	Oui[1]	Non	Oui[3]	Non	Non	Non	Non
Réseau DMZ frontale du SCADA Secteur P2	Non	Non	Non	Non	Non	Non	Non	Oui[2]	Non	x	Non	Non	Oui[1]	Non	Non	Non	Non	Non
Installation DMZ frontale du SCADA Secteur P2	Non	Non	Non	Non	Non	Non	Non	Non	Oui[2]	Non	x	Non	Non	Oui[1]	Non	Non	Non	Non
Partenaire DMZ frontale du SCADA Secteur P2	Non	Non	Non	Non	Non	Non	Non	Oui[2]	Oui[2]	Non	Non	x	Non	Non	Non	Non	Non	Non
Réseau LAN IHM locale Secteur P4	Non	Non	Non	Non	Non	Non	Non	Oui[3]	Non	Oui[1]	Non	Oui[1]	x	Non	Oui[1]	Non	Oui[1]	Non
Installation LAN IHM locale Secteur P4	Non	Non	Non	Non	Non	Non	Non	Non	Oui[3]	Non	Oui[1]	Oui[1]	Non	x	Non	Oui[1]	Non	Oui[1]
Réseau LAN contrôleurs Secteur P5	Non	Non	Non	Non	Non	Non	Non	Oui[3]	Non	Oui[1]	Non	Non	Oui[1]	Non	x	Non	Oui[1]	Non
Installation LAN contrôleurs Secteur P5	Non	Non	Non	Non	Non	Non	Non	Non	Oui[3]	Non	Oui[1]	Non	Non	Oui[1]	Non	x	Non	Oui[1]
Réseau appareils de terrain Secteur P6	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Oui[1]	Non	x	Oui[4]
Installation appareils de terrain Secteur P6	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Oui[1]	Oui[4]	x

Oui[1]	Possible après la procédure de «whitelisting»
Oui[2]	Si la source est un ALG: nécessité d'obtenir l'approbation de l'équipe architecture et sécurité, autres serveurs: non
Oui[4]	Possible uniquement sans IP, contacts analogiques ou binaires
Non	Non autorisé

Figure 19 Matrice de connexion interne pour le secteur E2, SCADA / DMZ / OT / IT

d) Cas particuliers

(1) Dans le secteur de l'énergie, il faut prendre en considération un certain nombre de cas particuliers en matière de communication. Les connexions nécessaires entre les dispositifs de protection pour les déclenchements à distance (protection à distance et protection différentielle) sont considérées comme des cas particuliers. Ici, les éléments de protection communiquent avec ceux des installations voisines. Étant donné que ces connexions posent des exigences élevées en termes de disponibilité et de temps de latence maximal, on recourt à des équipements de communication spécifiques. L'essentiel est que les communications pour ces connexions soient sécurisées et fiables. De telles connexions représentent un grand potentiel de dommages pour un cyberpirate, car les manipulations entraînent des déclenchements de protection et des débranchements de câbles subséquents. Ces systèmes ainsi que les connexions correspondantes doivent par conséquent être «très bien protégés». En cas de transmission via des «réseaux non sécurisés», il est impératif de crypter la connexion.

(2) Les cas particuliers suivants, qui requièrent une protection spéciale, sont connus:

- Dispositifs de protection et leurs connexions
- Équipement pour le délestage automatique sur seuil de fréquence (UFLS) [6]

2.8.3 Accès à distance et authentification

a) Accès à distance

(1) Les systèmes de contrôle-commande industriels jouent un rôle important au sein des infrastructures critiques d'approvisionnement en électricité. Par le passé, le risque inhérent à ces systèmes a été réduit en assurant une séparation complète des environnements opérationnels des réseaux externes et en limitant l'accès à la fonction de contrôle aux utilisateurs autorisés disposant d'un accès physique à une installation. Aujourd'hui, les besoins des entreprises ont accéléré la mise en réseau de ces systèmes autrefois isolés. Ces nouvelles possibilités de connexion ont permis aux propriétaires d'installations de maximiser leurs processus d'exploitation et de diminuer les coûts liés à la surveillance, à la mise à niveau et à l'entretien des appareils. Parallèlement, elles créent de nouvelles exigences en matière de sécurité pour la protection des systèmes OT dans les installations critiques d'approvisionnement en électricité contre les accès indésirables depuis des réseaux externes et Internet.

(2) Lors de la mise en place des accès à distance, il faut trouver un équilibre entre, d'une part, la façon dont les systèmes OT sont gérés et accessibles et, d'autre part, le maintien de leur position de cybersécurité. Un danger majeur est que les accès à distance sont souvent mal compris ou mal exécutés par les entreprises. L'utilisation de solutions d'accès à distance éprouvées et acceptées peut toutefois ne pas être adaptée de manière optimale au pilotage des environnements système. Les exigences en matière de disponibilité et d'intégrité, combinées aux nuances et attributs uniques que l'on retrouve souvent dans les systèmes «spécialement développés», conduisent à un nouveau profil d'exigences applicable à la création de solutions d'accès à distance sécurisées pour les systèmes au sein de l'environnement OT.

(3) Les accès à distance aux systèmes OT dédiés aux infrastructures critiques d'approvisionnement en électricité posent un défi de taille aux exploitants d'installations. Lorsqu'un poste de travail externe

[6] UFLS: Under Frequency Load Shedding, traduit par «délestage automatique sur seuil de fréquence»

établit une connexion cryptée directe à des éléments d'infrastructure critiques de l'approvisionnement en électricité, tout le segment est exposé aux dangers de l'environnement extérieur, et ce indépendamment du fait qu'il s'agisse d'un accès fournisseur ou de l'accès externe d'un technicien. Ces postes de travail externes sont souvent utilisés afin d'accéder à plusieurs installations. Ils constituent donc des emplacements idéaux pour diffuser des logiciels malveillants et un point central optimal pour accéder à l'ensemble des infrastructures. Ce sont précisément ces postes de travail qui deviennent la cible prioritaire d'un attaquant potentiel. La solution à ces problèmes est fournie par les accès à des jump stations, auxquelles seuls une connexion destinée à la transmission de la vidéo, le clavier et la souris peuvent être raccordés. Pour ce faire, il est possible d'utiliser différents types de connexions de bureau à distance (RDP, TeamViewer, pcAnywhere, etc.). Au niveau de la jump station, une connexion à l'installation critique d'approvisionnement en électricité peut ensuite être établie. Cela empêche les connexions directes entre les postes de travail externes et les infrastructures critiques en matière d'approvisionnement. Il est essentiel pour ces types de connexions d'entraver ou de contrôler la copie ou le transfert automatique de fichiers. Ces données doivent être vérifiées conformément aux directives de l'organisation d'exploitation. L'utilisation de jump stations, qui peuvent également être exécutées avec des machines virtuelles, permet également de résoudre le problème de l'authentification. Les accès aux jump stations peuvent en effet s'effectuer au moyen d'une authentification à deux facteurs (aussi appelée authentification à double facteur ou bifactorielle) et être surveillés et contrôlés à tout moment. De plus, les droits et possibilités pour l'utilisateur respectif peuvent y être attribués selon le principe de l'«absolue nécessité». De nombreuses infrastructures de pare-feu offrent des solutions complètes d'accès à distance qui pilotent et surveillent l'authentification et l'accès.

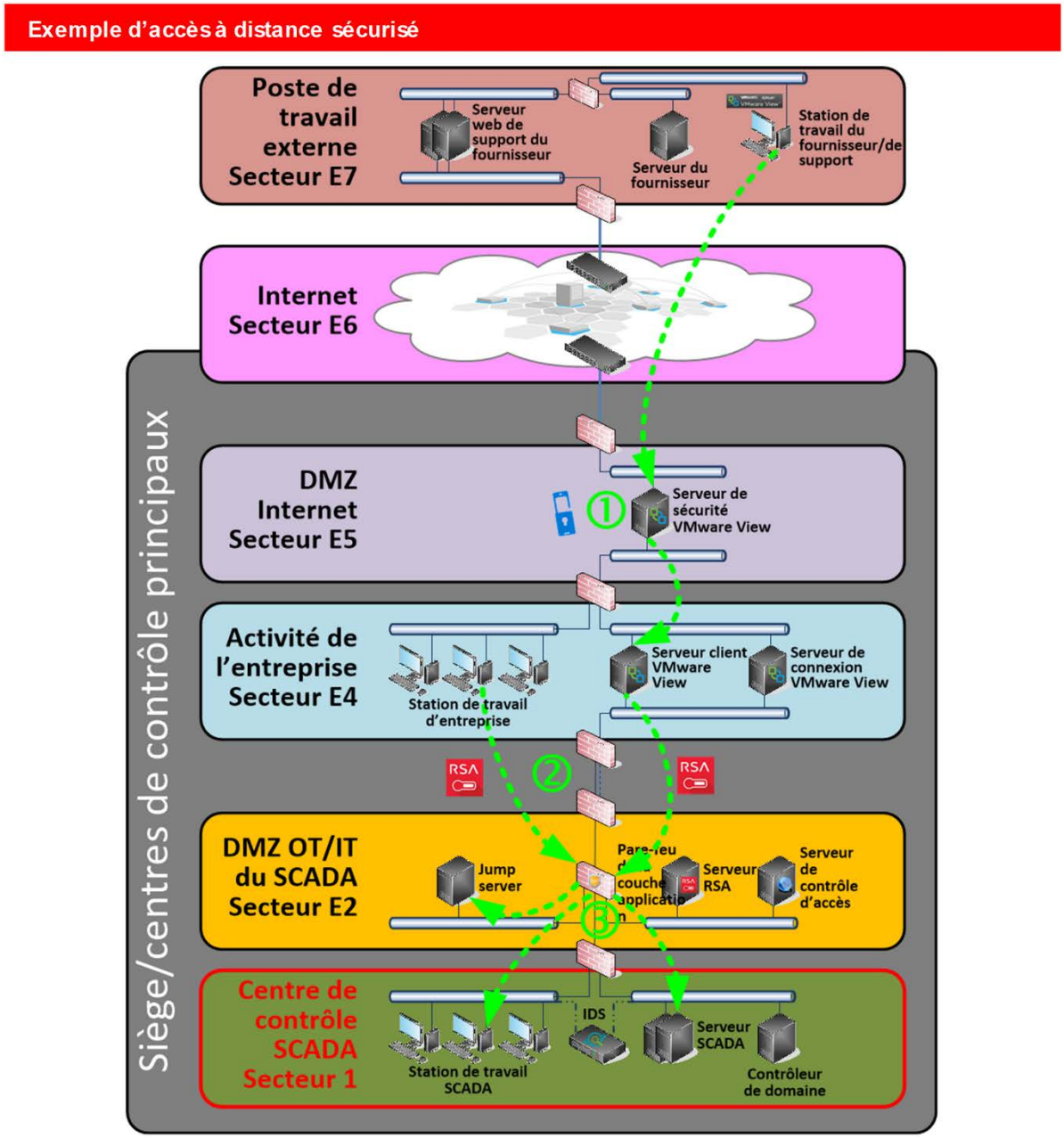

Figure 20 Exemple d'accès à distance sécurisé

① L'accès externe à un client dans l'environnement informatique métier est assuré par une connexion cryptée via le web. L'accès s'effectue par le biais d'une authentification à deux facteurs, ou authentification forte, p. ex. au moyen d'AD FS en combinaison avec une connexion au client via un compte informatique d'entreprise. On peut utiliser ici l'accès standard de l'informatique métier.

② Le client dans l'environnement informatique d'entreprise établit une connexion au pare-feu de la couche application à l'aide d'une connexion VPN SSL via le navigateur web. L'authentification sur le service de bureau à distance du pare-feu s'effectue au moyen de la méthode à deux facteurs. Il est conseillé que le deuxième facteur, p. ex le jeton RSA, se situe chez l'administrateur système de l'environnement OT et qu'il faille le lui demander.

③ Une fois validée par l'administrateur système, une session à distance peut être ouverte pour l'élément OT souhaité. La connexion à cet élément s'effectue conformément aux directives et aux exigences de l'exploitant du système OT.

(4) Il est recommandé que l'organisation d'exploitation doive autoriser et valider les accès à distance aux installations critiques d'approvisionnement en électricité. Dans l'idéal, cette organisation peut pour ce faire activer la connexion via la commande à distance au sein des installations. Cela permet de garantir à tout moment que l'organisation exploitante a connaissance des accès à distance aux systèmes et qu'elle peut également les empêcher en cas d'urgence. Les accès à distance automatisés sont déconseillés. De nombreux fournisseurs s'attendent à disposer d'un accès illimité aux installations afin de pouvoir effectuer des travaux d'entretien et de dépannage. Cela est très dangereux, car le contrôle d'accès et la surveillance ne peuvent plus être assurés. D'où la nécessité d'interdire strictement les connexions à distance automatisées.

(5) Lors de la mise en place d'un accès à distance aux systèmes OT, il convient de respecter les principes suivants:

- L'administration, la maintenance et la configuration de tous les composants doivent également être possibles par le biais d'un réseau hors bande, p. ex. en accès local, via une interface série, un réseau ou un contrôle direct des périphériques d'entrée (KVM[7]).
- Les accès à distance doivent s'effectuer via des serveurs gérés de manière centralisée. Ces serveurs d'accès doivent être exploités dans une DMZ et assurer l'isolement des réseaux OT. Il faut appliquer une méthode d'authentification forte, à deux facteurs.
- Il est en principe interdit d'accéder directement aux terminaux par ligne commutée, et il faut éviter d'établir des connexions VPN directes.
- Il est impératif de veiller à ce que les accès à distance s'effectuent uniquement au moyen d'«interruptions de protocole» et de jump stations, ce qui empêche une connexion directe entre différents réseau.
- L'utilisation des accès à distance doit être enregistrée (de manière centralisée), et les tentatives infructueuses répétées doivent être signalées.

(6) Les exploitants d'installations ne devraient permettre qu'aux utilisateurs externes autorisés d'établir une connexion à distance avec des serveurs d'authentification intermédiaires dans une DMZ. Outre l'utilisation de méthodes d'authentification multifactorielle, des règles et des états de connexion définitifs devraient être clairement identifiés et maintenus. Ces serveurs (souvent appelés «boîtes de saut» ou «jump boxes») fournissent des connexions à des ordinateurs distants qui sont probablement moins sécurisés que les boîtes de saut elles-mêmes. En plus de l'authentification multifactorielle et de la sécurité spécifique liée aux rôles des utilisateurs et aux autorisations les plus restreintes, les exploitants d'installations devraient durcir les boîtes de saut et l'ensemble des applications ou services ne permettant pas d'accès à distance sécurisé.

[7] KVM: Keyboard, Video und Maus = clavier, écran, souris

b) Authentification

(1) Il faut vérifier l'autorisation de l'utilisateur ou du composant du système demandeur avant certaines actions critiques ou touchant à la sécurité, comme p. ex. la lecture des points de données de processus ou des paramètres de configuration.

(2) Dans la plupart des réseaux ICS, un certain nombre d'utilisateurs différents se servent d'une grande variété de systèmes. Ces derniers doivent être appelés rapidement lorsque des opérations système sont nécessaires. Les pratiques d'authentification, d'autorisation et de gestion des comptes d'entreprise peuvent poser problème pour les ICS car ils sont «toujours en exploitation»; l'arrêt du système pour les utilisateurs ou la déconnexion et la connexion ne constituent donc généralement pas une option réalisable. Les processus d'authentification mis à disposition par les fournisseurs d'ICS peuvent également être limités. Gérer un grand nombre d'utilisateurs ayant des rôles définis différents sur plusieurs sites relève du défi. La seule solution consiste en fait à mettre en place une gestion centralisée des utilisateurs. Le même processus d'authentification peut contrôler l'accès à de nombreux systèmes (IHM, appareils de terrain, serveurs SCADA) et réseaux (réseaux locaux distants de transformation) requérant l'utilisation de données d'identification partagées. Les exploitants d'installations peuvent commander et surveiller l'accès aux systèmes ICS grâce à une approche décentralisée, locale ou centralisée. La gestion décentralisée des accès nécessite que chaque système effectue l'authentification séparément. Chacun d'entre eux recourt à une gamme distincte de comptes utilisateur, d'informations d'identification et de rôles. Cette approche serait une bonne solution pour mettre en œuvre de petits ICS, mais elle n'est pas très évolutive pour les grandes entreprises. Celles-ci appliquent généralement une gestion centralisée pour traiter un nombre important d'utilisateurs et de comptes. On utilise habituellement un système d'authentification centralisé (p. ex. Active Directory ou Lightweight Directory Access Protocol (LDAP)) qui gère les comptes. Un protocole d'authentification (p. ex. Kerberos, Remote Authentication Dial-In User Service (RADIUS) ou Terminal Access Controller Access-Control System (TACACS)) assure la communication entre le serveur d'authentification et les éléments ICS. Une approche centralisée est également extensible aux implémentations de systèmes à grande échelle. Elle peut toutefois devenir une vulnérabilité ou un risque lorsqu'elle est utilisée dans des environnements ICS Les serveurs centralisés doivent être très sécurisés car si le serveur d'authentification est compromis, tout l'environnement ICS peut l'être à son tour. Le système devant également être disponible en cas d'urgence, des serveurs redondants sont nécessaires. Il faut en outre disposer d'une gestion locale des utilisateurs, car sinon il est impossible d'accéder aux systèmes en cas de problèmes de communication avec la gestion centralisée des utilisateurs. Autant d'éléments qui posent un défi de taille à tout exploitant d'installations critiques en matière d'approvisionnement. Une solution pourrait consister à copier à chaque fois les données utilisateur centrales dans une gestion locale des utilisateurs et à mettre ainsi sur pied une structure locale, qui pourrait être administrée de manière centralisée. Étant donné que chaque connexion existante représente un risque potentiel, la liaison avec la gestion centralisée des utilisateurs doit faire l'objet d'une protection et d'une surveillance particulières. Il est recommandé que cette connexion soit active uniquement si une synchronisation des ensembles de données doit avoir lieu, et donc qu'elle peut être interrompue à distance.

Exemple de structure d’une installation critique en matière d’approvisionnement, dotée de fonctions de sécurité intégrées

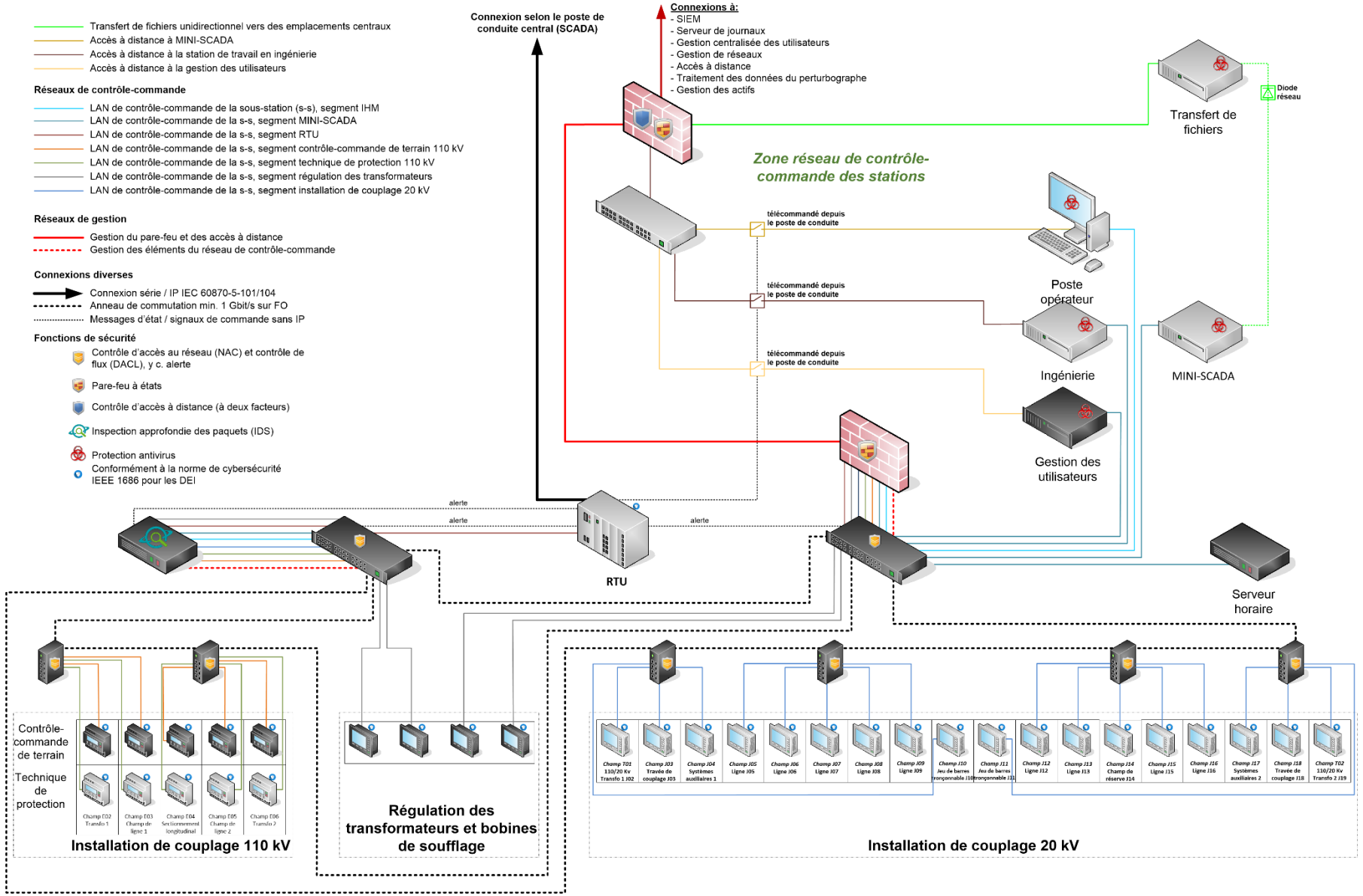

Figure 21 Exemple de structure d’une installation critique en matière d’approvisionnement

2.9 Sécurité des systèmes et des composants

2.9.1 Sécurité du système d'exploitation, du microprogramme et des applications

(1) Le niveau hôte ou station de travail implémente une autre couche de sécurité. Les pare-feux protègent la plupart des périphériques d'un réseau contre les intrusions extérieures, mais un bon modèle de sécurité nécessite des couches de défense supplémentaires. Cela est particulièrement important pour les clients IHM qui se connectent via une connexion VPN ou d'une autre manière depuis un endroit situé en dehors du périmètre digne de confiance du réseau ICS A l'instar d'une chaîne aussi solide que le maillon le plus faible, un réseau est aussi fort que l'hôte le plus faible.

(2) Globalement, de nombreuses pratiques de protection et mécanismes de sécurité basés sur l'hôte et recommandés sont peu, voire pas du tout pris en charge par les contrôleurs logiques programmables et d'autres technologies industrielles de pointe. Les mécanismes de contrôle de défense en profondeur pour ces dispositifs s'appliquent généralement au niveau du réseau. Bon nombre de systèmes d'IHM se fondent toutefois sur des plateformes X86 standard, que les administrateurs devraient «durcir» dans la mesure du possible (p. ex. désactiver les services et les ports inutilisés, éviter les comptes inutiles, restreindre l'accès, se servir des verrous du noyau) pour pouvoir garantir la fonctionnalité d'origine. Tout logiciel fourni qui n'est pas requis sur le système devrait être désinstallé. Ainsi, une IHM pour les systèmes de contrôle-commande ne nécessite pas de progiciels standard tels que les logiciels de traitement de texte, les tableurs ou les clients de messagerie, qui sont normalement fournis automatiquement sur les PC standard.

(3) La configuration des systèmes doit être gérée activement tout au long de leur cycle de vie. Il existe un certain nombre de techniques que les entreprises peuvent utiliser, telles que la création d'une «image» sécurisée pour configurer de nouveaux périphériques ou recréer des périphériques qui ne contiennent que le logiciel requis et dont la configuration comporte uniquement les services et ports nécessaires.

(4) Les mesures de sécurité des composants sont généralement les suivantes:

- Les mots de passe forts (ou robustes) pour tous les comptes utilisateur et les comptes utilisateur standard ou connus sur l'appareil sont modifiés (le système d'exploitation prend en charge de préférence les mots de passe forts et leur expiration).
- Des écrans de veille avec mot de passe sont installés dans la mesure du possible.
- Les correctifs du système d'exploitation et du microprogramme du matériel sont installés et mis à jour.
- Les protocoles sur les appareils sont configurés et surveillés.
- Les services et comptes inutilisés ou dont on n'a plus besoin sont désactivés.
- Les services non sécurisés (tels que telnet, remote shell (RSH) ou rlogin) sont remplacés par des alternatives plus sûres comme SSH.
- L'accès aux services ne pouvant pas être désactivés est restreint.
- Les sauvegardes système sont créées et testées de manière cohérente.
- Les ordinateurs portables et autres appareils mobiles qui ne sont pas connectés en permanence au réseau sont examinés et sécurisés séparément et, le cas échéant, isolés.

2.9.2 Protection contre les maliciels

(1) Les logiciels malveillants (virus et notamment chevaux de Troie) constituent une menace permanente et centrale pour toute infrastructure ICS. Il faut prendre des précautions pour détecter et empêcher leur introduction. Les logiciels et les composants des systèmes SCADA de traitement de l'information du contrôle-commande des réseaux, des stations et des centrales électriques sont vulnérables aux logiciels malveillants. Outre les défaillances de ces systèmes, la falsification de leurs fonctions et des données ou l'espionnage d'informations confidentielles peuvent également causer des dommages. Les utilisateurs de ces systèmes doivent donc être informés des dangers des logiciels malveillants

(2) Les responsables doivent, si nécessaire, prendre des mesures pour se protéger contre les logiciels malveillants ou pour les identifier et les supprimer ainsi que pour les surveiller. Une protection appropriée contre les maliciels doit être mise en œuvre sur tous les systèmes du périmètre et sur tous les postes de travail.

(3) Le balayage en ligne d'un ordinateur nécessite une certaine capacité de calcul, ce qui peut affecter le comportement en temps réel des systèmes SCADA. La mise en place d'une liste dite «noire» (blacklist) permet d'exclure des applications définies de l'exécution. Le processus est inverse dans le cas de la liste blanche (whitelist): seules des applications déterminées peuvent être exécutées. Cela évite le balayage permanent et décharge ainsi l'ordinateur des opérations qui y sont liées.

(4) Pour se protéger contre les maliciels, il faut tenir compte des points suivants:

- Sur les systèmes ICS équipés de systèmes d'exploitation universels (p. ex. Windows ou Linux), seuls les systèmes d'exploitation durcis doivent être utilisés.
- Dans la mesure du possible, les systèmes d'exploitation embarqués doivent être configurés de telle sorte que seuls les services requis soient actifs.
- Une protection contre les maliciels doit être mise en œuvre sur tous les systèmes du périmètre et sur tous les postes de travail.
- Les correctifs (patchs) de sécurité doivent être appliqués rapidement et classés par ordre de priorité dans la gestion des correctifs.
- Les systèmes ICS doivent être surveillés afin de détecter le plus rapidement possible les éventuels logiciels malveillants et activités de piratage.

2.9.3 Gestion des correctifs et des vulnérabilités

(1) L'application de correctifs (patchs) permet de réparer des failles de sécurité connues. Cela constitue un défi pour les administrateurs système, car la mise à jour du système et les correctifs peuvent perturber la fonctionnalité des ICS. Un correctif apporté à un composant ICS peut modifier son fonctionnement, ce qui risque d'entraîner sa défaillance ou une perte de sa fonctionnalité. Pour déterminer si le correctif a des conséquences involontaires, tous les patchs doivent être testés hors ligne dans un environnement de test avec le même matériel et le même logiciel qu'en production. De nombreux ICS utilisent en outre des versions du système d'exploitation plus anciennes, que le fabricant ne prend plus en charge.

(2) Les entreprises devraient mettre au point une approche systématique de la gestion des correctifs et des vulnérabilités pour les ICS. Il faut appliquer régulièrement des procédures standardisées afin d'identifier et d'éliminer systématiquement les points faibles techniques de l'infrastructure (réseau, clients, serveurs, applications, etc.).

(3) Les administrateurs devraient prévoir des procédures pour les mises à niveau et les correctifs logiciels réguliers. Le développement de procédures permettant d'appliquer rapidement les correctifs de sécurité et régulièrement les recommandations logicielles actuelles peut réduire fortement la surface exposée aux attaques des délinquants.

(4) Tous les composants de l'ensemble du système de processus doivent pouvoir faire l'objet de correctifs. L'application d'un correctif devrait si possible s'effectuer sans interrompre le fonctionnement normal et avec des conséquences mineures sur la disponibilité du système global. Il faut par exemple éviter de procéder à la mise hors service technique primaire de l'installation complète pour réparer les composants techniques secondaires. Les correctifs sont appliqués de préférence d'abord aux composants passifs redondants, puis installés sur les autres composants après un processus de commutation (passage au composant actif dans le système redondant) suivi d'un test. Le fabricant doit prendre en charge pour l'ensemble du système un processus de gestion des correctifs permettant de piloter et de gérer les tests, l'installation et la documentation des correctifs de sécurité et des mises à jour. Ces dernières doivent être effectuées par le personnel d'exploitation qui administre ces systèmes. L'installation ou la désinstallation des correctifs doit être autorisée par l'exploitant d'installation et ne doit pas se faire automatiquement.

(5) Les principes de la gestion du changement sont en général également applicables à la gestion des correctifs. Une gestion efficace des correctifs et des vulnérabilités comprend de plus habituellement les mesures suivantes:

- Des procédures régulières et standardisées sont documentées pour identifier et éliminer les points faibles techniques de l'infrastructure.
- Les correctifs visant à remédier aux failles constatées sont appliqués rapidement et classés par ordre de priorité dans la gestion des correctifs.
- Un concept ad hoc décrit les procédés et outils techniques de détection des vulnérabilités et régit les rôles et responsabilités en matière d'évaluation des risques, de correction, de tenue d'inventaire et de documentation.
- Les faiblesses identifiées sont documentées, classées et traitées en fonction de leur gravité dans le cadre de la responsabilité opérationnelle.
- Si un correctif est disponible pour corriger la vulnérabilité, les risques sont évalués avant de l'appliquer et comparés aux risques de cette dernière.
- Les nouveaux correctifs sont testés dans un environnement de test adéquat et ressemblant au maximum à l'environnement de production en termes de versions logicielles et de microprogramme.
- Des échanges réguliers ont lieu avec les fabricants.

2.9.4 Gestion et contrôle des accès

(1) Dans de nombreux réseaux ICS, différents systèmes sont utilisés par une grande variété d'utilisateurs. Ces systèmes doivent souvent être rapidement accessibles, comme l'exige p. ex. leur exploitation. Les méthodes d'authentification, d'autorisation et de gestion des comptes sécurisées au niveau de l'entreprise peuvent représenter un défi pour les ICS, car ils sont «toujours allumés». Les mécanismes d'authentification mis à disposition par les fournisseurs d'ICS sont également fréquemment restreints; ainsi, il n'est pas rare que les mots de passe soient limités quelques lettres. Les exigences courantes actuelles en matière de mots de passe sécurisés ne sont souvent pas ou seulement partiellement prises en charge par le matériel ou le microprogramme. La gestion d'un

grand nombre d'utilisateurs sur différents sites devient un défi lorsqu'il s'agit d'ajouter, de modifier et de supprimer l'accès au système et les changements de rôle des utilisateurs. Le même processus d'authentification peut contrôler l'accès à de nombreux systèmes (IHM, appareils de terrain, serveurs SCADA) et réseaux (réseaux locaux distants du sous-système) requérant l'utilisation de données d'identification partagées.

(2) Ces exigences de la part des utilisateurs contrastent en outre souvent avec celles liées à la menace ou à la sécurité: avec l'augmentation de la mise en réseau, le risque de propagation généralisée et rapide des logiciels malveillants s'accroît lui aussi, ce qui exige des barrières de sécurité plus élevées. Les fabricants réclament aujourd'hui de façon quasi standard des mécanismes d'accès basés sur les rôles (cf. p. ex. le livre blanc du BDEW), et la tendance s'oriente même vers un modèle de «confiance zéro» avec une virtualisation et des menaces croissantes (la sécurité de confiance zéro nécessite d'abandonner le vieux paradigme «faire confiance mais contrôler» et de passer à un nouveau paradigme presque paranoïaque «ne jamais faire confiance, toujours contrôler»).

(3) En principe, le contrôle de l'accès aux systèmes ICS peut être réparti ou centralisé. Pour la gestion répartie des accès, chaque système doit effectuer l'authentification séparément. Chacun d'entre eux recourt à un ensemble distinct de comptes utilisateur, d'informations d'identification et de rôles. Cette approche, qui constitue une bonne solution pour mettre en œuvre de petits ICS, n'est pas très évolutive pour les grandes entreprises.

(4) On utilise la plupart du temps un système centralisé de gestion des comptes pour administrer un grand nombre d'utilisateurs et de comptes. Il faut habituellement disposer d'un système d'authentification centralisé (p. ex. Active Directory ou Lightweight Directory Access Protocol (LDAP)) pour gérer les comptes. Un protocole d'authentification (p. ex. Kerberos, Remote Authentication Dial-In User Service (RADIUS) ou Terminal Access Controller Access-Control System (TACACS)) assure la communication entre le serveur d'authentification et l'ICS. Une approche centralisée est évolutive pour les implémentations de systèmes de grande envergure, mais entraîne également des risques supplémentaires tels que le point de défaillance unique (single point of failure ou SPOF) dans les environnements ICS: Les serveurs centraux doivent être très sécurisés, car l'ensemble du système de contrôle-commande peut être compromis si le serveur d'authentification est menacé. Ces serveurs centraux sont également nécessaires en cas d'urgence et pourraient engendrer des pertes de disponibilité sans redondance.

(5) En résumé, il convient de tenir compte des points suivants:

- Une directive relative au contrôle d'accès est documentée et mise en œuvre sur la base des exigences de sécurité de l'entreprise et de l'information.
- Il faut définir et implémenter le concept d'autorisation basé sur les rôles, tous les accès aux applications et aux systèmes devant être mis en œuvre selon ce concept.
- L'application des conditions et prescriptions d'utilisation des comptes de groupe, lorsque le recours aux comptes utilisateur personnels est impossible, doit décrire des règles précises en matière d'exceptions et des mesures complémentaires pour garantir un niveau suffisant de sécurité d'accès et de traçabilité.
- Les conditions et règles s'appliquant aux systèmes qui ne prennent pas en charge une politique de mots de passe forts ou qui la rendent impossible pour des raisons d'exploitation devraient notamment définir des mesures supplémentaires afin de garantir une sécurité d'accès suffisante.
- L'utilisateur ne peut avoir accès qu'au réseau et aux services expressément autorisés.

- Un processus formel d'enregistrement et de déconnexion des utilisateurs est mis en œuvre pour permettre l'attribution des droits d'accès.
- Un processus formel de préparation de l'accès des utilisateurs doit être réalisé pour permettre l'attribution ou la révocation des droits d'accès de tous les types d'utilisateurs à l'ensemble des systèmes et des services.
- L'attribution et l'utilisation des droits d'accès privilégiés sont restreintes et contrôlées.
- L'affectation des informations secrètes d'authentification est contrôlée par un processus de gestion formel.
- Les propriétaires d'installations doivent vérifier les droits d'accès des utilisateurs à intervalles réguliers.
- Les droits d'accès de tous les collaborateurs et prestataires de services externes aux dispositifs de traitement de l'information sont supprimés ou modifiés après la résiliation de leurs rapports de travail, de leur contrat ou d'une convention.
- Les utilisateurs doivent suivre et appliquer les pratiques prescrites en matière d'emploi des mots de passe.
- Dans le domaine du contrôle de processus, il n'est pas toujours possible de garantir l'utilisation de mots de passe sécurisés, p. ex. souvent, les systèmes hérités (aussi appelés systèmes patrimoniaux ou legacy systems) ne permettent pas de mots de passe individuels et/ou suffisamment forts.
- Il est généralement impossible d'exploiter des systèmes dotés de services d'annuaire centralisés qui fonctionnent dans des installations décentralisées, telles que des postes de transformation ou des unités de production dispersées, ce qui signifie qu'il faut utiliser des comptes et mots de passe locaux. Il est donc pratiquement impossible de changer de mot de passe régulièrement.
- C'est pourquoi il convient d'indiquer clairement à l'utilisateur les cas où la politique générale en matière de mots de passe s'applique, ceux où il faut utiliser des mots de passe différents ou encore ceux où l'emploi d'un mot de passe est absolument impossible (systèmes hérités).
- Le mot de passe choisi devrait être le plus sûr possible, notamment dans les situations où l'accès général au système se fait au moyen d'un seul mot de passe. Les mots de passe par défaut utilisés par les fournisseurs de systèmes devraient en particulier être considérés comme peu sûrs et largement connus. Les mots de passe ne devraient être accessibles qu'aux personnes participant à l'exploitation du système.
- Ces situations doivent être documentées et examinées périodiquement.
- L'accès aux informations et aux systèmes applicatifs doit être limité conformément à la politique d'accès.
- Les systèmes de gestion des mots de passe doivent être interactifs et prendre en charge ou faire respecter les règles de mots de passe exigées sur le plan qualitatif.
- Si la politique de contrôle d'accès l'exige, l'accès aux systèmes et aux applications doit être contrôlé par une procédure de connexion sécurisée.

2.9.5 Gestion des sauvegardes et restauration du système

(1) Diverses raisons et intentions peuvent expliquer la création de sauvegardes: les données et les informations sont protégées contre la perte ou la manipulation ou font l'objet d'un archivage de longue durée sur différents supports; les logiciels et leur configuration peuvent être conservés ou servent à la résilience en cas d'attaque de logiciels malveillants (p. ex. cryptage); la restauration est rapide en cas d'interruption physique, etc. Par le passé, de telles sauvegardes s'effectuaient la plupart du temps sur des supports peu coûteux comme les bandes magnétiques. Suite à

l'effondrement du prix des disques physiques, elles sont de plus en plus créées en ligne sur des disques disponibles selon une structure hiérarchique. Alors que dans le premier cas, trois ensembles de données étaient généralement sauvegardés séparément et stockés plus longtemps suivant un schéma de rotation «grand-père/père/fils», dans le second cas, ils ne sont souvent conservés en ligne que sur une période définie, habituellement trois mois. Or cela peut entraîner la perte totale des données, des informations, des logiciels et des configurations, en particulier en cas d'infestation par un logiciel malveillant (en général un randsomware, ou rançongiciel), qui n'est réalisée qu'au bout d'un certain temps. Il est donc important d'utiliser également des systèmes d'archivage dans ce type de cas, afin que les données ne soient pas perdues, volées ni cryptées par un randsomware qui les rendra ainsi inaccessibles et causera au final leur perte.

(2) Tant au niveau de la transmission que du stockage, les sauvegardes doivent être conservées de manière à être protégées contre tous les risques qui peuvent également s'appliquer aux données et aux systèmes en exploitation productive. Il en va de même lors des éventuelles phases de restauration, au cours desquelles les sauvegardes sécurisées doivent être restaurées dans un environnement productif, temporaire ou transitoire.

(3) Dans le cadre du plan de continuité des activités (business continuity plan) à l'échelle de l'entreprise, il faut également élaborer un plan de restauration des moyens IT et OT. Un tel plan de reprise après sinistre (disaster recovery plan) se base sur la criticité des exigences opérationnelles, qui définissent quels sont les éléments à restaurer, dans quel délai et dans quel ordre. En s'appuyant sur ces informations, on établit des plans détaillés qui fournissent des instructions conformes au manuel en vue du redémarrage, de sorte que même les personnes possédant les connaissances techniques de base requises mais ne disposant peut-être pas des connaissances approfondies propres à l'entreprise peuvent restaurer un environnement. Ces plans doivent être continuellement mis à jour lorsque des changements sont apportés aux environnements, et ils doivent également faire l'objet de formations et de vérifications périodiques. Pour ce faire, on procède habituellement chaque année à des tests de récupération qui peuvent aller de simples «passages en revue» sur papier à des simulations exhaustives de scénarios d'urgence.

(4) Les mesures de sauvegarde et de récupération comprennent les éléments suivants:

- Sauvegarde des données: la création de copies de sauvegarde des données, des logiciels et des configurations est définie, effectuée régulièrement et testée selon un cycle convenu.
- Les supports de sauvegarde sont conservés dans un endroit éloigné et protégés contre les influences environnementales (température, incendie, humidité, rayonnement électromagnétique, etc.), ainsi que contre le vol, la manipulation ou la destruction.
- La continuité de la sécurité de l'information est intégrée au système de gestion de la continuité des activités (business continuity management system ou système BCM) à l'échelle de l'entreprise.
- L'entreprise définit et met en œuvre ses exigences en matière de sécurité de l'information et de continuité en situations normales, d'urgence, de catastrophe et de crise.
- Pour pouvoir satisfaire aux exigences de continuité, l'entreprise doit documenter, appliquer et mettre à jour des processus, des procédures et des contrôles.
- L'entreprise vérifie à intervalles réguliers les mesures établies et mises en œuvre en vue de la sécurité de l'information et de sa continuité pour s'assurer qu'elles sont valides et efficaces.
- Les exigences légales, régulatoires et de l'entreprise en matière d'archivage à long terme sont définies, mises en œuvre et contrôlées régulièrement.

- Plan de reprise après sinistre (disaster recovery plan ou DRP): un plan d'ensemble comprenant les responsabilités du personnel, des plans d'accessibilité, des dispositifs alternatifs et des plans de redémarrage détaillés est établi.

2.9.6 Cas particuliers (appareils de terrain, éléments virtuels, etc.)

a) Appareils de terrain

(1) De nombreux appareils de terrain (DEI de terrain ou de protection, anciens automates programmables et RTU) ne disposent souvent pas – ou seulement de manière limitée – des fonctions de sécurité que possèdent d'autres composants, tels que les PC Windows. Ils ne peuvent donc pas être gérés de manière centralisée. La plupart du temps, ces dispositifs ne bénéficient que d'une protection physique dans la mesure où ils sont exploités dans des pièces ou des armoires fermées à clé. Or il serait également important de protéger la configuration de ces appareils sans pour autant restreindre les fonctionnalités requises.

b) Appareils mobiles (smartphones, tablettes)

(1) Les smartphones, tablettes et autres dispositifs similaires sont de plus en plus utilisés pour la commande et la surveillance locales. Ces appareils mobiles doivent être sécurisés autant que possible pour empêcher les maliciels de pénétrer dans le contrôle-commande de la station. Un organisme devrait en outre gérer l'équipement employé pour garantir le respect des normes de sécurité de l'entreprise. Il faut aussi tenir compte des interfaces avec le contrôle-commande de la station (p. ex. WLAN), qui exigent des mesures de sécurité appropriées afin de ne pas pouvoir être utilisées pour l'accès non autorisé à ce dernier.

2.10 Surveillance de la sécurité

«La sécurité n'est pas un état, c'est un processus!»

(1) Cette maxime se vérifie de plus en plus. Un système qualifié de «sûr» ne décrit jamais que l'état à l'instant t. L'idée de la «sécurité comme processus continu» reconnaît en revanche que la sécurité absolue n'existe pas et qu'il faut donc toujours s'attendre à de nouveaux incidents en la matière. Dans ce contexte, il est primordial de renforcer au préalable les capacités de l'organisation pour pouvoir détecter à temps la survenue de nouveaux incidents de sécurité.

2.10.1 Principes et fondements

(1) L'utilisation de systèmes et de réseaux de surveillance pour procéder à des adaptations afin de discerner les comportements anormaux ou les signatures d'attaque peut s'avérer difficile dans un environnement ICS. Les fonctions de surveillance et de détection sont toutefois essentielles au concept de défense en profondeur destiné à assurer la protection des infrastructures critiques. Des jonctions totalement renforcées et surveillées vers d'autres réseaux ne suffisent pas à protéger efficacement les actifs stratégiques d'un accès non autorisé. Car les cybercriminels savent comment contourner toute protection déployée dans un environnement réseau. Le concept de défense en profondeur énonce que le système d'une entreprise doit détecter et faire remonter l'intrusion à un stade précoce, afin que des mesures défensives soient prises avant que les fonctions des infrastructures critiques ne soient entravées. La plupart des sociétés informatiques ont un certain degré de surveillance au niveau de l'entreprise, mais elles ne l'utilisent que rarement dans les réseaux ICS.

(2) Sans surveillance du système, des intrus pourraient lui porter atteinte et personne n'en saurait rien avant qu'ils n'aient atteint leur objectif. Alors que la communauté des fournisseurs d'ICS est consciente de la nécessité d'une surveillance centralisée de la sécurité de ces systèmes, l'intégration des fonctions de surveillance standard à l'ICS en est encore à ses balbutiements. Les exploitants d'installations peuvent et doivent prendre des mesures pour s'assurer que le personnel de sécurité et les exploitants OT sont au courant des modifications de systèmes ou des changements de comportements indiquant une intrusion potentielle dans l'environnement ICS.

(3) Les entreprises peuvent surveiller leurs réseaux et collecter des informations à leur sujet de plusieurs façons, telles que l'utilisation de serveurs Syslog centralisés pour les équipements Linux et réseau et la centralisation des événements Windows avec WinRM (Windows Remote Management) et WEVTUTIL (outil Windows de gestion des journaux d'événements). Toutefois, ces événements (journaux) doivent être contrôlés en permanence. Des solutions, telles que la gestion des informations et des événements de sécurité (security information and event management ou SIEM), combinent la gestion des informations de sécurité (security information management ou SIM) et la gestion des événements de sécurité (security event management ou SEM), et peuvent collecter, consigner et corréler des informations provenant de sources multiples pour attirer l'attention sur des activités anormales ou spécifiées. Ces systèmes peuvent de plus fournir une analyse en temps réel. Les «canaries» et pots de miel/réseaux de pots de miel (honeypots/honeynets) peuvent également marquer toute intrusion non autorisée, et les exploitants d'installations devraient envisager de les utiliser dans les zones à haute criticité/à haut risque. L'introduction d'un SIEM est indispensable pour l'investigation informatique. Il est ainsi possible de rechercher et de détecter les attaques survenues et les vulnérabilités exploitées.

2.10.2 Systèmes de détection et de prévention des intrusions

(1) Les environnements ICS offrent une occasion unique de surveiller les mécanismes de protection sur le réseau. Bien que le trafic réseau soit considérable, il est très simple, car il s'agit de réseaux plutôt statiques. Ainsi, dans un environnement ICS type, l'automate programmable (PLC) communique de manière standardisée avec l'IHM et le serveur d'archivage. Les applications et les services du système de commande des processus (PCS) sont tous connus, et les protocoles, les connexions et le trafic réseau nécessaire sont définis et prévisibles. Les exploitants d'installations peuvent recourir à une solution IDS pour surveiller facilement l'ensemble de l'environnement ICS et pour mettre en place des alertes pour tout événement, même en dehors du fonctionnement normal. Un IDS se base sur la surveillance passive du trafic réseau. Le trafic réseau escompté est déterministe, et les écarts sont utilisés comme déclencheurs d'alerte. Il est possible d'écrire des règles simples pour surveiller les sources et les cibles IP, les protocoles, les longueurs de paquets, etc. De nombreux fournisseurs d'ICS peuvent eux aussi mettre à disposition des définitions et des descriptions de leurs systèmes IDS.

(2) Les solutions IPS sont toujours utilisées en relation avec des pare-feux ou des appareils ICS et peuvent bloquer le trafic réseau qui ne respecte pas les règles fixées. De nombreux fournisseurs et exploitants d'installations font preuve d'inquiétude et de prudence lors de l'utilisation d'IPS, car le blocage d'un service peut nuire au fonctionnement des installations et l'exploitation continue n'est alors plus garantie. Cependant, en raison de la nature déterministe du trafic ICS, les IPS ne peuvent être adaptés qu'à des anomalies extrêmes. L'IDS et l'IPS constituent un élément essentiel de la stratégie de défense en profondeur. Un réseau ICS peut comporter un grand nombre de vulnérabilités insoupçonnées. Un IDS/IPS permet d'être attentif aux imprévus et d'y réagir de manière

automatisée. Pour autant, tous les problèmes ne peuvent pas être éliminés grâce à ce système. L'IDS et l'IPS peuvent être décrits sommairement comme suit:

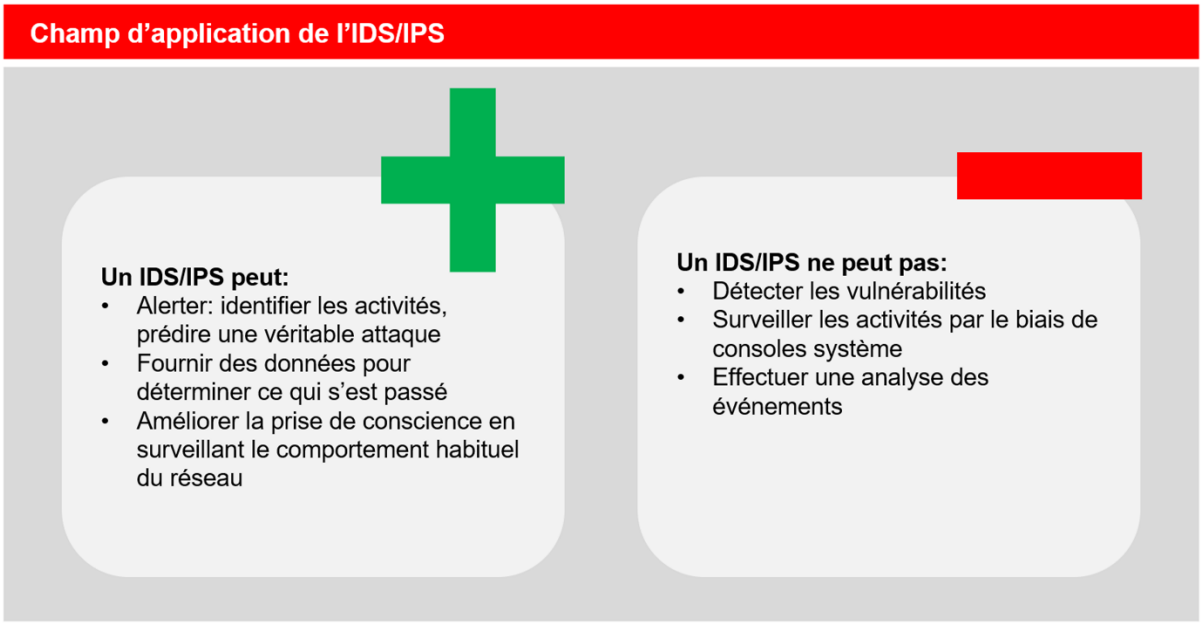

Figure 22 Champ d'application et délimitation de l'IDS/IPS

Fonction	Description
IDS	Un système de détection des intrusions (intrusion detection system ou IDS) vise à identifier les attaques dirigées contre un système ou un réseau informatique. L'IDS peut compléter un pare-feu ou fonctionner directement sur le système informatique à surveiller, augmentant ainsi la sécurité des réseaux et des ordinateurs. Les attaques détectées sont généralement collectées dans des fichiers journaux et signalées à l'utilisateur ou à l'administrateur; l'IDS se distingue sur ce point du système de prévention des intrusions (intrusion prevention system ou IPS), qui prévient les attaques de manière automatisée et active.
IPS	Les systèmes de détection et de prévention des intrusions sont des outils qui surveillent activement les systèmes ou réseaux informatiques. L'objectif est de filtrer les événements indiquant des attaques, des tentatives d'abus ou des atteintes à la sécurité, ces événements devant être repérés et signalés rapidement. Les procédures se basent sur la reconnaissance de formes pour indiquer une divergence par rapport à un état normal. Des méthodes heuristiques sont également utilisées pour détecter des attaques jusqu'ici inconnues. Alors que l'IDS peut uniquement déceler les attaques, l'IPS doit également les bloquer ou les prévenir. Or ce terme a été inventé à l'origine par le marketing: c'est pourquoi sa désignation sous le nom de système de prévention des intrusions est parfois controversée.

Tableau 11 Description fonctionnelle de l'IDS et de l'IPS

(3) Les systèmes de détection des intrusions (IDS) sont des systèmes autonomes qui détectent les intrus et préviennent les attaques sur les systèmes et réseaux informatiques. Il faudrait que ces systèmes

de surveillance IDS ne soient pas connus, n'offrent aucun service, consignent les attaques, repèrent les intrus et, si possible, prennent des contre-mesures. Tout événement anormal sur le réseau devrait être identifié et consigné par le système IDS. À cet effet, les méthodes IDS utilisent des capteurs ou des renifleurs qui détectent tout trafic de données inhabituel et le comparent à des formes prédéfinies. Dans ce contexte, on établit une distinction entre la détection des abus (misuse detection) et celle des anomalies (anomaly detection).

(4) La détection des abus se fonde sur la comparaison de formes – autrement dit de motifs – ou de signatures. Pour ce faire, on compare les formes enregistrées à d'autres motifs d'une base de données, qui sont principalement utilisés par les intrus. Avec cette méthode, baptisée appariement de formes ou filtrage par motif (pattern matching), seuls les schémas d'attaque déjà connus sont repérés. Les nouvelles attaques, dont il n'existe pas encore de schéma, passent inaperçues.

(5) Dans le cas de la détection d'anomalies, en revanche, tout comportement qui s'écarte du trafic de données normal est considéré comme une attaque. Ce procédé permet également de détecter les divergences par rapport aux attaques précédentes. Il est inutile de mettre à jour les schémas d'attaque dans une base de données. Cependant, dans la détection d'anomalies, il est nécessaire de définir quel motif fait partie du trafic de données normal, ce qui peut entraîner une augmentation du seuil pour les fausses alertes.

(6) Ces deux méthodes illustrent l'évolution du système IDS vers les systèmes de prévention des intrusions (IPS), qui bloquent le passage de certains paquets de données.

Méthodes de détection	
Détection basée sur les signatures	- Surveille certains événements - Ne contrôle que ce qui lui a été dit - Peut faire face à toute menace connue - Ne détecte pas les changements de configuration du réseau - Inspection objective importante - Comportement prévisible - Facilité d'utilisation
Détection basée sur les anomalies	- Surveille l'évolution des tendances - Tire des enseignements des changements progressifs - Peut faire face à des menaces inconnues, chaque intrusion déclenche une alerte - Sensible aux variations au sein des réseaux - Approche subjective, sujette aux erreurs d'interprétation - Comportement imprévisible - Le système doit être entièrement fiable

Tableau 12 Différences entre la détection basée sur les signatures et la détection basée sur les anomalies

Critères de sélection	
Détection basée sur les signatures	- Analyse le trafic réseau (paquets) à la recherche de motifs connus - N'analyse que le trafic sur ou de son propre réseau - Peut explorer les deux côtés d'une connexion - Peut réagir et bloquer le trafic (mode IPS) - Ne distingue pas le trafic – ignore souvent si un système est Windows, Linux ou un automate programmable
Détection basée sur les anomalies	- Doit apprendre au système à identifier le trafic réseau «normal» (et que faire si des attaques se produisent en période d'apprentissage?) - Détecte les écarts par rapport au comportement normal - Plus difficile à manipuler ou à tromper - Aucune connaissance des signatures d'attaque requise - Peut provoquer davantage de fausses alertes - Très difficile et complexe à mettre en œuvre dans un environnement dynamique

Tableau 13 Principes de détection des systèmes basés sur les signatures et les anomalies

(7) En matière de technologie IDS, il existe également des solutions basées sur le réseau (network intrusion detection system ou NIDS) et des approches basées sur un hôte (host intrusion detection system ou HIDS).

(8) Contrairement à un système de détection des intrusions (IDS), le système de prévention des intrusions (IPS) n'a pas de fonction de surveillance ni de déclenchement d'alerte, mais contrôle directement le trafic. Le système IPS est directement connecté aux lignes et surveille les paquets de données entrants et sortants des composants du réseau. Les attaques et les configurations binaires qui s'écartent du trafic de données normal sont détectées par le biais des signatures et bloquent le trafic. Cette fonction de verrouillage est prise en charge par des comportements intelligents et des algorithmes anormaux qui fonctionnent au niveau applicatif.

(9) Les systèmes IPS devraient être en mesure d'analyser les données à grande vitesse et ne doivent pas bloquer le trafic légitime, même en cas de forte charge. Les mécanismes de protection, tels que les analyses de signatures, la détection des écarts de protocole, les fonctions de pare-feu et les contrôles d'accès, doivent être robustes.

2.10.3 Surveillance des incidents et des événements de sécurité

(1) Les journaux d'audit de sécurité contiennent des informations sur l'activité de connexion, l'utilisation des ressources, les modifications de fichiers et d'autres informations touchant à la sécurité. Sans des pratiques d'audit et d'enregistrement correctement configurées et mises à jour, les équipes d'intervention en cas d'incident ne peuvent souvent pas déterminer l'importance d'un événement potentiel. Des journaux d'audit correctement configurés au niveau du réseau, de l'hôte et des applications fournissent des informations critiques pour déterminer la manière dont un événement s'est produit, l'impact et la portée du problème, ainsi que la façon de prévenir au mieux les événements futurs.

(2) Des politiques complètes de gestion et d'analyse des journaux définissent les exigences minimales relatives aux appareils, aux systèmes d'exploitation et aux applications. Les paramètres de sécurité et les contrôles d'accès des utilisateurs font respecter ces exigences. Si les exploitants d'installations ne configurent pas les systèmes et les applications pour enregistrer les événements clés, ils ne peuvent pas saisir de données importantes sur ces événements et les équipes d'intervention en cas d'incident peuvent ne pas disposer de suffisamment d'informations pour déterminer la cause d'un événement.

(3) La définition d'une base de référence de la fonctionnalité attendue du trafic et des processus pour les opérations normales et exceptionnelles et l'utilisation du système permet d'isoler la commande des processus et le pilotage des systèmes d'exploitation des actions inhabituelles du trafic de données ou de l'utilisateur, ce qui pourrait indiquer des incidents de sécurité potentiels.

(4) Les systèmes d'exploitation et applications plus récents offrent des options plus détaillées de configuration et d'audit d'événements. L'utilisation de la configuration standard pour la plupart des journaux d'exploitation et d'application ne fournit cependant que des fonctions minimales de surveillance et de journalisation, et les exploitants peuvent manquer un événement critique. Il importe que le personnel d'exploitation et de sécurité dans l'environnement ICS examine toutes les capacités de surveillance et d'enregistrement et configure les systèmes de manière à ce qu'ils ne mettent à disposition que les données nécessaires pour saisir tous les événements potentiellement pertinents. Il faut s'assurer que les paramètres ne génèrent pas de journaux inutiles qui pourraient surcharger les capacités de stockage du système. Dans les configurations standard, les données peuvent être écrasées. En conséquence, exportez tous les journaux et protocoles vers un serveur central ou un système de gestion des événements pour garantir leur disponibilité en cas de besoin.

2.10.4 Surveillance des incidents et des événements de sécurité SIEM (SIM et SEM)

(1) Non seulement les technologies SIEM prennent en charge le processus de réponse aux incidents, mais elles peuvent aussi soutenir les exploitants d'ICS. Si elles sont correctement configurées et analysées, les données peuvent aider à prédire les défaillances des appareils, les capacités en matière d'équipement et les points de défaillance, ainsi qu'à fournir des informations relatives à la sécurité. Les exploitants d'installations peuvent les configurer de façon à ce qu'elles donnent l'alerte lorsqu'un incident de sécurité potentiel se produit. Les solutions SIEM sont capables de synthétiser une grande quantité de données d'événements et de journaux nécessaires, qui proviennent des composantes ICS et s'accumulent. En offrant une visibilité sur les données de sécurité agrégées, les SIEM peuvent réduire au maximum le temps de réaction à l'incident.

(2) Un SIEM centralise les informations des équipements réseau, des systèmes d'exploitation et des bases de données au sein d'environnements ICS complexes. Il simplifie le processus d'examen du journal de vérification en transférant les journaux de plusieurs systèmes vers une seule solution qui élimine le temps et l'effort requis pour évaluer manuellement ces journaux. Les exploitants peuvent mettre en place un SIEM de manière à intégrer plusieurs formats de journaux à partir de sources éparpillées, ce qui permet de collecter les informations requises à distance et automatiquement.

(3) Le SIEM peut également intégrer les informations IDS/IPS et les résultats d'analyse, puis générer des alertes sur les formes de trafic identifiées. Le moteur d'analyse du SIEM accélère le traitement et le formatage des données, réduisant ainsi le coût de ces processus. Cela facilite par ailleurs la vérification des données fonctionnelles, d'exploitation et de sécurité. L'utilisation d'un SIEM offre en

outre la possibilité de sélectionner des événements spécifiques pour le reporting de conformité, l'analyse des causes profondes de défaillances et la détection des incidents.

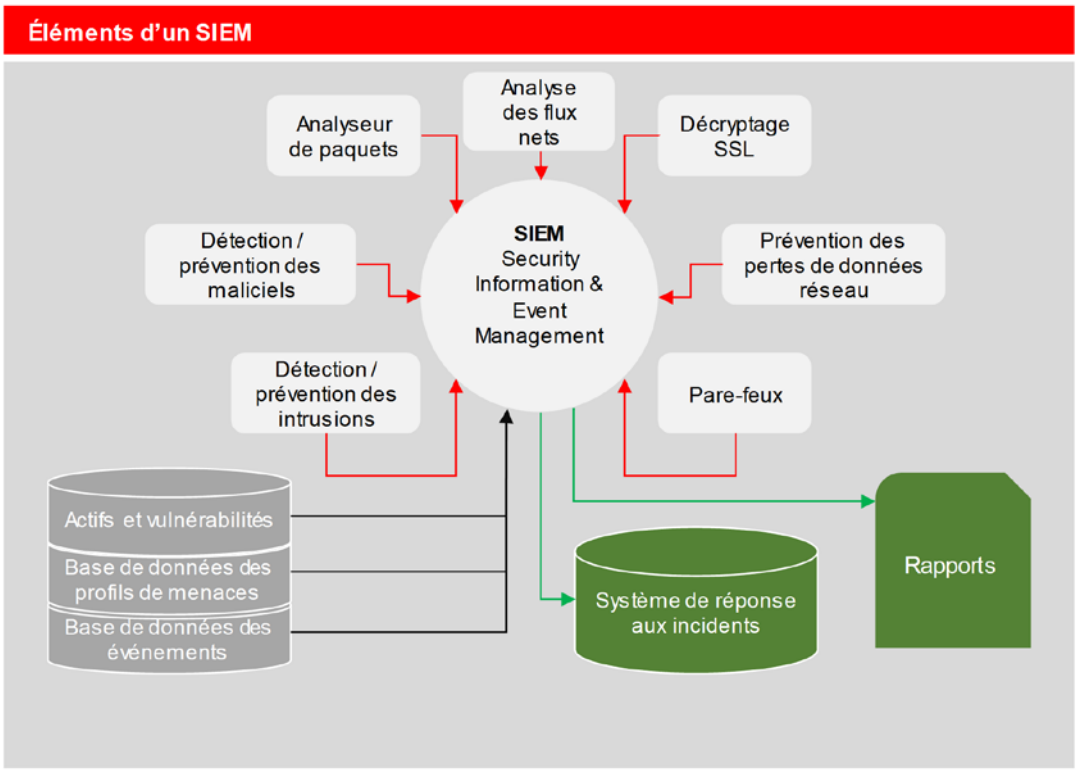

Figure 23 Éléments d'un SIEM (1)

Figure 24 Éléments d'un SIEM (2)

a) SIM (security information management)

(1) Dans un système de gestion des informations de sécurité (SIM), les événements et les fichiers journaux provenant des emplacements les plus divers sont collectés dans des systèmes de communication en vue de les associer, de les archiver, de les traiter et de les analyser en temps réel, l'objectif étant d'élaborer des rapports actuels et historiques à partir de ces données. Une telle gestion des informations de sécurité (SIM) correspond à la gestion des journaux.

(2) Le SIM surveille le réseau en temps réel et l'analyse pour détecter les événements critiques. Les événements peuvent être évalués sous différents angles, tels que le point de vue de l'utilisateur, qui conduit à s'interroger sur le lieu et le moment où une personne s'est connectée et la manière dont elle a procédé, sur les systèmes auxquels elle a accédé et sur les événements que cela a déclenchés.

(3) Étant donné que les données des systèmes SIM proviennent de sources différentes, qu'il s'agisse de composants réseau, de systèmes, de pare-feux, d'applications ou de logiciels antivirus, leur contenu est adapté à leur fonction. Ces outils évaluent donc les événements qui surviennent sous des angles radicalement différents. Ils disposent en outre des formats les plus divers qu'une plateforme SIM doit traiter.

(4) La gestion des informations de sécurité (SIM) se combine avec la gestion des événements de sécurité (SEM) pour former la gestion des informations et des événements de sécurité (SIEM).

(5) La gestion des journaux (log management) correspond à la notion de SIM (security information management) et désigne la collecte, la transmission, le stockage, l'analyse et le transfert centralisés des données de journalisation issues des composants réseau, des systèmes d'exploitation et des applications. Parmi ses fonctionnalités typiques, citons les analyses axées sur les politiques – y compris celles concernant les tendances –, les rapports périodiques et les fonctions de base destinées aux messages d'alerte, ce qui en fait le fondement de l'investigation informatique et de la gestion des niveaux de service (service level management ou SLM). Selon le fournisseur, la gestion des journaux offre un stockage des données de journalisation sécurisé et conforme aux exigences en matière de révision et tient compte des directives en matière de protection des données lors de la représentation de ces dernières.

b) SEM (security event management)

(1) La gestion des événements de sécurité (SEM) se caractérise par une surveillance en temps réel, la corrélation des fichiers journaux en fonction de règles prédéfinies, la notification et l'affichage sur la console ainsi que des fonctionnalités d'alarme. Cette gestion couvre les fonctions des systèmes IDS et IPS pour la détection et la protection des intrusions et surveille le trafic réseau afin de repérer les anomalies et les motifs répétitifs.

(2) Le SEM (security event management) prend en charge la corrélation des journaux en s'appuyant sur des règles définies, compare ces données automatiquement à des référentiels ou à des normes comme ITIL, COBIT, la loi SOX ou ISO et dispose de fonctionnalités d'alarme en temps réel performantes. Le SEM et l'IDS/IPS (intrusion detection system/intrusion prevention system) se recoupent en partie. Lorsqu'ils sont basés sur le réseau, ces systèmes surveillent l'utilisation et la communication de ce dernier ainsi que les ports, et détectent les motifs ou les écarts dans le trafic réseau. En tant que solutions basées sur l'hôte, ils contrôle les manipulations de fichiers et surveillent par exemple les stratégies de groupe et les comptes utilisateur.

Approche visant à renforcer la cybersécurité

3. Détermination du niveau de sécurité mis en œuvre (évaluation)

(1) Pour réduire le risque qui pèse sur les réseaux et systèmes ICS, il ne suffit pas simplement de recourir à des technologies de sécurité au sein des environnements ICS. Bien que les ICS plus récents appliquent souvent les mêmes protocoles sous-jacents que ceux utilisés dans les réseaux informatiques et d'entreprise, le mode de commande ou la fonctionnalité des systèmes de contrôle-commande (combinés aux exigences d'exploitation et aux disponibilités) peuvent rendre inappropriées des technologies de sécurité omniprésentes, comme les programmes antivirus. Certains secteurs ICS, tels que ceux de l'énergie, des transports et des produits chimiques, sont soumis à des contraintes de temps, de sorte que les problèmes de latence et de débit introduits par les solutions de sécurité peuvent causer des retards et affecter les performances optimales du système. Au vu de l'évolution des réseaux de commande, qui passent du statut de domaines autonomes à celui de réseaux interconnectés coexistant avec les environnements informatiques d'entreprise, les administrateurs système doivent mettre en œuvre des contre-mesures qui n'entravent pas la fonctionnalité. Il est essentiel de comprendre les vulnérabilités et les vecteurs d'attaque qui y sont liés et de savoir comment les exploiter pour élaborer une stratégie efficace d'atténuation de la sécurité.

3.1 Modèle de sécurité proactif

(1) Lorsqu'il s'agit de protéger une infrastructure d'information, les pratiques de sécurité débutent par un modèle de sécurité proactif (cf. figure 25). La plupart des programmes de sécurité sont des applications réactives d'architectures de sécurité; ils réagissent après un incident ou font des compromis. Ils sont généralement coûteux et peuvent interrompre l'exploitation continue des installations critiques en matière d'approvisionnement.

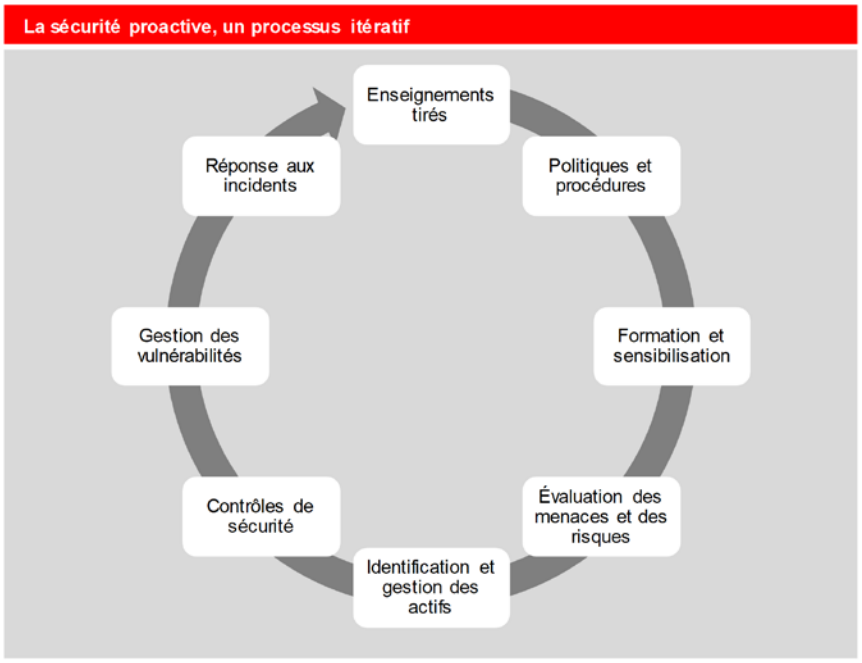

Figure 25 La sécurité proactive, un processus itératif

(2) Pour développer une stratégie solide de défense en profondeur, on commence par s'assurer qu'il existe des politiques et des procédures soutenant les comportements escomptés. Il convient d'établir des directives pour la formation des individus afin de garantir qu'ils effectuent leur travail en toute sécurité. Une stratégie robuste de défense en profondeur identifie les menaces et les risques et est à même d'évaluer leur impact. Elle élabore également une cartographie de l'architecture ICS et comprend un inventaire complet de tous les actifs ICS. Un inventaire précis et bien documenté permet à l'entreprise de bénéficier d'une analyse réaliste des risques effectuée par les administrateurs système, ce qui suppose d'appliquer des contrôles de sécurité basés sur la priorité en matière d'actifs et de mettre en place des contre-mesures efficaces pour gérer les vulnérabilités. Les propriétaires d'installations devraient évaluer les incidents en fonction de leur impact et apprendre comment y faire face ou prendre des contre-mesures appropriées. Les connaissances acquises tout au long du processus doivent être intégrées à l'adaptation permanente des contrôles de programmes et de sécurité afin de garantir une amélioration continue de la sensibilisation aux menaces émergentes et aux modifications subséquentes du système.

4. Mesures à mettre en œuvre

(1) Le cadre du National Institute of Standards and Technology (NIST) destiné à améliorer la cybersécurité des infrastructures critiques (Framework for Improving Critical Infrastructure Cybersecurity) et ses recommandations visent à fournir aux exploitants de ces infrastructures un instrument leur permettant d'accroître leur résilience de manière autonome et responsable. À cet égard, il prend également en compte la recherche de rentabilité et d'efficacité, ainsi que la confidentialité et la protection des données. Afin de faciliter la poursuite du développement et l'innovation technique, le cadre du NIST est technologiquement neutre. Il se base sur une sélection de normes, de directives et de bonnes pratiques existantes.

Noyau / vue d'ensemble

(2) Le noyau du cadre du NIST est une approche fondée sur le risque, 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. *Rétablir (Recover)*

(3) Ensemble, ces cinq fonctions forment une vision stratégique de la gestion des risques liés à la cybersécurité d'une organisation.

Niveaux de mise en œuvre

(4) Les niveaux de mise en œuvre du cadre fournissent le contexte général de la gestion du risque de cybersécurité et de l'organisation des processus y afférents. Les différents niveaux décrivent le degré ou le stade de développement qu'une entreprise a mis en œuvre (p. ex. le risque et la menace; qui sont reproductibles et adaptables). Ces niveaux caractérisent le stade de développement d'une organisation, qui va de partiel (niveau 1) à adaptatif (niveau 4). Ils reflètent une progression des approches informelles et réactives vers des stratégies agiles et axées sur les risques. Au cours du processus de sélection du niveau, une organisation devrait avoir une connaissance approfondie de ses pratiques actuelles de gestion des risques, de l'environnement de la menace, des exigences légales et régulatoires, des objectifs d'affaires et des contraintes organisationnelles.

Profils

(5) Le profil peut être caractérisé comme un alignement des normes, des directives et des pratiques du noyau du cadre sur un scénario de mise en œuvre individuel. Les profils peuvent être utilisés pour identifier les options permettant d'améliorer la cybersécurité en associant un profil «réel» à un profil «cible». Pour élaborer un tel profil, une organisation peut examiner toutes les catégories et sous-catégories et les évaluer en fonction des objectifs d'affaires et de l'estimation des risques. Il est possible d'ajouter des catégories et des sous-catégories afin d'ajuster les risques de l'organisation.et d'y faire face. Le profil peut également servir à l'auto-évaluation au sein d'une organisation ou entre organisations et à illustrer les progrès réalisés pour passer du profil réel au profil cible.

(6) Les titres des chapitres prédéfinis couvrent les thèmes à traiter. Le contenu de ces chapitres peut être consulté, repris ou référencé à partir de la norme minimale de cybersécurité publiée par l'Approvisionnement économique du pays.

4.1 Stratégie de sécurité – Identify

Gestion d'inventaire (Asset Management)

(1) Les données, les personnes, les appareils, les systèmes et les installations d'une organisation sont identifiés, catalogués et évalués en fonction de leur criticité vis-à-vis des processus d'affaires à exécuter, ainsi que de la stratégie de l'organisation en matière de risques.

Désignation	Tâche
ID.AM-1	Élaborez un processus d'inventaire qui garantit l'existence à tout moment d'un inventaire complet de vos ressources TIC (actifs).
ID.AM-2	Dressez l'inventaire de toutes les plateformes/licences logicielles et applications au sein de votre organisation.
ID.AM-3	Cataloguez tous vos flux internes de communication et de données.
ID.AM-4	Cataloguez tous les systèmes TIC externes pertinents pour votre organisation.
ID.AM-5	Classez par ordre de priorité les ressources inventoriées (appareils, applications, données) en fonction de leur criticité.
ID.AM-6	Définissez clairement les rôles et les responsabilités dans le domaine de la cybersécurité.

Tableau 14 Tâches ID.AM

Environnement des affaires (Business Environment)

(2) Les objectifs, les tâches et les activités de l'entreprise sont classés par ordre de priorité et évalués. Ces informations servent de base à l'attribution des responsabilités en matière de cybersécurité et de gestion des risques.

Désignation	Tâche
ID.BE-1	Identifiez, documentez et communiquez le rôle exact de votre entreprise dans la chaîne d'approvisionnement (critique).
ID.BE-2	L'importance de l'organisation en tant qu'infrastructure critique et sa position au sein du secteur critique sont identifiées et communiquées.
ID.BE-3	Les objectifs, les tâches et les activités au sein de l'organisation sont classés par ordre de priorité et évalués.
ID.BE-4	Cataloguez tous les systèmes TIC externes pertinents pour votre organisation.
ID.BE-5	Classez par ordre de priorité les ressources inventoriées (appareils, applications, données) en fonction de leur criticité.

Tableau 15 Tâches ID.BE

Gouvernance (Governance)

(3) La gouvernance constitue le cadre réglementaire pour la gestion et la surveillance de la cybersécurité. Elle se compose de directives, de procédures et de processus. Elle règle les responsabilités, surveille et garantit que les exigences régulatoires et légales de l'environnement des affaires ainsi que les exigences opérationnelles sont bien comprises et informe la direction en conséquence.

Désignation	Tâche
ID.GV-1	Édictez des directives relatives à la sécurité de l'information dans votre entreprise.
ID.GV-2	Les rôles et les responsabilités dans le domaine de la sécurité de l'information sont coordonnés avec les rôles internes (p. ex. de la gestion des risques) et avec les partenaires externes.
ID.GV-3	Veillez à ce que votre organisation remplisse toutes les exigences légales et régulatoires dans le domaine de la cybersécurité, y compris celles en matière de protection des données.
ID.GV-4	Assurez-vous que les cyberrisques font partie intégrante de la gestion des risques à l'échelle de l'entreprise.

Tableau 16 Tâches ID.GV

Gestion des risques (Risk Assessment)

(4) L'organisation connaît l'impact des risques de cybersécurité sur l'activité commerciale, sur les moyens d'exploitation et sur les individus, y compris les risques de réputation.

Désignation	Tâche
ID.RA-1	Identifiez et documentez les vulnérabilités (techniques) de vos moyens d'exploitation.
ID.RA-2	Participez régulièrement à des forums et à des comités pour vous tenir au courant des cybermenaces.
ID.RA-3	Identifiez et documentez les cybermenaces internes et externes.
ID.RA-4	Déterminez les effets potentiels sur l'activité commerciale et évaluez leur probabilité d'occurrence.
ID.RA-5	Évaluez les risques pour votre organisation en fonction des menaces, des vulnérabilités, des effets (sur l'activité commerciale) et de leur probabilité d'occurrence.
ID.RA-6	Définissez et classez par ordre de priorité les mesures d'urgence possibles lors de la survenance d'un risque.

Tableau 17 Tâches ID.RA

Stratégie de gestion des risques (Risk Management Strategy)

(5) Définissez les priorités, les contraintes et les risques maximaux supportables pour votre organisation. Basez-vous sur ces définitions pour évaluer les risques opérationnels.

Désignation	Tâche
ID.RM-1	Les processus de gestion des risques sont définis et établis, approuvés et acceptés par les parties prenantes impliquées et gérés activement.
ID.RM-2	Définissez et communiquez le risque maximal supportable pour votre organisation.
ID.RM-3	Assurez-vous que la définition du risque maximal supportable a été élaborée en tenant compte de l'importance comme infrastructure critique et des analyses de risques propres au secteur.

Tableau 18 Tâches ID.RM

Gestion des risques de la chaîne d'approvisionnement (Supply Chain Risk Management)

(6) Définissez les priorités, les contraintes et les risques maximaux que votre organisation est disposée à supporter en relation avec les risques fournisseurs. Basez-vous sur la définition des risques fournisseurs pour évaluer les risques opérationnels.

Désignation	Tâche
ID.SC-1	Mettez en place des processus clairs afin de gérer les risques de la chaîne d'approvisionnement. Soumettez ces processus à toutes les parties prenantes impliquées pour examen et obtenez leur consentement.
ID.SC-2	Identifiez et classez par ordre de priorité les fournisseurs et les prestataires de vos systèmes, composants et services critiques à l'aide des processus définis dans le cadre d'ID.SC-1.
ID.SC-3	Obligez contractuellement vos fournisseurs et vos prestataires à développer et à mettre en œuvre des mesures appropriées pour atteindre les objectifs et remplir les exigences découlant du processus de gestion des risques de la chaîne d'approvisionnement.
ID.SC-4	Établissez un suivi pour garantir que tous vos fournisseurs et prestataires satisfont à leurs obligations conformément aux exigences. Faites-le vous confirmer régulièrement par des rapports d'audit ou les résultats de tests techniques.
ID.SC-5	Définissez avec vos fournisseurs et vos prestataires les processus de réaction et de rétablissement après des incidents de cybersécurité. Testez ces processus dans le cadre d'exercices.

Tableau 19 Tâches ID.SC

4.2 Stratégie de sécurité – Protect

Gestion et contrôle des accès (Access Control)

(1) Veillez à ce que l'accès physique et logique aux ressources et installations TIC ne soit réservé qu'aux personnes, processus et appareils autorisés et qu'il soit limité aux activités définies comme étant permises.

Désignation	Tâche
PR.AC-1	Mettez en place un processus clair d'octroi et de gestion des autorisations et des données d'accès pour les utilisateurs, les appareils et les processus.
PR.AC-2	Assurez-vous que seules les personnes autorisées disposent d'un accès physique aux ressources TIC. Veillez par des mesures (architecturales) à ce que ces ressources soient protégées contre tout accès physique non autorisé.
PR.AC-3	Mettez sur pied des processus de gestion des accès à distance.
PR.AC-4	Définissez vos niveaux d'autorisation selon le principe de l'autorisation minimale et de la séparation des fonctions.
PR.AC-5	Assurez-vous que l'intégrité de votre réseau est protégée. Séparez votre réseau logiquement et physiquement lorsque cela s'avère nécessaire et judicieux.
PR.AC-6	Veillez à ce que les identités soient vérifiées et confirmées et à ce que seuls les niveaux d'autorisation et les données d'accès confirmés soient attribués.

Tableau 20 Tâches PR.AC

Sensibilisation et formation (Awareness and Training)

(2) Assurez-vous que vos collaborateurs et vos partenaires externes reçoivent régulièrement une formation adéquate sur tous les aspects de la cybersécurité. Veillez à ce qu'ils exécutent leurs tâches liées à la sécurité conformément aux exigences et aux processus correspondants.

Désignation	Tâche
PR.AT-1	Assurez-vous que tous les collaborateurs sont informés et formés en matière de cybersécurité.
PR.AT-2	Veillez à ce que les utilisateurs bénéficiant de niveaux d'autorisation plus élevés soient particulièrement conscients de leur rôle et de leur responsabilité.
PR.AT-3	Assurez-vous que tous les acteurs impliqués extérieurs à votre entreprise (fournisseurs, clients et partenaires) ont conscience de leur rôle et de leur responsabilité.
PR.AT-4	Veillez à ce que tous les dirigeants soient conscients de leur rôle et de leur responsabilité spécifiques.
PR.AT-5	Assurez-vous que les responsables de la sécurité physique et de la sécurité de l'information ont conscience de leur rôle et de leur responsabilité spécifiques.

Tableau 21 Tâches PR.AT

Sécurité des données (Data Security)

(3) Veillez à ce que les informations, les données et leurs supports soient gérés de manière à ce que la confidentialité, l'intégrité et la disponibilité des données puissent être protégées conformément à la stratégie de l'organisation en matière de risques.

Désignation	Tâche
PR.DS-1	Assurez-vous que les données stockées sont protégées (contre les atteintes à la confidentialité, à l'intégrité et à la disponibilité).
PR.DS-2	Veillez à ce que les données soient protégées pendant leur transfert.
PR.DS-3	Assurez-vous qu'un processus formel est en place pour vos ressources informatiques, qui protège les données lorsque ces ressources sont supprimées, déplacées ou remplacées.
PR.DS-4	Veillez à disposer de réserves de capacité suffisantes en ce qui concerne la disponibilité des données.
PR.DS-5	Assurez-vous que des mesures adéquates sont mises en œuvre pour prévenir les fuites de données.
PR.DS-6	Mettez en place un processus pour vérifier l'intégrité du microprogramme, des systèmes d'exploitation, des logiciels d'application et des données.
PR.DS-7	Fournissez un environnement informatique totalement indépendant des systèmes de production pour le développement et les tests.
PR.DS-8	Mettez sur pied un processus pour vérifier l'intégrité du matériel utilisé.

Tableau 22 Tâches PR.DS

Protection des données (Information Protection Processes and Procedures)

(4) Élaborez des directives relatives à la protection des systèmes d'information et des moyens d'exploitation. Veillez à ce qu'elles définissent au minimum l'objectif, la portée, les rôles et les responsabilités, ainsi que la coordination au sein de l'organisation. Utilisez ces directives pour protéger les systèmes d'information et les moyens d'exploitation.

Désignation	Tâche
PR.IP-1	Créez une configuration standard pour l'infrastructure d'information et de communication, ainsi que pour les systèmes de contrôle industriels. Assurez-vous que cette configuration intègre des principes de sécurité caractéristiques (p. ex. redondance N-1, configuration minimale, etc.).
PR.IP-2	Mettez en place un processus de cycle de vie pour le développement des systèmes.
PR.IP-3	Mettez sur pied un processus afin de contrôler les changements de configuration.
PR.IP-4	Veillez à ce que des sauvegardes de vos informations soient régulièrement effectuées, gérées et testées (vérifiez que ces sauvegardes peuvent être restaurées).

Désignation	Tâche
PR.IP-5	Assurez-vous de satisfaire à toutes les exigences et directives (régulatoires) concernant les moyens d'exploitation matériels.
PR.IP-6	Veillez à ce que les données soient détruites conformément aux exigences.
PR.IP-7	Assurez-vous que vos processus de protection de l'information sont continuellement développés et améliorés.
PR.IP-8	Échangez avec vos partenaires au sujet de l'efficacité des différentes technologies de protection.
PR.IP-9	Mettez en place des processus pour réagir aux cyberincidents survenus (planification des réponses aux incidents, gestion de la continuité des activités, reprise après incident, reprise après sinistre).
PR.IP-10	Testez les plans d'intervention et de rétablissement.
PR.IP-11	Prenez en compte les aspects de la cybersécurité dès le processus de recrutement du personnel (p. ex. en procédant à des vérifications des antécédents et à des contrôles de sécurité relatifs aux personnes).
PR.IP-12	Élaborez et mettez en œuvre un processus pour remédier aux vulnérabilités identifiées.

Tableau 23 Tâches PR.IP

Maintenance

(5) Veillez à ce que les travaux d'entretien et de réparation sur les composants du système informatique et/ou de l'ICS soient effectués conformément aux directives et aux processus applicables.

Désignation	Tâche
PR.MA-1	Assurez-vous que le fonctionnement, l'entretien et les réparations éventuelles des moyens d'exploitation sont enregistrés et documentés (journalisation). Veillez à ce que ces opérations soient exécutées rapidement et uniquement à l'aide d'instruments vérifiés et approuvés.
PR.MA-2	Assurez-vous que les travaux d'entretien de vos systèmes d'accès à distance sont enregistrés et documentés. Veillez à ce que tout accès non autorisé soit impossible.

Tableau 24 Tâches PR.MA

Technologie de protection (Protective Technology)

(6) Installez des solutions techniques de sécurité pour garantir la sécurité et la résilience de votre système et de vos données conformément aux exigences et aux processus.

Désignation	Tâche
PR.PT-1	Définissez des exigences en matière d'audits et d'enregistrements de journal. Créez et vérifiez les journaux réguliers conformément aux exigences et aux directives.
PR.PT-2	Veillez à ce que les supports amovibles soient protégés et à ce qu'ils soient uniquement utilisés selon les directives.
PR.PT-3	Assurez-vous que votre système est configuré de manière à garantir une fonctionnalité minimale en tout temps.
PR.PT-4	Veillez à ce que vos réseaux de communication et de commande soient protégés.
PR.PT-5	Assurez-vous que vos systèmes fonctionnent selon des scénarios prédéfinis. P. ex.: fonctionnalité durant une attaque, fonctionnalité en phase de récupération, fonctionnalité en phase d'exploitation normale.

Tableau 25 Tâches PR.PT

4.3 Stratégie de sécurité – Detect

Incidents (Anomalies and Events)

(1) Veillez à ce que les anomalies et les événements liés à la sécurité soient détectés à temps et que les effets potentiels de l'incident soient compris.

Désignation	Tâche
DE.AE-1	Définissez les valeurs par défaut pour les opérations réseau autorisées et les flux de données attendus pour les utilisateurs et les systèmes. Gérez ces valeurs en continu.
DE.AE-2	Assurez-vous que les incidents de cybersécurité détectés sont analysés quant à leurs objectifs et à leurs méthodes.
DE.AE-3	Veillez à ce que les informations relatives aux incidents de cybersécurité soient agrégées et traitées à partir de sources et de capteurs multiples.
DE.AE-4	Déterminez les effets des éventuels événements.
DE.AE-5	Définissez les valeurs seuils au-delà desquelles les incidents de cybersécurité déclenchent une alerte.

Tableau 26 Tâches DE.AE

Surveillance (Security Continuous Monitoring)

(2) Veillez à ce que le système TIC, y compris l'ensemble des ressources, fasse l'objet d'une surveillance à intervalles réguliers afin, d'une part, de détecter les incidents de cybersécurité et, d'autre part, de garantir l'efficacité des contre-mesures.

Désignation	Tâche
DE.CM-1	Établissez une surveillance continue du réseau pour repérer les éventuels incidents de cybersécurité.
DE.CM-2	Mettez en place une surveillance continue de tous les moyens d'exploitation matériels et bâtiments afin de détecter les incidents de cybersécurité.
DE.CM-3	Établissez une surveillance des cyberactivités des collaborateurs pour déceler les éventuels incidents de cybersécurité.
DE.CM-4	Assurez-vous que les logiciels malveillants peuvent être détectés.
DE.CM-5	Veillez à ce que les programmes exécutables puissent être identifiés dans les pièces jointes aux courriels, les macros, les périphériques de stockage USB ou les appareils mobiles.
DE.CM-6	Assurez-vous que les activités des prestataires externes sont surveillées, de sorte que les incidents de cybersécurité puissent être détectés.
DE.CM-7	Surveillez votre système en permanence pour garantir que les activités/accès de personnes, d'appareils et de logiciels non autorisés peuvent être repérés.
DE.CM-8	Effectuez régulièrement des analyses de vulnérabilité.

Tableau 27 Tâches DE.CM

Processus de détection (Detection Processes)

(3) Les processus et instructions relatifs à la détection des événements de cybersécurité sont actualisés, testés et maintenus de façon à ce que les incidents puissent être identifiés rapidement.

Désignation	Tâche
DE.DP-1	Définissez clairement les rôles et les responsabilités, de sorte que l'on sache précisément qui est responsable de quoi et quelles sont ses compétences.
DE.DP-2	Assurez-vous que les processus de détection remplissent toutes vos exigences et conditions.
DE.DP-3	Testez vos processus de détection.
DE.DP-4	Communiquez les événements détectés aux instances compétentes (fournisseurs, clients, partenaires, autorités, etc.)
DE.DP-5	Améliorez continuellement vos processus de détection.

Tableau 28 Tâches DE.DP

4.4 Stratégie de sécurité – Respond

Planification des réponses (Response Planning)

(1) Élaborer un plan d'intervention pour faire face aux incidents de cybersécurité identifiés. Assurez-vous que ce plan est exécuté correctement et à temps en cas d'incident.

Désignation	Tâche
RS.RP-1	Veillez à ce que le plan d'intervention soit exécuté correctement et rapidement pendant ou après un incident de cybersécurité détecté.

Tableau 29 Tâches RS.RP

Communication (Communications)

(2) Veillez à ce que vos processus d'intervention soient coordonnés avec les parties prenantes internes et externes. En cas d'incident, assurez-vous de recevoir l'aide des pouvoirs publics, si cela s'avère nécessaire et opportun.

Désignation	Tâche
RS.CO-1	Veillez à ce que toutes les personnes connaissent leurs tâches et l'ordre de leurs actions en réponse aux incidents de cybersécurité survenus.
RS.CO-2	Définissez des critères de reporting et assurez-vous que les incidents de cybersécurité sont signalés et traités selon ces critères.
RS.CO-3	Partagez les informations et les conclusions sur les incidents de cybersécurité détectés en fonction des critères définis.
RS.CO-4	Coordonnez-vous avec l'ensemble de vos parties prenantes selon les critères prédéfinis.
RS.CO-5	Améliorez la sensibilisation aux incidents de cybersécurité en échangeant régulièrement avec vos partenaires.

Tableau 30 Tâches RS.CO

Analyse (Analysis)

(3) Veillez à ce que des analyses régulières soient effectuées, qui vous permettent de réagir de manière adéquate aux incidents de cybersécurité.

Désignation	Tâche
RS.AN-1	Assurez-vous que les notifications des systèmes de détection sont prises en compte et donnent lieu à des enquêtes.
RS.AN-2	Veillez à ce que les effets d'un incident de cybersécurité puissent être correctement identifiés.
RS.AN-3	Effectuez des analyses d'investigation après la survenance d'un incident.
RS.AN-4	Classez les incidents survenus en fonction des exigences définies dans le plan d'intervention.

Tableau 31 Tâches RS.AN

Atténuation (Mitigation)

(4) Effectuez des actions qui empêchent la propagation d'un incident de cybersécurité, en atténuent les effets et en éliminent la cause.

Désignation	Tâche
RS.MI-1	Assurez-vous que les incidents de cybersécurité peuvent être circonscrits et que leur propagation est interrompue.
RS.MI-2	Veillez à ce que les effets des incidents de cybersécurité puissent être atténués.
RS.MI-3	Assurez-vous que les vulnérabilités nouvellement identifiées sont réduites ou documentées comme des risques acceptés.

Tableau 32 Tâches RS.MI

Améliorations (Improvements)

(5) Veillez à ce que la capacité de votre organisation à réagir aux incidents de cybersécurité soit continuellement améliorée en tirant les leçons des incidents antérieurs.

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

Tableau 33 Tâches RS.IM

4.5 Stratégie de sécurité – Recover

Planification du rétablissement (Recovery Planning)

(1) Veillez à ce que les processus de rétablissement soient actualisés et exécutés de manière à ce qu'une restauration rapide des systèmes puisse être garantie.

Désignation	Tâche
RC.RP-1	Assurez-vous que le plan de rétablissement est exécuté correctement après la survenance d'un incident de cybersécurité.

Tableau 34 Tâches RC.RP

Améliorations (Improvements)

(2) Veillez à ce que vos processus de rétablissement soient continuellement améliorés en tirant les leçons des restaurations précédentes.

Désignation	Tâche
RC.IM-1	Assurez-vous que les conclusions et les enseignements tirés des précédents incidents de cybersécurité sont intégrés à vos plans de rétablissement.
RC.IM-2	Mettez à jour votre stratégie de rétablissement.

Tableau 35 Tâches RC.IM

Communication (Communications)

(3) Coordonnez vos activités de rétablissement avec des partenaires internes et externes tels que les fournisseurs d'accès Internet, les équipes d'intervention en cas d'urgence informatique (CERT), les autorités, les intégrateurs de systèmes, etc.

Désignation	Tâche
RC.CO-1	Veillez à ce que votre image publique soit gérée activement.
RC.CO-2	Assurez-vous que votre réputation est rétablie après la survenance d'un incident de cybersécurité.
RC.CO-3	Communiquez toutes vos activités de rétablissement aux parties prenantes internes, notamment à la direction.

Tableau 36 Tâches RC.CO

4.6 21 mesures pour accroître la cybersécurité des réseaux OT

(1) Basées sur les explications du Département américain de l'Énergie (Department of Energy), ces 21 étapes ont pour objectif de protéger les infrastructures critiques d'approvisionnement en électricité.

(2) **Les étapes suivantes mettent l'accent sur les mesures spécifiques à prendre pour améliorer la sécurité des réseaux OT dédiés aux infrastructures critiques d'approvisionnement en électricité:**

Mesures spécifiques pour accroître la sécurité des réseaux OT	Cadre du NIST
1. Identifiez toutes les connexions aux réseaux OT dédiés aux infrastructures critiques d'approvisionnement en électricité Effectuez une analyse approfondie afin d'évaluer le risque et la nécessité de chaque connexion aux réseaux OT dédiés aux infrastructures critiques d'approvisionnement en électricité. Développez une compréhension globale de toutes ces connexions et de la façon dont elles sont protégées. Identifiez et évaluez les types de connexions suivants: - Réseaux internes locaux et étendus, y compris les réseaux d'entreprise - Internet - Dispositifs de réseau sans fil, y compris les liaisons montantes par satellite - Connexions modem ou commutée - Connexions avec des partenaires commerciaux, des fournisseurs ou des autorités de régulation	ID.AM ID.GV ID.RA ID.RM PR.AC PR.DS PR.MA PR.PT
2. Supprimez les connexions inutiles aux réseaux OT dédiés aux infrastructures critiques d'approvisionnement en électricité Pour garantir une sécurité maximale des systèmes au sein des réseaux OT dédiés aux infrastructures critiques d'approvisionnement en électricité, isolez autant que possible les réseaux OT des autres réseaux. Toute connexion à un autre réseau entraîne des risques de sécurité, surtout si elle crée un chemin d'accès à ou depuis Internet. Bien que les connexions directes à d'autres réseaux puissent permettre de transmettre des informations importantes de manière efficace et pratique, les connexions non sécurisées ne valent tout simplement pas le risque encouru. L'isolement des réseaux OT dédiés aux infrastructures critiques d'approvisionnement en électricité doit être un objectif prioritaire afin d'assurer la protection requise. Des stratégies telles que l'utilisation de «zones démilitarisées» (DMZ), les diodes réseau et l'entreposage de données peuvent faciliter le transfert sécurisé des données au sein des réseaux OT dédiés aux infrastructures critiques d'approvisionnement en électricité et vers les réseaux d'entreprise. Elles doivent toutefois être correctement conçues et mises en œuvre pour éviter l'introduction de risques supplémentaires dus à une configuration inappropriée	ID.BE PR.DS PR.IP PR.MA PR.PT

Mesures spécifiques pour accroître la sécurité des réseaux OT	Cadre du NIST
3. Évaluez et renforcez la sécurité de toutes les connexions restantes au sein des réseaux OT dédiés aux infrastructures critiques d'approvisionnement en électricité et vers les autres réseaux. Effectuez des tests de pénétration ou des analyses de vulnérabilité sur toutes les connexions restantes au sein des réseaux OT dédiés aux infrastructures critiques d'approvisionnement en électricité et vers les autres réseaux afin d'évaluer les mesures de protection associées à ces voies. Exploitez ces informations en relation avec les processus de gestion des risques afin de développer une stratégie de protection robuste pour toutes les connexions possibles au sein des réseaux OT dédiés aux infrastructures critiques d'approvisionnement en électricité et vers les autres réseaux. Étant donné que les réseaux OT dédiés aux infrastructures critiques d'approvisionnement en électricité sont aussi sûrs que le point de connexion le plus faible, il est nécessaire de mettre en œuvre des pare-feux, des systèmes de détection d'intrusion (IDS) et d'autres mesures de sécurité appropriées à chaque point d'entrée. Configurez les règles de pare-feu pour empêcher l'accès aux et depuis les réseaux OT dédiés aux infrastructures critiques d'approvisionnement en électricité et assurez-vous que seules les connexions absolument indispensables sont autorisées. Ainsi, un gestionnaire de réseau indépendant (ISO) ne devrait pas se voir accorder un accès au réseau «global» simplement parce qu'il est nécessaire de se connecter à certains composants du système SCADA. Il est impératif de placer stratégiquement des IDS à chaque point d'entrée pour informer le personnel ad hoc des violations potentielles de la sécurité des réseaux. La direction doit comprendre et assumer la responsabilité des risques liés à la connexion au sein des réseaux OT dédiés aux infrastructures critiques d'approvisionnement en électricité et vers les autres réseaux.	ID.AM PR.AT PR.DS PR.IP PR.MA PR.PT
4. Renforcez les réseaux OT dédiés aux infrastructures critiques d'approvisionnement en électricité en supprimant ou en désactivant les services inutiles. Les serveurs de commande SCADA basés sur des systèmes d'exploitation commerciaux ou open source peuvent être attaqués par le biais de services réseau standard. Dans la mesure du possible, supprimez ou désactivez les services non utilisés et les démons réseau pour réduire le risque d'attaque directe. Cela est particulièrement important lorsque les réseaux OT dédiés aux infrastructures critiques d'approvisionnement en électricité sont reliés à d'autres réseaux. N'autorisez pas sur le réseau SCADA des services et des fonctions qui ne peuvent pas être directement conciliés avec la tâche principale du SCADA. Réfléchissez attentivement afin d'identifier les services qui apportent une réelle valeur ajoutée et ne se bornent pas à affaiblir inutilement l'ensemble du système. Parmi les services qu'il faudrait enlever des réseaux OT dédiés aux infrastructures critiques d'approvisionnement en électricité, on peut citer par exemple les systèmes de relevé des compteurs et de facturation à distance, les services de messagerie électronique et l'accès Internet. Autre fonction qui devrait être désactivée: la télémaintenance. De nombreux guides de configuration sécurisée pour les systèmes d'exploitation commerciaux et open source sont accessibles au public, comme la série de guides de sécurité publiée par la National Security Agency (NSA). Collaborez étroitement avec les fournisseurs SCADA pour définir des configurations sécurisées et coordonner tous les changements apportés aux systèmes d'exploitation. Vous garantissez ainsi que la suppression ou la désactivation des services ne provoquera aucune défaillance, interruption ni perte de support.	PR.DS PR.IP PR.MA PR.PT

Mesures spécifiques pour accroître la sécurité des réseaux OT	Cadre du NIST
5. Ne vous fiez pas à des protocoles propriétaires pour protéger votre système. Certains systèmes OT dédiés aux infrastructures critiques d'approvisionnement en électricité utilisent des protocoles uniques et propriétaires pour la communication entre les appareils de terrain et les serveurs. Souvent, la sécurité de ces systèmes OT repose exclusivement sur la confidentialité de ces protocoles. Des protocoles obscurs n'offrent malheureusement pas de «réelle» sécurité. Ne vous fiez pas à des protocoles propriétaires ou aux paramètres d'usine par défaut pour protéger votre système. En outre, exigez que les fournisseurs de systèmes SCADA et de composants de contrôle-commande divulguent toutes les interfaces de portes dérobées ou de fabricants avec vos systèmes OT dédiés aux infrastructures critiques d'approvisionnement en électricité. Enjoignez-les à fournir des systèmes pouvant être sécurisés et surveillés.	PR.AT PR.DS PR.IP PR.MA PR.PT
6. Mettez en œuvre les caractéristiques de sécurité des fournisseurs d'appareils et de systèmes. La plupart des anciens systèmes OT dédiés aux infrastructures critiques d'approvisionnement en électricité (c'est-à-dire la majorité des systèmes utilisés) ne disposent pas de fonctions sécurité. Les exploitants de ces systèmes OT doivent insister auprès de leur fabricant pour qu'il mette en place des fonctionnalités de sécurité sous forme de correctifs ou de mises à niveau de produits. Certains systèmes OT plus récents dédiés aux infrastructures critiques d'approvisionnement en électricité sont livrés avec des fonctions de sécurité de base, mais celles-ci sont généralement désactivées pour faciliter l'installation. Analysez chaque appareil des systèmes OT dédiés aux infrastructures critiques d'approvisionnement en électricité pour déterminer si des dispositifs de sécurité sont présents et activés. En outre, les paramètres d'usine par défaut (p. ex. dans les pare-feux des réseaux informatiques) sont souvent réglés de manière à offrir une convivialité maximale, mais une sécurité minimale. Utilisez toutes les fonctions de sécurité pour garantir le niveau maximum de protection. N'autorisez des paramètres inférieurs à la sécurité maximale qu'après une évaluation approfondie des risques induits par la réduction du niveau de sécurité.	ID.RA ID.RM PR.AC PR.AT PR.DS PR.IP PR.MA PR.PT
7. Contrôlez rigoureusement tout support utilisé pour les connexions de portes dérobées ou de fabricants aux réseaux OT dédiés aux infrastructures critiques d'approvisionnement en électricité. Lorsqu'il existe des connexions de portes dérobées ou de fabricants aux systèmes OT dédiés aux infrastructures critiques d'approvisionnement en électricité, il faut mettre en place une authentification forte pour garantir une communication sécurisée. Les modems ainsi que les réseaux sans fil et câblés utilisés pour la communication et la maintenance représentent une vulnérabilité importante des réseaux OT dédiés aux infrastructures critiques d'approvisionnement en électricité et aux sites distants. En cas de scannage de numéros de téléphone (war dialing) ou de trébuchage sans fil (war driving) réussi, un attaquant pourrait contourner toutes les autres mesures de contrôle et de protection et accéder ainsi directement aux ressources ou aux réseaux OT dédiés aux infrastructures critiques d'approvisionnement en électricité. Pour réduire au maximum le risque de telles attaques, désactivez l'accès entrant et remplacez-le par une fonction de rappel.	PR.AC PR.AT PR.DS PR.MA PR.PT

Mesures spécifiques pour accroître la sécurité des réseaux OT	Cadre du NIST
8. Mettez en œuvre des systèmes internes et externes de détection des intrusions et assurez une surveillance 24 heures sur 24. Pour pouvoir réagir efficacement aux cyberattaques, mettez en place une stratégie de détection des intrusions qui englobe la notification aux administrateurs réseau des activités réseau malveillantes provenant de sources internes ou externes. La surveillance du système de détection des intrusions est importante 24 heures sur 24. Cette fonction peut être configurée au moyen d'une alarme par radiomessageur (pager). De plus, des procédures de réponse aux incidents doivent être en place pour pouvoir réagir efficacement à toute attaque. En complément de la surveillance du réseau, activez l'enregistrement quotidien de tous les systèmes et journaux du système d'audit afin de détecter les activités suspectes le plus rapidement possible.	PR.DS PR.IP PR.MA PR.PT DE.CM RS.RP RS.CO RS.AN
9. Effectuez des audits techniques sur les appareils et les réseaux de l'environnement OT dédié aux infrastructures critiques d'approvisionnement en électricité ainsi que sur tous les autres réseaux connectés afin d'identifier les problèmes de sécurité. Les audits techniques des appareils et des réseaux de l'environnement OT dédié aux infrastructures critiques d'approvisionnement en électricité revêtent une importance cruciale pour l'efficacité continue de la sécurité. Il existe de nombreux outils de sécurité commerciaux et open source, qui permettent aux administrateurs système de réaliser des audits de leurs systèmes/réseaux afin d'identifier les services actifs, le niveau des correctifs et les vulnérabilités communes. L'utilisation de ces outils ne résoudra pas les problèmes systémiques, mais éliminera les «voies de moindre résistance» qu'un attaquant pourrait exploiter. Analysez les vulnérabilités détectées pour déterminer leur importance et prendre des mesures correctives. Opérez un suivi de ces mesures et analysez les informations recueillies afin de dégager les tendances. Il faut en outre réitérer les tests après la mise en œuvre des mesures correctives pour s'assurer que les vulnérabilités ont bien été éliminées. Il convient également d'analyser les environnements non productifs afin d'identifier et de résoudre les problèmes potentiels.	PR.AC PR.DS PR.IP PR.MA PR.PT
10. Procédez à des inventaires et à l'évaluation de la sécurité physique de tous les sites connectés aux réseaux OT dédiés aux infrastructures critiques d'approvisionnement en électricité. Tout emplacement abritant un élément des réseaux OT dédiés aux infrastructures critiques d'approvisionnement en électricité est une cible potentielle d'attaques. Les sites éloignés sans personnel ou sans surveillance, en particulier, présentent un risque majeur. Effectuez une analyse de la sécurité physique, notamment aux points d'entrée possibles, dans toute installation contenant un élément des réseaux OT dédiés aux infrastructures critiques d'approvisionnement en électricité. Identifiez et évaluer tous les points d'entrée potentiels, y compris la téléphonie à distance, le réseau informatique et les câbles à fibres optiques qui pourraient être mis sur écoute, les liaisons sans fil et radio qui sont exploitables, les terminaux d'ordinateur auxquels on pourrait avoir accès et les points d'accès au réseau local sans fil. Repérez et éliminez les points uniques de défaillance. La sécurité des sites doit être suffisante pour détecter ou empêcher tout accès non autorisé. N'autorisez pas l'accès sans fil aux réseaux OT dédiés aux infrastructures critiques d'approvisionnement en électricité dans les installations éloignées et sans surveillance simplement pour des raisons de commodité.	ID.AM ID.GV ID.RA PR.AC PR.AT PR.DS PR.IP PR.PT

Mesures spécifiques pour accroître la sécurité des réseaux OT	Cadre du NIST
11. Mettez en place des «red teams» relatives à l'environnement OT dédié aux infrastructures critiques d'approvisionnement en électricité afin d'identifier et d'évaluer les scénarios d'attaques possibles. Mettez sur pied une «red team» pour identifier les scénarios d'attaques possibles et évaluer les vulnérabilités potentielles du système. Faites appel à une variété de personnes pouvant fournir un aperçu des faiblesses de l'ensemble de l'environnement OT dédié aux infrastructures critiques d'approvisionnement en électricité, des systèmes physiques et des contrôles de sécurité. Les personnes qui travaillent quotidiennement sur le système ont une bonne idée des vulnérabilités de leur environnement OT dédié aux infrastructures critiques d'approvisionnement en électricité, et devraient par conséquent être consultées et impliquées dans la détermination des scénarios d'attaques possibles et de leurs conséquences potentielles. Veillez par ailleurs à ce que le risque d'un initié malveillant soit pleinement évalué, car il s'agit là de l'une des principales menaces auxquelles doit faire face une entreprise. Intégrer les connaissances de la «red team» aux processus de gestion des risques afin d'analyser les informations et d'élaborer des stratégies de protection appropriées.	ID.RA DE.CM PR.AC PR.AT PR.DS PR.IP PR.PT

Tableau 37 Mesures spécifiques pour accroître la sécurité des réseaux OT

(3) **Les étapes suivantes sont axées sur les mesures de gestion visant à établir un programme efficace de cybersécurité:**

Mesures spécifiques pour accroître la sécurité des réseaux OT	Cadre du NIST
12. Définissez clairement les rôles, les compétences et les responsabilités en matière de cybersécurité pour la direction, les administrateurs système et les utilisateurs. Les collaborateurs d'une entreprise doivent comprendre les attentes et les obligations spécifiques liées à la protection des ressources informatiques. Pour ce faire, il faut définir des rôles et des responsabilités clairs et logiques. Les personnes clés doivent en outre disposer de droits suffisants pour accomplir leurs tâches. Trop souvent, une bonne cybersécurité est laissée à l'initiative des individus, ce qui conduit généralement à une mise en œuvre incohérente et à une sécurité inefficace. Créez une structure organisationnelle de cybersécurité qui définit les rôles et les responsabilités et qui précise la manière de faire remonter les problèmes, ainsi que les personnes à prévenir en cas d'urgence.	ID.AM ID.GV DE.DP PR.AC PR.AT PR.DS

Mesures spécifiques pour accroître la sécurité des réseaux OT	Cadre du NIST
13. Documentez l'architecture de réseau et identifiez les systèmes qui exécutent des fonctions critiques ou contiennent des informations sensibles nécessitant des niveaux de protection supplémentaires. Élaborez et documentez une solide architecture de sécurité de l'information dans le cadre d'un processus visant à établir une stratégie de protection efficace. Il est essentiel que les entreprises surveillent en permanence et vérifient périodiquement la sécurité de leur réseau afin de garantir une compréhension à jour de l'architecture de réseau tout au long de son cycle de vie Il est particulièrement important de bien appréhender les fonctions que les systèmes exécutent ainsi que la sensibilité nécessaire aux informations stockées. Sans cette compréhension, le risque ne peut pas être correctement évalué et les stratégies de protection peuvent s'avérer insuffisantes. La documentation de l'architecture de sécurité de l'information et de ses composantes est essentielle à la compréhension de la stratégie globale de protection et à l'identification des points uniques de défaillance.	ID.AM PR.DS PR.IP PR.MA PR.PT
14. Définissez un processus de gestion des risques rigoureux et continu. Une compréhension approfondie des risques que représentent les attaques par déni de service pour les ressources informatiques du réseau et la vulnérabilité des informations sensibles à la compromission est essentielle à l'efficacité d'un programme de cybersécurité. Les évaluations des risques constituent la base technique de cette compréhension et sont indispensables à la formulation de stratégies performantes visant à atténuer les vulnérabilités et à préserver l'intégrité des ressources informatiques. Effectuez tout d'abord une analyse référentielle des risques en vous fondant sur une évaluation actuelle des menaces pour élaborer une stratégie de protection du réseau. L'évolution rapide de la technologie et l'émergence de nouvelles menaces au quotidien requièrent également une procédure continue d'évaluation des risques afin que des changements systématiques puissent être apportés à la stratégie de protection, garantissant ainsi le maintien de son efficacité. La gestion des risques repose sur l'identification du risque résiduel avec une stratégie de protection du réseau et l'acceptation de ce risque par la direction d'une entreprise.	ID.RA ID.RM PR.IP
15. Mettez en place une stratégie de protection du réseau fondée sur le principe de défense. Un principe fondamental qui doit faire partie d'une stratégie de protection du réseau est axé sur la défense. Cette dernière doit être prise en compte dès le début de la phase de conception du processus de développement et faire partie intégrante de toutes les décisions techniques associées au réseau. Mettez à profit les contrôles techniques et administratifs pour atténuer les menaces liées aux risques identifiés, dans la mesure du possible à tous les niveaux du réseau. Les points uniques de défaillance doivent être évités, et la défense de la cybersécurité doit être superposée afin de limiter et de prévenir les effets des incidents de sécurité. De plus, chaque niveau doit être protégé contre d'autres systèmes de la même couche. Par exemple, il ne faut mettre à la disposition des utilisateurs que les privilèges et les ressources réellement nécessaires à l'exercice de leur fonction.	PR.AC PR.DS PR.IP PR.MA PR.PT

Mesures spécifiques pour accroître la sécurité des réseaux OT	Cadre du NIST
16. Identifiez les exigences en matière de cybersécurité. Les organisations et les entreprises ont besoin de programmes de sécurité structurés assortis d'exigences obligatoires pour justifier les attentes et demander des comptes au personnel. Des directives et procédures formalisées sont généralement utilisées pour établir et institutionnaliser un programme de cybersécurité. Un programme formel est essentiel à la définition d'une approche cohérente et fondée sur des normes en matière de cybersécurité au sein d'une entreprise et élimine la dépendance exclusive à l'égard de l'initiative individuelle. Les exigences et les processus permettent également d'informer les collaborateurs des responsabilités spécifiques qui leur incombent dans le domaine de la sécurité de l'information et des conséquences d'un manquement à ces dernières. Ils fournissent également des lignes directrices pour les mesures à prendre lors d'un incident de cybersécurité et encouragent des actions efficaces et efficientes en période de crise. Les accords avec les utilisateurs et la notification font partie de l'identification des exigences en matière de cybersécurité. Il faut définir des exigences et des règles visant à réduire au maximum la menace constituée par les initiés malveillants, y compris la nécessité de procéder à des vérifications des antécédents et de limiter les privilèges réseau à ceux qui sont absolument indispensables.	PR.AC PR.AT PR.DS PR.IP PR.MA PR.PT
17. Créez des processus efficaces de gestion des configurations. La gestion des configurations constitue un processus de gestion fondamental pour pouvoir entretenir un réseau sécurisé. Elle doit couvrir aussi bien les configurations matérielles que logicielles. Les modifications apportées au matériel ou aux logiciels peuvent facilement introduire des vulnérabilités qui sapent la sécurité du réseau. Des processus sont nécessaires pour évaluer et contrôler tout changement afin de garantir que le réseau demeure sûr. La gestion des configurations commence par des bases de sécurité éprouvées et documentées pour les différents systèmes.	PR.DS PR.IP PR.MA PR.PT
18. Effectuez des auto-évaluations de routine. De solides processus d'évaluation des performances sont nécessaires pour fournir aux entreprises un feed-back sur l'efficacité de la politique de cybersécurité et sur sa mise en œuvre technique. Une bonne organisation se caractérise par sa capacité à identifier les problèmes, à analyser les causes et à prendre des mesures correctives efficaces afin de gommer les défauts individuels et systémiques. Les processus d'auto-évaluation qui font habituellement partie d'un programme de cybersécurité performant comprennent l'analyse systématique des vulnérabilités, la vérification automatisée du réseau et l'auto-évaluation des résultats organisationnels et individuels.	PR.AC PR.AT PR.DS PR.IP PR.PT
19. Créez des sauvegardes système et des plans de reprise après sinistre. Élaborez un plan de reprise après sinistre qui vous permet de vous remettre rapidement de toute situation d'urgence (y compris d'une cyberattaque). Élément essentiel des mesures nécessaires, les sauvegardes système permettent une reconstruction rapide du réseau. Contrôlez régulièrement les plans de reprise après sinistre pour vous assurer qu'ils fonctionnent et que les surveillants de systèmes et les utilisateurs les connaissent bien. Apportez continuellement des modifications pertinentes aux plans de reprise après sinistre en fonction des enseignements tirés des exercices.	PR.DS PR.IP PR.MA PR.PT RC.RP RC.CO RC.IM

Mesures spécifiques pour accroître la sécurité des réseaux OT	Cadre du NIST
20. La direction devrait fixer des attentes quant aux performances en matière de cybersécurité et tenir les individus responsables de leurs résultats. L'efficacité des performances en matière de cybersécurité requiert l'engagement et le leadership des dirigeants des entreprises. Il est essentiel que les membres les plus haut placés de la direction fixent des attentes élevées en matière de cybersécurité et les communiquent à leurs cadres subordonnées dans toute l'organisation. Il importe également que la haute direction organisationnelle mette en place une structure pour la mise en œuvre d'un programme de cybersécurité. Cette structure permet de soutenir un solide programme dans ce domaine. Il est important que chaque collaborateur soit tenu responsable de ses actes en matière de cybersécurité. C'est notamment le cas des gestionnaires, des administrateurs système, des techniciens et des utilisateurs/exploitants.	PR.AC PR.AT PR.IP
21. Définissez des directives et dispensez des formations pour réduire au maximum la probabilité que le personnel organisationnel divulgue par inadvertance des informations confidentielles sur la conception du système de l'environnement OT dédié aux infrastructures critiques d'approvisionnement en électricité, sur les opérations ou sur les contrôles de sécurité. Les données relatives aux réseaux OT dédiés aux infrastructures critiques d'approvisionnement en électricité sont communiquées selon le principe strict du besoin d'en connaître et accessibles uniquement aux personnes expressément autorisées à recevoir de telles informations. L'ingénierie sociale, qui consiste à recueillir des informations au sujet d'un ordinateur ou d'un réseau informatique en posant des questions à des utilisateurs naïfs, est souvent la première étape d'une attaque malveillante sur les réseaux informatiques. Plus on dispose de renseignements sur un ordinateur ou un réseau informatique, plus il est vulnérable. Ne divulguez jamais de données se rapportant aux réseaux OT dédiés aux infrastructures critiques d'approvisionnement en électricité, y compris les noms et les coordonnées des exploitants de système et des administrateurs, les systèmes d'exploitation informatiques et/ou les emplacements physiques et logiques des ordinateurs et des systèmes réseau par téléphone ou au personnel, à moins qu'il ne soit explicitement autorisé à recevoir de telles informations. Toute demande de renseignements émanant d'inconnus doit être signalée à une instance compétente pour vérification. Les personnes peuvent constituer un maillon faible sur un réseau au demeurant sécurisé. La réalisation de campagnes de formation et d'information est impérative pour s'assurer que le personnel fait preuve d'une prudence suffisante dans le traitement des informations réseau sensibles, notamment de ses mots de passe.	PR.AC PR.AT PR.IP

Tableau 38 Mesures de gestion visant à établir un programme efficace de cybersécurité

5. Autres outils et aides destinés à la vérification et à l'évaluation

(1) Il existe différents outils et aides permettant de vérifier et d'évaluer sa propre architecture mise en œuvre.

5.1 Common Vulnerability Scoring System (CVSS)

(1) Common Vulnerability Scoring System (littéralement «Système commun de notation des vulnérabilités»), abrégé en CVSS, désigne une norme industrielle visant à évaluer la gravité des failles de sécurité potentielles ou réelles dans les systèmes informatiques. Dans CVSS, les vulnérabilités sont évaluées et comparées entre elles selon divers critères appelés «métriques», ce qui permet d'établir une liste de priorités pour les contre-mesures. CVSS lui-même n'est pas un dispositif d'alerte en cas de vulnérabilités, mais une norme destinée à rendre différents systèmes de description et de mesure compatibles entre eux et compréhensibles pour tous.

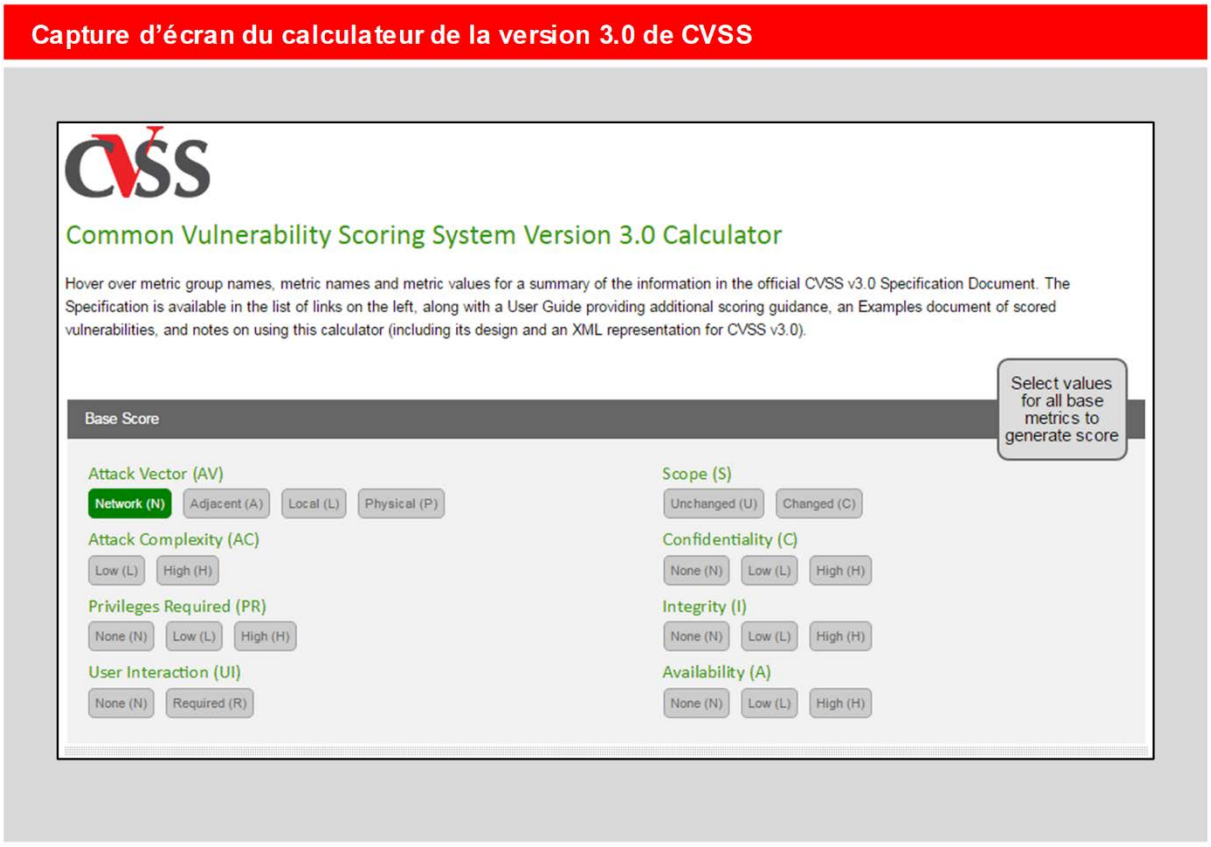

Figure 26 Capture d'écran du calculateur de la version 3.0 de CVSS

(2) CVSS a été commandé en 2005 par le National Infrastructure Advisory Council (NIAC), un groupe de travail du Département de la Sécurité intérieure des États-Unis, et est actuellement géré par le Forum of Incident Response and Security Teams. Le président actuel du groupe de travail «CVSS-SIG team» est David Ahmad, de Symantec. Les acteurs suivants sont impliqués dans le développement de CVSS: CERT, Cisco, DHS/MITRE, eBay, IBM, Microsoft, Qualys et Symantec. CVSS est en outre pris en charge par HP, McAfee, Oracle et Skype. La deuxième version du système de notation a été publiée en juin 2007. Révisions: avec CVSS v3.0, le système a été réédité en juin 2015 et inclut,

outre diverses révisions de la métrique, l'introduction de mots clés pour les niveaux de gravité (Nul/Faible/Moyen/Élevé/Critique), ainsi qu'un guide utilisateur et un document rassemblant des exemples pratiques d'évaluation.

5.2 Light and Right Security ICS (LARS ICS)

(1) Light and Right Security ICS (LARS ICS) est un outil gratuit de l'Office fédéral allemand de la sécurité des technologies de l'information (Bundesamt für Sicherheit in der Informationstechnik, BSI), qui facilite l'accès à la cybersécurité pour les petites et moyennes entreprises du domaine des systèmes de contrôle-commande industriels. Il propose une auto-évaluation – guidée par des questions – de l'état actuel de la cybersécurité et formule des recommandations sur les mesures à mettre en œuvre ultérieurement dans tel ou tel domaine.

Capture d'écran de l'interface utilisateur de LARS ICS

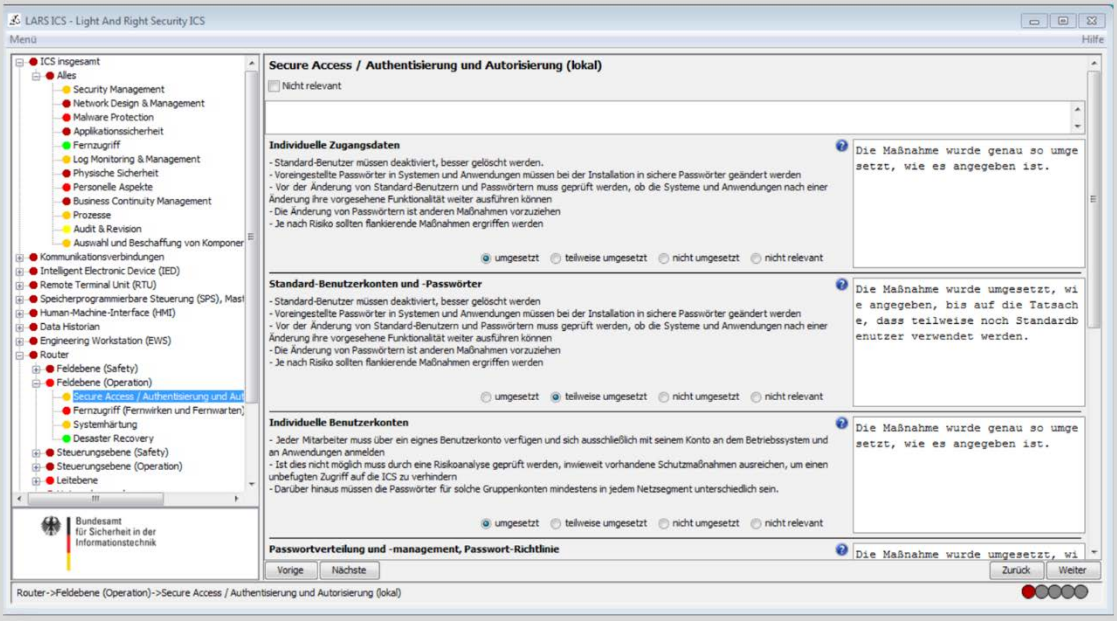

Figure 27 Capture d'écran de l'interface utilisateur de LARS ICS

(2) Toutes les mesures sont affectées aux parties correspondantes des normes et procédures IT-Grundschutz, ISO 27001, IEC 62443 et BSI ICS Security Compendium, ce qui facilite le passage à l'utilisation d'un système global de gestion en matière de sécurité de l'information.

(3) Outre le programme proprement dit, les archives renferment un manuel et le code source complet de LARS ICS.

5.3 Cyber Security Evaluation Tool CSET®

(1) Cyber Security Evaluation Tool (CSET®) offre une approche systématique, disciplinée et reproductible pour évaluer la situation sécuritaire dans une entreprise. Il s'agit d'un outil logiciel permettant aux propriétaires et aux exploitants d'installations d'évaluer, au moyen d'un processus séquentiel, les pratiques de sécurité qu'ils ont mises en œuvre au sein des réseaux de contrôle-commande industriels (ICS) et des réseaux informatiques (IT). Les utilisateurs peuvent ainsi apprécier et comparer leurs propres directives et exigences en matière de cybersécurité par rapport à de nombreuses normes et recommandations gouvernementales et industrielles reconnues. L'Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) du Département américain de la Sécurité intérieure (Department of Homeland Security, DHS) a développé l'application CSET et la propose gratuitement aux utilisateurs finaux.

(2) CSET aide les propriétaires et les exploitants d'installations à évaluer leurs informations et leurs systèmes opérationnels quant aux actions de cybersécurité mises en place en leur posant une série de questions détaillées sur les composants et les architectures des systèmes, ainsi que sur les mesures et procédures opérationnelles. Ces questions découlent des normes de cybersécurité reconnues dans l'industrie. Une fois les questionnaires remplis, CSET offre un tableau de bord assorti de diagrammes indiquant les points forts et les points faibles. Il fournit également une liste de recommandations classées par ordre de priorité pour accroître la cybersécurité dans sa propre entreprise et ses propres systèmes. CSET comprend des solutions, des pratiques communes, des mesures de compensation et des extensions de composants.

(3) La figure ci-dessous illustre le processus de haut niveau suivi par les évaluations CSET.

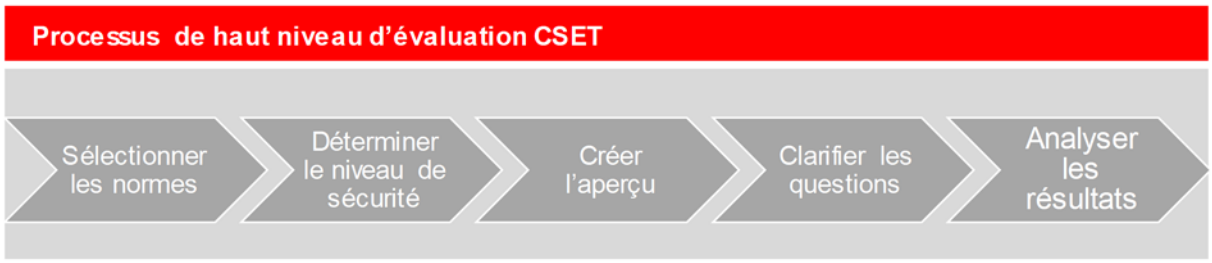

Figure 28 Processus de haut niveau d'évaluation CSET

(4) Une évaluation CSET dure en général environ une journée. Elle comporte habituellement une évaluation des exigences clés et une évaluation des composants. L'outil utilise des aperçus de réseau intégrés pour fournir une représentation visuelle de l'état actuel de la sécurité du système, pour identifier les objectifs des composants à évaluer et pour donner des instructions sur l'emplacement des mécanismes de protection de la cybersécurité, le but étant que les entreprises puissent en tirer une utilité maximale.

6. Annexe

6.1 Documents de référence et normes

(1) Le présent document tient compte des concepts, recommandations et mesures de diverses normes et autres documents normatifs (cf. tableau ci-dessous).

Titre	Année	Éditeur(s) et description
Mesures de protection des systèmes de contrôle industriels (SCI)	2013	**Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI** Basées sur des documents américains de l'Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) du Département de la Sécurité intérieure (DHS) ainsi que du National Institute of Standards and Technology (NIST), ces instructions décrivent en 8 pages, de façon succincte et pragmatique, les 11 principales mesures à mettre en œuvre par les exploitants de SCI.
Analyse des risques et des vulnérabilités du secteur partiel de l'approvisionnement électrique	2016	**Office fédéral pour l'approvisionnement économique du pays (OFAE)** Cette 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'analyser la vulnérabilité aux défaillances ou aux perturbations des TIC dans le secteur partiel critique de l'approvisionnement en électricité.
Guide pour la protection des infrastructures critiques (guide PIC)	2015	**Office fédéral de la protection de la population (OFPP)** Ce guide constitue un instrument d'examen et, le cas échéant, d'amélioration de la résilience des infrastructures critiques. Il est notamment conçu pour être utilisé dans des sous-secteurs (aussi appelés secteurs partiels) critiques (tels que l'approvisionnement en électricité) par les exploitants, les associations sectorielles (comme l'AES) et les autorités compétentes. Le guide décrit pour l'essentiel une procédure potentielle de gestion des risques: analyse (identification des ressources, vulnérabilités, risques), évaluation, mesures et leurs mise en œuvre, contrôle et amélioration. Cette procédure peut tout à fait ou devrait être intégrée aux processus de gestion existants ou exécutée sur la base de ces derniers.

Titre	Année	Éditeur(s) et description
Stratégie nationale pour la protection des infrastructures critiques (PIC)	2012	**Office fédéral de la protection de la population (OFPP)** La stratégie transcrit le champ d'application, désigne les infrastructures critiques (notamment l'approvisionnement en électricité de criticité très importante) et fixe les principes directeurs de la PIC. La stratégie nationale PIC s'adresse à tous les services qui ont des responsabilités dans ce domaine, en particulier aux différentes autorités concernées, aux responsables politiques et aux exploitants d'infrastructures critiques (p. ex. entreprises d'approvisionnement en énergie EAE).
Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC)	2012	**Département fédéral de la défense, de la protection de la population et des sports (DDPS)** La protection des infrastructures TIC contre les cyberrisques représentant un intérêt majeur pour la Suisse, le Conseil fédéral a ordonné l'élaboration d'une stratégie nationale visant à protéger notre pays contre de tels risques. Cette stratégie a pour but de dresser un panorama actuel de ces risques et de montrer les moyens dont dispose la Suisse pour y faire face, où se situent les lacunes et comment y remédier le plus efficacement possible. La stratégie identifie les structures existantes et définit des objectifs ainsi que 7 champs d'action assortis de mesures ad hoc (p. ex. analyses des risques et des vulnérabilités d'un secteur partiel tel que l'approvisionnement en électricité – cf. ci-dessus).
ICT Continuity	2011	**Association des entreprises électriques suisses (AES)** Ce document clé de l'association de branche contient des recommandations pour assurer la disponibilité constante des technologies de l'informatique et des télécommunications dans le contexte de la continuité de l'approvisionnement.
BDEW et oe: Whitepaper et Ausführungshinweise: Anforderungen an sichere Steuerungs- und Telekommunikationssysteme/Requirements for Secure Control and Telecommunication Systems (en allemand et en anglais uniquement)	2015	**Bundesverband der Energie- und Wasserwirtschaft (BDEW) et Österreichs E-Wirtschaft (oe)** Ces deux documents décrivent des mesures de sécurité techniques et opérationnelles pour les systèmes informatisés de contrôle-commande et de télécommunication nouvellement acquis ou introduits dans le domaine des processus des entreprises d'approvisionnement en énergie. L'objectif est d'influencer positivement le développement de produits et de véhiculer une compréhension commune. Ces publications ciblent les mandataires potentiels ainsi que les planificateurs et exploitants internes à l'entreprise. Les références aux normes internationales ISO 27002 et 27019 n'ont qu'une valeur indicative: seules les exigences explicitement énoncées dans les présents documents revêtent un caractère contraignant. Leur structure diffère quelque peu de celle des normes ISO.

Titre	Année	Éditeur(s) et description
Catalogue de sécurité informatique en vertu de l'art. 11, al. 1a, Energiewirtschaftsgesetz (loi relative à l'approvisionnement en électricité et en gaz)	2015	**Bundesnetzagentur (BNetzA)** En vertu de la loi (art. 11 de l'EnWG 2011), les fournisseurs d'énergie allemands ont jusqu'au 31 janvier 2018 au plus tard pour démontrer qu'ils protègent de manière adéquate leurs systèmes TIC nécessaires à l'exploitation sûre du réseau et présenter à l'Agence fédérale allemande des réseaux (Bundesnetzagentur, BNetzA) un certificat prouvant qu'ils satisfont aux exigences qui leur sont imposées. À cet effet, la BNetzA a publié le catalogue de sécurité informatique, en accord avec l'Office fédéral allemand de la sécurité des technologies de l'information (Bundesamt für Sicherheit in der Informationstechnik, BSI). La revendication majeure de ce catalogue porte sur la mise en place d'un système de gestion de la sécurité de l'information, aussi appelé système de management de la sécurité de l'information (SMSI), selon la norme DIN ISO/IEC 27001. Les exigences du catalogue de sécurité doivent être respectées par tous les gestionnaires de réseau, indépendamment de la taille ou du nombre de clients raccordés. Ce catalogue contient des obligations concrètes pour les gestionnaires de réseau, qui doivent être mises en œuvre conformément aux normes internationales.
ISO/CEI 27001:2013 **Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences**	2013	**Organisation internationale de normalisation (ISO) / Commission électrotechnique internationale (CEI)** Cette norme détaille les exigences relatives à un système de management de la sécurité de l'information (SMSI). La suite ISO/CEI 27 000 (ou ISO 27k) comprend une série de normes concernant la sécurité de l'information, dont les suivantes présentent intérêt ici: 27000:2016 Vue d'ensemble et vocabulaire (:2016 indique l'année de publication.) 27001:2013 Exigences: principes de base avec contrôles et objectifs de contrôle en annexe 27002:2013 Guide pour les contrôles 27003:2010 Lignes directrices pour la mise en œuvre 27005:2011 Gestion des risques 27019:2013 Rapport technique avec des ajouts spécifiques aux contrôles des procédés dans l'approvisionnement en électricité
ISO/CEI 27002:2013 **Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour le management de la sécurité de l'information**		

Titre	Année	Éditeur(s) et description
ISO/CEI TR 27019:2013 **Technologies de l'information – Techniques de sécurité – Lignes directrices de management de la sécurité de l'information fondées sur l'ISO/CEI 27002 pour les systèmes de contrôle des procédés spécifiques à l'industrie de l'énergie**		Désormais les plus répandues, les normes de sécurité ISO 27000 devraient s'avérer décisives dans les années à venir. Aujourd'hui déjà, la bonne approche consiste à observer les normes de sécurité ISO. Contrairement à d'autres textes normatifs comme IT-Grundschutz ou les normes du NERC, de l'ANSI/ISA ou du NIST, elles ne sont pas aussi détaillées, sont utilisables de manière flexible et peuvent être améliorées et étendues en permanence sur une plus longue période.
NERC CIP – Critical Infrastructure Protection	2006 ss	**North American Electric Reliability Corporation (NERC)** Nous en sommes actuellement à la version 5 et, pour certaines, à la version 6 des normes de protection des infrastructures critiques (normes CIP) du NERC. Il s'agit des seules normes américaines qui ne doivent pas être appliquées sur une base volontaire, mais impérativement par les «Bulk Electric Systems» (BES) ou leurs exploitants. Il est nécessaire que les BES définissent et mettent en œuvre au moins une politique de sécurité couvrant quatre domaines: sensibilisation à la sécurité, sécurité physique, accès à distance et intervention en cas d'incident. Ce faisant, il ne suffit pas simplement de documenter les politiques, mais il faut aussi mettre en œuvre les processus, les procédures et les contrôles et le vérifier dans le cadre d'un audit.
Guide to Industrial Control Systems (ICS) Security SP 800-82 Rev.2	2015	**National Institute of Standards and Technology (NIST)** Ce guide fournit une introduction complète aux ICS, aux topologies et aux architectures, identifie les menaces et les vulnérabilités, et formule des recommandations pour les contre-mesures et l'atténuation des risques. Des contrôles spécifiques aux ICS, basés sur le cadre 800-53 du NIST, sont également présentés.
ISA/CEI 62443 **Industrial Communication Networks – Network and System Security**	2009 ss	**International Society of Automation (ISA) / Commission électrotechnique internationale (CEI)** Série d'un total de 13 normes de sécurité et rapports techniques en matière de systèmes de contrôle-commande industriels (IACS). Ces normes sont généralement applicables dans le domaine de l'automatisation industrielle et ne sont pas spécifiques à l'approvisionnement en électricité. Elles se basent sur les normes ISO 27000 et les étoffent par l'ajout de différences et de particularités propres à l'automatisation industrielle. Il convient de mentionner notamment le traitement de l'architecture réseau et zonale, qui n'est guère ou pas aussi détaillé dans d'autres normes.

Titre	Année	Éditeur(s) et description
CEI 62351 **Power Systems Management and Associated Information Exchange – Data and Communications Security (Gestion des systèmes électriques et échanges d'informations connexes – Sécurité des données et des communications)**	2007 ss	**Commission électrotechnique internationale (CEI)** Cette norme spécifique à l'approvisionnement en électricité complète la norme CEI 62443 par l'adjonction de différences et d'extensions en matière de production, de transport et de distribution de courant. Elle s'ajoute à d'autres normes telles que CEI 61850 relative à l'automatisation des sous-stations et CEI 60870 concernant ICCP/TASE.2 avec des protocoles de communication série et IP. Les normes CEI 62351 (il en existe aujourd'hui 13 parties) sont techniquement détaillées et difficiles à comparer avec les normes de sécurité conceptuelles.
IEEE 1686 **IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities**	2013	**Institute of Electrical and Electronics Engineers (IEEE)** Cette norme définit les fonctions et les configurations qui doivent être fournies dans les dispositifs électroniques intelligents (DEI) en vue d'assurer la sécurité OT de l'infrastructure critique. Les thèmes abordés sont la sécurité concernant l'accès, l'exploitation, la configuration, la révision du microprogramme et la récupération des données d'un DEI, ainsi que le cryptage des données en provenance et à destination de celui-ci. Cette norme ne traite pas des communications à des fins de protection électrique (téléprotection) ni de protection de la vie, de l'intégrité corporelle et de l'environnement. Elle se base dans une certaine mesure sur les normes NERC CIP (Critical Infrastructure Protection) et les complètent au niveau des DEI, de sorte que les dispositifs électroniques ne portent pas atteinte aux exigences NERC CIP.
Recommended Practice: **Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies**	2016	**Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)** Édition revue et corrigée d'une précédente publication datant de 2006. Introduction complète à la stratégie de défense en profondeur dans le cadre de la sécurité des systèmes de contrôle industriels.

Titre	Année	Éditeur(s) et description
BSI IT-Grundschutz **BSI – Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz** **(V1.2 2014)** **BSI – Zuordnungstabelle ISO 27001 sowie ISO 27002 und IT-Grundschutz**	2014 SS	**Bundesamt für Sicherheit in der Informationstechnik (BSI)** A l'aide des normes 100-1 à 100-3 du BSI, l'«IT-Grundschutz» (méthodologie de protection de base des technologies de l'information) décrit une procédure de mise en place et de maintien d'un système de management de la sécurité de l'information (SMSI). Les catalogues et le compendium de l'IT-Grundschutz détaillent la mise en œuvre des mesures et des objectifs qui en découlent. Le SMSI ainsi créé satisfait aux exigences de la norme ISO 27001 et dispose d'un équivalent aux recommandations de la norme ISO 27002. La sécurité peut être introduite et contrôlée selon les procédures de l'IT-Grundschutz developpées par le BSI, mais aussi conformément aux normes de la famille ISO 27000. Ces deux options sont compatibles dans leur approche. Elles sont utilisées pour mettre en place et exploiter un SMSI, qui identifie les risques dans le domaine de la sécurité de l'information et les réduit à un niveau acceptable par le biais de mesures appropriées. Alors que l'analyse et l'évaluation des risques constituent un élément essentiel d'un SMSI conforme à la norme ISO 27001, cette analyse n'est requise que dans certains cas particuliers pour l'IT-Grundschutz du BSI. Les catalogues de cette protection de base décrivent par le menu la procédure permettant de réduire au maximum les risques. Quant aux normes ISO, elles laissent davantage de place à l'interprétation et offrent une plus grande souplesse, mais fournissent également des instructions et un soutien moins détaillés. À l'inverse, l'approche de l'IT-Grundschutz, comme son nom l'indique, offre une «protection de base». L'effort requis pour obtenir la certification ISO est moindre.
BSI – ICS-Security-Kompendium	2013	**Bundesamt für Sicherheit in der Informationstechnik (BSI)** Ce compendium est un ouvrage de référence destiné à faciliter l'accès à la sécurité informatique dans les ICS. Les bases nécessaires à la compréhension des ICS, les processus y afférents, les normes pertinentes et un lien concret avec l'IT-Grundschutz y sont expliqués, les différences et lacunes des normes établies, et en particulier de l'IT-Grundschutz dans le domaine de la sécurité ICS étant mises en lumière.
BSI-Standard 200-1 Managementsysteme für Informationssicherheit (ISMS)	2017	**Bundesamt für Sicherheit in der Informationstechnik (BSI)** Cette norme décrit les méthodes, les tâches et les activités pertinentes qui font le succès d'un SMSI et précise les tâches qui incombent à la direction. La méthodologie de l'IT-Grundschutz, qui explique pas à pas comment développer un SMSI dans la pratique et cite des mesures concrètes pour tous les aspects relevant de la sécurité de l'information, favorise la mise en œuvre des recommandations. La norme 200-1 s'adresse aux responsables de l'exploitation informatique, aux délégués à la sécurité, ainsi qu'aux experts et conseillers en sécurité chargés de la gestion de la sécurité de l'information.

Titre	Année	Éditeur(s) et description
BSI-Standard 200-2 IT-Grundschutz Vorgehensweise	2017	**Bundesamt für Sicherheit in der Informationstechnik (BSI)** La procédure de l'IT-Grundschutz décrit, étape par étape, comment mettre en place et exploiter un système de management de la sécurité de l'information dans la pratique et à l'aide des catalogues de cette protection de base. Elle se penche de façon très approfondie sur la manière d'élaborer en pratique un concept de sécurité, sur le choix des mesures de sécurité adéquates, ainsi que sur les éléments à prendre en compte lors de la mise en œuvre.
BSI-Standard 200-3 Risikoanalyse	2017	**Bundesamt für Sicherheit in der Informationstechnik (BSI)** Ce document décrit une méthodologie pour réaliser des analyses de risques, qui complètent un concept de sécurité existant en matière de protection de base des technologies de l'information. Les dangers présentés dans les catalogues de l'IT-Grundschutz sont utilisés comme outils. Une différence essentielle par rapport à la plupart des autres méthodes d'analyse de risques est l'omission totale de la probabilité de survenance des dommages.
BSI-Standard 100-4 Notfallorganisation	2008	**Bundesamt für Sicherheit in der Informationstechnik (BSI)** Ce document décrit une méthodologie pour mettre en place un système de gestion des cas d'urgence fondée sur les procédures figurant dans la norme 100-2 et les complétant. Il présente tous les processus au sein d'une organisation pour cas d'urgence, de l'analyse d'impact sur les affaires à la gestion de crise, en passant par le retour à l'exploitation normale et les activités continues de processus en dehors des situations de crise.
ISA 95 / IEC/ISO 62264 **Intégration du système de commande d'entreprise**	2010 ss	**International Society of Automation (ISA) / Commission électrotechnique internationale (CEI)** Série de 5 normes relatives à l'intégration des systèmes informatiques d'entreprise et de contrôle-commande.
Framework for Improving Critical Infrastructure Cybersecurity	2014 Draft v1.1 2017	**National Institute of Standards and Technology (NIST)** Ce cadre découle de l'exigence posée par le décret présidentiel américain intitulé «Improving Critical Infrastructure Cybersecurity» (Améliorer la cybersécurité des infrastructures critiques), datant de 2013. Il s'agit d'une compilation de différentes orientations visant à déterminer le statut actuel d'une entreprise et à définir une feuille de route pour l'amélioration des pratiques de cybersécurité en se référant à d'autres cadres et normes tels que ISO 27001, ISA 62443, NIST 800-53 et COBIT.
Energy Sector Cybersecurity Framework Implementation Guidance	2015	**Department of Energy (DOE)** Instructions du Département américain de l'Énergie (DOE) pour la mise en œuvre d'un cadre de cybersécurité des infrastructures critiques basé sur le cadre du NIST.

Titre	Année	Éditeur(s) et description
Report on Cyber Security Information Sharing in the Energy Sector	2016	**Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)** Ce rapport a pour objectif de comprendre et d'en savoir plus sur le développement des CSIRT (Computer Security Incident Response Teams) et des ISAC (Information Sharing and Analysis Centres), ainsi que sur les initiatives pertinentes concernant l'échange d'informations sur les incidents de cybersécurité dans le secteur de l'énergie. Il se concentre sur les sous-secteurs de l'électricité, du pétrole et du gaz identifiés dans la directive NIS (Parlement européen et Conseil, 2016: sécurité des réseaux et des systèmes d'information).
Communication network dependencies for ICS/SCADA Systems	2016	**Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)** Ce rapport se focalise sur les aspects des réseaux de communication et de l'intercommunication entre les systèmes ICS/SCADA et l'identification des vulnérabilités, des risques, des menaces et des conséquences en matière de sécurité pouvant être causés par les systèmes cyber-physiques. Il comporte également un certain nombre de recommandations destinées à réduire les risques détectés. La principale conclusion de l'étude préliminaire est une liste de pratiques et de directives éprouvées visant à limiter autant que possible la surface des systèmes ICS/SCADA exposée aux attaques. Le document a pour objectif principal de fournir un aperçu des dépendances des réseaux de communication des systèmes ICS/SCADA et d'identifier les ressources critiques en matière de sécurité et les scénarios d'attaques et menaces réalistes contre ces réseaux de communication.
VDI/VDE 2182 **Informationssicherheit in der industriellen Automatisierung (IT-security for industrial automation)**	2011 – 2016	**Verein Deutscher Ingenieure (VDI) / Verband der Elektrotechnik, Elektronik und Informationstechnik (VDE)** Cette directive explique comment atteindre la sécurité de l'information des machines et installations automatisées par la mise en œuvre de mesures de protection concrètes. Pour ce faire, les aspects des dispositifs, systèmes et applications d'automatisation utilisés sont pris en compte. Une procédure uniforme et réalisable précisant comment garantir a sécurité informatique tout au long du cycle de vie des dispositifs, systèmes et applications d'automatisation est décrite, sur la base d'une définition commune des termes convenus entre leurs fabricants et leurs utilisateurs (p. ex. constructeurs de machines, intégrateurs et exploitants). Le cycle de vie couvre les phases de développement, d'intégration, d'exploitation, de migration et de mise hors service. Cette directive définit un modèle de procédure simple pour le traitement et la présentation de la sécurité de l'information, modèle qui comprend plusieurs étapes de processus.

Tableau 39 Normes nationales et internationales relatives à la sécurité des TIC

6.2 Glossaire

Termes	Définition
Accord sur le niveau de service (SLA)	«SLA» est l'abréviation de «service level agreement». On entend par là une prestation contractuellement convenue qu'un prestataire de services informatiques s'est engagé à fournir. Le SLA définit habituellement les temps d'arrêt et de réaction maximaux autorisés.
Adresse MAC (media access control)	On appelle adresse MAC l'adresse matérielle unique dans un adaptateur réseau. Elle est gravée par le fabricant dans la ROM de manière inaltérable. Chaque adresse attribuée est unique au monde.
Appareil de terrain	Dans le domaine de l'automatisation, un appareil de terrain est un dispositif technique directement lié à un processus de production. En automatisation, «terrain» désigne la zone située à l'extérieur des armoires de couplage ou des salles de contrôle.
Audit de sécurité	On entend par «audit de sécurité» un examen complet des mesures organisationnelles et techniques de cybersécurité. Il s'agit de l'analyse des vulnérabilités de la cybersécurité dans les domaines de la conception/de l'architecture, de la mise en œuvre, de l'exploitation, des erreurs humaines et de la sécurité du site, ainsi que de la sécurité des différents composants du système.
Automate programmable industriel (API)	Un automate programmable industriel est un dispositif utilisé pour commander ou réguler une machine ou une installation et programmé sur une base numérique. (Source: Wikipédia allemand)
Bus de station	Système de bus dans une sous-station (SST) situé entre le poste de conduite de la SST et les capteurs du champ électrique.
Bus de terrain	Un bus de terrain est un élément de réseau permettant d'interconnecter plusieurs appareils dans un environnement OT. Les bus de terrain fonctionnent par définition en temps réel. En règle générale, au sein d'une installation, des appareils de terrain, tels que des détecteurs (capteurs) et des actionneurs, sont connectés à un dispositif d'automatisation à des fins de communication.
Business continuity management (BCM)	Le business continuity management (BCM), ou gestion de la continuité des activités (CGA), est une méthode de gestion mise en œuvre à l'échelle de l'entreprise, qui a pour but d'assurer la continuité opérationnelle des processus d'exploitation critiques en cas d'événements, internes ou externes, ayant une incidence massive et radicale sur l'activité de l'entreprise. Le BCM vise à réduire au maximum les conséquences de tels événements sur les plans opérationnel, financier et juridique ainsi qu'en termes de réputation (source: instructions en matière de BCM).
Commande de processus	La commande de processus désigne les moyens et les procédés servant à piloter, à réguler et à sécuriser les installations de traitement. Le système de contrôle-commande des processus et l'automate programmable y jouent un rôle essentiel.
Commutateur (en anglais switch)	Dans les réseaux informatiques, un commutateur, ou switch, est un élément de couplage qui relie des segments de réseau entre eux.

Termes	Définition
Compteur	Cf. compteur électrique
Compteur électrique	Compteur destiné à la mesure de l'énergie électrique (totalisation de la puissance active).
Confidentialité	La confidentialité est la protection contre la divulgation prohibée d'informations. Les données et informations confidentielles peuvent uniquement être accessibles aux personnes autorisées de manière licite. (Source: BSI)
Contrôle-commande	Le contrôle-commande regroupe les flux de données des niveaux subordonnés, du terrain ou de cellules individuelles, comme par exemple les signaux des techniques de mesure, de commande et de régulation, afin de piloter et de surveiller l'ensemble du processus de production.
Contrôle-commande de la station	Commande globale dans une sous-station, constituée d'un poste de conduite, de capteurs et d'actions. Elle assure la liaison entre le processus et le niveau de commande du réseau.
Contrôle-commande de terrain	Contrôle-commande «sur site» et surveillance «sur site» des différentes cellules de couplage.
Cryptage	Le cryptage (ou chiffrement) est la conversion, à l'aide d'une clé, de données appelées «texte en clair» en un «cryptogramme» (ou «texte chiffré»), de sorte qu'on ne peut déchiffrer ce message codé qu'en utilisant une clé secrète.
Culture de sécurité	La culture de sécurité comprend les valeurs, les visions du monde, les comportements verbaux et non verbaux ainsi que les caractéristiques de l'environnement physique créé par l'être humain partagés par les membres de l'organisation de l'exploitant d'une installation nucléaire. Les valeurs, visions du monde, comportements et caractéristiques de l'environnement qui déterminent ou montrent comment les membres de l'organisation traitent de la sûreté nucléaire appartiennent à la culture de sécurité. (Source: IFSN)
Cybersécurité	Le terme «cybersécurité» désigne toutes les mesures organisationnelles et techniques visant à protéger la disponibilité, l'intégrité et la confidentialité des informations, aussi bien dans le domaine des technologies de l'information que des technologies opérationnelles.
Défense en profondeur	On entend par «défense en profondeur» («defense in depth») des concepts de sécurité sur plusieurs niveaux, qui vont au-delà de la sécurité informatique purement technique. Les concepts de défense en profondeur prennent également en compte par exemple la sécurité physique, la gestion de la continuité des activités, les processus, les personnes et les prestataires de services externes.
Diode réseau	Une diode réseau est un dispositif qui n'autorise le trafic réseau que dans une seule direction. Le principe est le suivant: les données peuvent uniquement être transférées d'une zone sécurisée vers une zone non sécurisée du réseau, et non l'inverse.

Termes	Définition
Disponibilité	La disponibilité de services, de fonctions d'un système informatique, d'applications ou de réseaux informatiques ou d'informations est assurée si les utilisateurs peuvent toujours s'en servir comme prévu. (Source: BSI)
Dispositif électronique intelligent (DEI)	Un dispositif électronique intelligent (DEI, en anglais intelligent electronic device ou IED) est un terme utilisé dans le secteur de l'électricité pour décrire les commandes à microprocesseur des systèmes d'alimentation électrique, comme par exemple les disjoncteurs, les transformateurs et les batteries de condensateurs.
Durcissement	En informatique, le durcissement est le processus destiné à sécuriser un système. La démarche consiste principalement à réduire à l'indispensable les objets (logiciels, bibliothèques logicielles, outils) installés sur le système, ainsi qu'à éliminer les utilisateurs et les droits non indispensables, tout en conservant les fonctionnalités requises. Le principe sous-jacent est la réduction de la surface d'attaque possible. (Source: Wikipédia)
Exploitation normale	État de l'installation respectant des limites d'exploitation spécifiées et conforme aux prescriptions en vigueur. (Source: IFSN)
Facility management	Cf. gestion technique de bâtiment
Field bus	Cf. bus de terrain
Field device	Cf. appareil de terrain
Frontal (frontend ou front-end)	Cf. poste maître de téléconduite
Gestion technique de bâtiment	La GTB désigne l'administration et la gestion de bâtiments ainsi que de leurs installations et équipements techniques.
Hiérarchie numérique plésiochrone (PDH)	La hiérarchie numérique plésiochrone (en anglais plesiochronous digital hierarchy, PDH) est une technologie standardisée à l'échelle internationale, destinée au multiplexage des flux de données numériques transmis sur de longues distances. Les flux de données doivent être sensiblement synchrones. Aujourd'hui, cette technologie est presque exclusivement utilisée à des débits allant jusqu'à 45 Mbit/s.
Hiérarchie numérique synchrone (SDH)	La hiérarchie numérique synchrone (en anglais synchronous digital hierarchy, SDH) est l'une des techniques de multiplexage utilisées dans les télécommunications, qui permet de compiler des flux de données à bas débit pour former un flux de données à haut débit. L'ensemble du réseau est alors synchrone.
Human-machine-interface (HMI)	Cf. interface homme-machine
Immotique	Cf. gestion technique de bâtiment
Information communications technology (ICT)	Cf. technologies de l'information et de la communication

Termes	Définition
Intégrité	L'intégrité désigne la garantie de l'exactitude (intégrité) des données et du fonctionnement correct des systèmes. Lorsque ce terme s'applique aux données, il indique que celles-ci sont complètes et n'ont subi aucune altération. Toutefois, dans les technologies de l'information, l'intégrité est en général prise dans une acception plus large qui couvre les «informations». Le terme «information» désigne des «données» auxquelles, en fonction du contexte, on peut affecter certains attributs tels que l'auteur ou la date de création. La perte d'intégrité des informations peut donc signifier que celles-ci ont été modifiées de manière illicite, que les données relatives à l'auteur ont été falsifiées ou que la date et l'heure de création ont fait l'objet d'une manipulation. (Source: BSI)
Interface homme-machine (IHM)	L'interface utilisateur est aussi appelée «interface homme-machine» (IHM) ou, en anglais, «human-machine interface» (HMI) ou «man-machine interface» (MMI). Elle permet à l'opérateur, le cas échéant, d'observer l'état des installations et d'intervenir dans le processus, en plus de manœuvrer la machine.
IT security	Cf. sécurité informatique
KPI	Le terme Key Performance Indicator (KPI) ou indicateur clé de performance désigne des chiffres clés au moyen desquels le progrès ou le degré de réalisation d'objectifs importants ou de facteurs de succès critiques au sein d'une organisation peut être mesuré ou calculé.
Local area network (LAN)	Un réseau local, ou LAN, est un réseau informatique qui relie des ordinateurs et des appareils intelligents dans une zone géographique limitée (habituellement moins de 10 km).
Logiciel malveillant	Cf. maliciel
Maliciel	Programme informatique conçu pour exécuter des fonctions indésirables ou potentiellement nuisibles.
Man-machine interface (MMI)	Cf. interface homme-machine
MELANI	La Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI est une organisation de l'administration fédérale, qui a pour principale mission de protéger les infrastructures critiques de la Suisse.
Multiprotocol Label Switching - Transport Profile (MPLS-TP)	MPLS-TP a été spécialement optimisé pour les réseaux métropolitains, d'agrégation et d'accès. Les objectifs sont les suivants: offrir des fonctionnalités comparables à celles des technologies de multiplexage par répartition dans le temps (MRT, en anglais time division multiplexing ou TDM) et prendre en charge les liaisons point à point et les connexions any-to-any avec un niveau de prévisibilité et de fiabilité et des fonctions OAM (operations, administration and management) similaires à ce que proposent les réseaux TDM éprouvés depuis longtemps.

Termes	Définition
Multiprotocol Label Switching (MPLS)	Multiprotocol Label Switching permet la transmission en mode connecté de paquets de données dans un réseau sans connexion sur un chemin d'accès préalablement défini («signalé»). Ce procédé de commutation est principalement utilisé par les opérateurs de grands réseaux de transport qui offrent des services voix et données basés sur IP. (Source: Wikipédia allemand)
Network access control (NAC)	Le NAC ou contrôle d'accès au réseau désigne une technique utilisée pour se protéger contre les accès non autorisés au réseau.
Network address translation (NAT)	Network address translation (NAT) est le nom d'un procédé de remplacement automatique et transparent des informations d'adresse dans les paquets de données. Les procédés NAT sont généralement utilisés sur les routeurs et les barrières de sécurité, notamment pour exploiter le plus efficacement possible l'espace d'adressage IPv4 restreint et pour cacher les adresses IP locales des réseaux publics. (Source: BSI)
Objectif de protection	Les objectifs de protection décrivent les objets à protéger par des mesures ad hoc.
Objet à protéger	Les objets à protéger sont des infrastructures, des services, des systèmes, des applications, des réseaux, des fichiers de données, etc., qui sont utilisés pour accomplir la mission de l'entreprise et doivent donc être protégés.
OEM	Original Equipment Manufacturer, traduit par «fabricant d'équipement d'origine». On entend par là un fabricant de composants ou de produits qui produit ces éléments dans ses propres usines, mais ne les apporte pas lui-même dans le commerce de détail. Un logiciel OEM peut se différencier de la «version complète» (*retail*) par une plus faible étendue des fournitures ou des fonctionnalités restreintes.
Pare-feu (ou firewall)	Un pare-feu, ou firewall (également connu sous le nom de barrière de sécurité), est un système de composants logiciels et matériels permettant de coupler en toute sécurité des réseaux IP. (Source: BSI)
Passerelle	En informatique, une passerelle (en anglais, gateway) est le nom générique d'un dispositif permettant de relier deux réseaux de types différents. (Source: Wikipédia)
Poste maître de téléconduite	On utilise le concentrateur de données comme appareil de télécommande pour automatiser la station du réseau local et pour saisir les données des compteurs.
Programmable logic controller (PLC)	Cf. automate programmable industriel
Protection SIS	Cf. système de protection
Remote terminal unit (RTU)	On appelle «remote terminal unit» (RTU) ou «unité terminale distante» un instrument de régulation ou de pilotage permettant d'effectuer la commande à distance.

Termes	Définition
Risque	Le risque désigne la prédiction, souvent basée sur des calculs, d'un dommage possible dans le cas négatif (danger) ou d'un avantage potentiel dans le cas positif (chance). La perception d'un dommage ou d'un avantage dépend des valeurs. Par ailleurs, on définit fréquemment le risque comme la combinaison de la probabilité de survenance et de l'ampleur d'un dommage. (Source: BSI)
Routeur	Un routeur est un dispositif réseau capable d'acheminer des paquets entre plusieurs réseaux informatiques.
Sandbox	Une sandbox (anglicisme signifiant «bac à sable») est une zone isolée au sein d'une application ou d'un système d'exploitation, qui empêche l'exécution d'actions indésirables en dehors de l'environnement contrôlé. Cela permet de parer aux dangers et aux conséquences des logiciels malveillants. (Source: BSI)
Sécurité informatique	Le terme «sécurité informatique», aussi appelée «sécurité TI» ou «sécurité IT», désigne toutes les mesures organisationnelles et techniques visant à protéger la disponibilité, l'intégrité et la confidentialité des informations. Dans ce contexte, on entend par technologies de l'information (TI) les technologies de traitement des données qui ne sont pas directement liées à la fourniture d'électricité (p. ex. gestion des données clients, centres de calcul).
Sécurité OT	Le terme «sécurité OT» désigne toutes les mesures organisationnelles et techniques visant à protéger la disponibilité, l'intégrité et la confidentialité des informations requises pour la surveillance et le pilotage des installations de distribution (et de production) d'électricité, ainsi que la protection des personnes et des équipements. Dans ce contexte, on entend par technologies opérationnelles (OT) les technologies directement nécessaires à la mise à disposition ou à la fourniture de courant (p. ex. système SCADA, système PIA, accès à distance aux installations des sous-stations, télécommande centralisée, smart meter).
Security information and event management (SIEM)	Les systèmes de gestion des informations et des événements de sécurité (SIEM) sont utilisés pour identifier et évaluer les incidents de sécurité et pour alerter l'administrateur en conséquence.
Smart metering	Systèmes de mesure intelligents capables de transmettre leurs données de mesure et d'effectuer des tâches de commande via une communication bidirectionnelle.
Supervisory control and data acquisition (SCADA)	Un système d'acquisition et de contrôle de données, ou système SCADA, désigne la surveillance et la commande de processus techniques au moyen d'un système informatique. Synonyme: système ICS (industrial control system, système de contrôle industriel)
Système de couplage de processus	Le système de couplage de processus constitue l'élément de liaison entre le niveau des processus et le niveau de commande.

Termes	Définition
Système de détection des intrusions (intrusion detection system, IDS)	Un IDS est un système destiné à la détection automatique des attaques sur les réseaux informatiques.
Système de management de la sécurité de l'information (SMSI)	Un système de management ou de gestion de la sécurité de l'information (en anglais information security management system ou ISMS) est un ensemble de procédures et de règles au sein d'une entreprise, qui servent à définir, à commander, à contrôler, à maintenir durablement et à améliorer continuellement la sécurité de l'information.
Système de prévention des intrusions (intrusion prevention system, IPS)	Un IPS est capable de détecter les attaques sur des réseaux ou des systèmes informatiques et de prendre des mesures de défense automatiques.
Système de protection	Système de sécurité constitué de capteurs, d'une unité de traitement logique et d'éléments de commande, conçu pour ramener un processus à un état sûr en cas de non-respect des conditions prédéfinies.
Système patrimonial (legacy system)	Un système patrimonial décrit, en informatique, une application établie qui continue d'être utilisée dans le domaine logiciel d'une entreprise.
Système PIA (Partner Informationsaustauch)	Système d'échange d'informations entre partenaires. Plateforme fermée suisse ayant pour but d'échanger des données entre les postes de conduite. Ces informations sont avant tout utilisées pour la gestion et la conduite du réseau.
Systèmes de contrôle industriels (industrial control systems, ICS)	Les systèmes de contrôle industriels sont utilisés dans l'industrie et dans le domaine des infrastructures critiques pour assurer les fonctionnalités de commande, de mesure et de régulation.
Technique de conduite de réseau	Elle englobe les techniques de mesure, de commande et de régulation des réseaux, tels que les réseaux électriques. La technique de conduite de réseau est un domaine particulier de la commande de processus; elle fait partie de l'ingénierie appliquée.
Technique primaire	Outre les transformateurs nécessaires à la conversion de la tension, le poste de transformation dispose également d'installations de couplage pour les lignes sortant du côté de la tension primaire et de la tension secondaire. Les équipements techniques (transformateurs, barres collectrices, etc.) et les lignes sont en général conçus de manière redondante, de sorte que l'approvisionnement reste garanti en cas de défaillance d'un moyen d'exploitation.
Technique secondaire	Le terme «technique secondaire» regroupe les équipements d'un poste de transformation qui ne sont pas directement impliqués dans la transformation de la tension. Il s'agit p. ex. de la commande locale, de la régulation de tension, de la protection du réseau, du comptage d'énergie ou de la commande à distance.
Technologies de l'information et de la communication (TIC)	Les technologies de l'information et de la communication (TIC) désignent les méthodes et les technologies utilisées pour transmettre, recevoir et traiter les informations (y compris les technologies numériques).

Termes	Définition
Téléconduite	On entend par «téléconduite», ou «téléaction», la surveillance et la commande à distance d'objets éloignés au moyen de procédés de conversion de signaux, à partir d'un ou de plusieurs emplacements. (Source: Wikipédia allemand)
Téléphonie interne	Téléphone d'urgence destiné à la communication entre les postes de conduite, les centrales électriques et les stations. Il est utilisé notamment en cas de défaillance du système de contrôle-commande et pour la téléphonie mobile et de bureau.
Test d'intrusion	Un test d'intrusion (penetration test en anglais) est un test de sécurité complet des différents systèmes ou réseaux. Il s'agit de contrôler la mise en œuvre technique des mesures de cybersécurité. Les tests d'intrusion font partie intégrante d'un audit de sécurité.
Tunnellisation	Dans un réseau, la tunnellisation, ou mise sous tunnel, désigne la conversion et la transmission d'un protocole de communication qui est intégré dans un autre protocole de communication pour le transport.
Utility	Entreprise d'approvisionnement en énergie
Virtual LAN (VLAN)	Les réseaux locaux virtuels, ou VLAN, sont utilisés pour la structuration logique des réseaux. Une structure logique de réseau est mappée au sein d'un réseau physique en connectant des postes de travail et des serveurs liés de manière fonctionnelle à un réseau virtuel.
Virtual private network (VPN)	Un réseau privé virtuel est un réseau de communication privé (fermé) qui utilise un réseau de communication existant comme moyen de transport.
Wide area network (WAN)	Un réseau étendu, ou WAN, est un réseau informatique qui, contrairement à un LAN, couvre une très grande zone géographique.
Zone démilitarisée (demilitarized zone, DMZ)	Une zone démilitarisée désigne un sous-réseau logiquement et/ou physiquement séparé, avec un contrôle de sécurité des possibilités d'accès aux systèmes qui y sont raccordés.

Tableau 40 Glossaire

6.3 Abréviations

Abréviation	Développé
API	Automate programmable industriel
DMZ	Demilitarized zone
HMI	Human-machine interface
ICS	Industrial control systems
ICT	Information and communication technology
ICT	Information communications technology
IDS	Intrusion detection system
IED	Intelligent electronic device
IHM	Interface homme-machine
IPS	Intrusion prevention system
IT	Information technology
KVM	Keyboard, Video und Maus = clavier, écran, souris
LAN	Local area network
MAC address	Media access control address
MMI	Man-machine interface
MPLS	Multiprotocol Label Switching
MPLS-TP	Multiprotocol Label Switching - Transport Profile
NAC	Network access control
NAT	Network address translation
OT	Operational technology
PDH	Plesiochronous digital hierarchy
PIA	Partner Informationsaustausch, échange d'informations entre partenaires
PLC	Programmable logic controller
RTU	Remote terminal unit
SCADA	Supervisory control and data acquisition
SDH	Synchronous digital hierarchy
SIEM	Security information and event management
SLA	Service level agreement, accord sur le niveau de service
SMSI	Système de management de la sécurité de l'information
TIC	Technologies de l'information et de la communication
UFLS	Under Frequency Load Shedding = délestage automatique sur seuil de fréquence
VLAN	Virtual LAN
VPN	Virtual private network
WAN	Wide area network

Tableau 41 Liste des abréviations