Norme minimale pour garantir la sécurité des technologies de l'information et de la communication (TIC) requises pour l'approvisionnement du chauffage et du froid à distance

F1001 f édition février 2023

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Thermische Netze
Réseaux Thermiques
Reti Termiche

SVGW
SSIGE

Résumé

La généralisation et l'interconnexion des technologies de l'information et de la communication (TIC) offrent un potentiel économique et social incontournable. Cependant, cette numérisation croissante génère aussi de nouveaux risques, auxquels il convient de réagir rapidement et de manière appropriée. La cybersécurité des infrastructures critiques d'un pays relève d'une importance capitale et il est essentiel de les protéger convenablement en accordant un intérêt particulier à leurs systèmes TIC.

Dans le secteur des réseaux thermiques[1] qui englobent le chauffage et le froid à distance, la majorité des activités opérationnelles sont gérées par un système de contrôle industriel (ICS)[2]. Il s'agit d'un ensemble d'éléments de contrôle qui interagissent ensemble afin d'atteindre un objectif commun. La tâche de ce système consiste à collecter des données provenant de processus variables ou des statuts de machines industrielles mais aussi à contrôler et surveiller ces machines sur place ou à distance. Il s'agit donc d'un composant fondamental qui permet de gérer l'ensemble des tâches des installations industrielles et qu'il est primordial de protéger contre les cybermenaces et le vol de données qu'il encourt.

Pour gérer efficacement la problématique de la cybersécurité, il est nécessaire d'avoir une bonne connaissance des enjeux actuels en matière de sécurité et des contre-mesures disponibles. La présente norme minimale TIC constitue un cadre permettant aux organisations du secteur des réseaux thermiques, non seulement de se prémunir contre d'éventuelles attaques ou erreurs de manipulation, mais aussi de restaurer leurs systèmes le plus rapidement possible en cas d'incident. Ce cadre de sécurité permet à l'entreprise d'évaluer elle-même le risque encouru et de mettre en œuvre les mesures appropriées.

La norme minimale TIC repose essentiellement sur le programme de cybersécurité du *NIST Framework Core*[3] permettant ainsi de garantir une méthode de protection efficace et offrant aux différents secteurs économiques la possibilité de disposer d'un programme de cybersécurité aux résultats comparables et cohérents. En effet, la norme minimale TIC de l'Office fédéral pour l'approvisionnement économique du pays ainsi que ses différentes versions dédiées à un secteur spécifique reposent sur les mêmes mesures. Cette homogénéité offre ainsi la possibilité aux sociétés actives dans plusieurs domaines (ex : électricité[4], eau potable[5], gaz[6], réseaux thermiques, etc.) d'utiliser un programme de cybersécurité commun.

Le présent document est divisé en sept chapitres. Le premier constitue une introduction à la norme minimale et au secteur des réseaux thermiques en tant qu'infrastructure critique pour l'approvisionnement du pays. Le deuxième se concentre sur le secteur des réseaux thermiques en développant sa structure, ses processus TIC ainsi que l'évaluation de ses activités critiques. Le chapitre trois s'oriente sur les besoins et les contraintes particuliers d'un ICS. Les chapitres quatre et cinq détaillent les différentes parties du programme de cybersécurité de la norme minimale TIC comprenant la gestion des risques, la stratégie de *defense-in-depth* et les mesures de cybersécurité du *NIST Framework Core*. Finalement, les chapitres six et sept clôturent ce rapport en contenant, respectivement, la conclusion et les annexes.

[1] Dans le cadre de ce document, le terme « réseau thermique » fait toujours référence au chauffage et au froid à distance

[2] ICS : Industrial Control System (système de control industriel). Plus d'informations au chapitre 3.1.

[3] Il s'agit d'un cadre américain permettant aux organisations publiques et privées de renforcer leur cybersécurité, qui s'articule autour de cinq fonctions : identifier, protéger, détecter, réagir, récupérer. Plus d'information aux chapitres 4 et 5

[4] Handbuch Grundschutz für « Operational Technology » in der Stromversorgung. Association des entreprises électriques suisses (AES), Aarau 2018 (n'existe qu'en allemand).

[5] Norme minimale pour garantir les technologies de l'information et de la communication (TIC) requises pour l'approvisionnement en eau. Société Suisse de l'Industrie du Gaz et des Eaux (SSIGE), Zurich 2019.

[6] Norme minimale pour garantir les technologies de l'information et de la communication (TIC) requises pour l'approvisionnement en gaz. Société Suisse de l'Industrie du Gaz et des Eaux (SSIGE), Zurich 2020.

Sommaire

1 Introduction

1.1 Contexte et vue d'ensemble

L'approvisionnement économique du pays (AEP), respectivement l'Office fédéral de l'approvisionnement économique du pays, s'est intéressé à la vulnérabilité des systèmes TIC requis pour assurer l'approvisionnement des réseaux thermiques dans le cadre de la Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC)[7]. L'objectif étant d'introduire un niveau de sécurité TIC minimal permettant ainsi aux organisations de ce secteur de se protéger convenablement contre les cyberrisques auxquels elles peuvent être confrontées.

En Suisse, le secteur des réseaux thermiques (chauffage et froid à distance) a pour principale fonction de chauffer les bâtiments, de fournir de l'eau chaude sanitaire ainsi que de produire de la chaleur pour les secteurs industriels. Il s'agit d'un domaine particulièrement hétérogène qui est composé d'une multitude d'acteurs ayant recourt à des sources énergétiques et des processus industriels variés pour produire de la chaleur. Selon différents rapports d'experts[8], il s'agit d'un secteur qui devrait profiter des nouvelles politiques énergétiques du pays. Il est donc plausible de s'attendre à une augmentation de sa production ainsi qu'une extension de son réseau. Si dans les années à venir, l'expansion de ce secteur se concrétise, un dysfonctionnent impactant ses infrastructures n'en serait donc que plus préoccupant pour l'approvisionnement du pays. Il est donc nécessaire de protéger correctement ce secteur contre les risques qu'il encourt.

Les entreprises actives dans le secteur des réseaux thermiques utilisent quotidiennement des systèmes TIC pour mener à bien leurs tâches. Pour gérer leurs activités industrielles, elles se servent d'un système de contrôle industriel (ICS) dont le plus important est le système de commande qui est un élément central de la pyramide d'automatisation (voir chapitre 2.4.2). Il permet notamment de centraliser l'acquisition, la surveillance, le contrôle et le traitement des données. Il s'agit d'un élément primordial pour la partie opérationnelle d'une organisation qui lui permet de gérer ses installations industrielles en lien avec la production de la chaleur, son transport ainsi que sa consommation. Les systèmes TIC permettent aussi aux entreprises de réaliser un certain nombre d'activités organisationnelles liées à la gestion des tâches quotidiennes ou administratives. Il est question des infrastructures de télécommunication, des services de communication ou encore des systèmes de gestion intégré (ERP). Un dysfonctionnement TIC de l'un des différents éléments abordés dans ce paragraphe peut entrainer une paralysie complète ou partielle de l'entreprise engendrant ainsi des difficultés d'approvisionnement en chaleur pour le pays et sa population.

En se basant sur diverses analyses de vulnérabilité des TIC et autres documents techniques[9], la présente norme formule des recommandations pour optimiser le niveau de sécurité des technologies de l'information et de la communication de tous les acteurs du secteur des réseaux thermiques. L'objectif est d'atteindre un niveau de protection acceptable évitant aux organisations d'être complètement démunies face à une défaillance de ses systèmes TIC. Elles sont donc encouragées à implémenter la norme minimale TIC en tenant compte des activités critiques identifiées au chapitre 2, à définir le niveau de maturité de ses systèmes TIC grâce à l'outil d'auto-évaluation disponible au chapitre 5 et à améliorer la sécurité des systèmes TIC jugée insuffisante après l'évaluation.

[7] Stratégie nationale de protection de la Suisse contre les cyberrisques. Unité de pilotage informatique de la Confédération (UPIC), Bern 2018.

[8] Il s'agit principalement de :

- *Guide Chauffage à distance / froid à distance. Association suisse du chauffage à distance, Bern 2020.*
- *Fiche d'information Réseaux thermiques. Suisse Energie, Office fédéral de l'énergie OFEN, Ittigen 2021*

[9] Les quatre documents suivants ont notamment servi de base à la présente norme minimale TIC :

- *Norme minimale TIC de l'approvisionnement économique du pays. Office fédéral pour l'approvisionnement du pays, Bern 2018.*
- *Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology (NIST), USA 2014.*
- *Recommended Practice : Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies. Department of Homeland Security (DHS) and Industrial Control Systems Cyber Emergency Response Team (NCCIC), USA 2016.*
- *Plus de sécurité pour les systèmes informatiques des petites et moyennes entreprises (PME). Information Security Society Switzerland (ISSS), Bern 2016.*

La loi sur l'approvisionnement du pays (LAP ; RS 531) confère au Conseil fédéral la compétence de mettre en œuvre des mesures préventives pour favoriser la résilience des processus d'approvisionnement vitaux pour notre pays. La norme minimale TIC constitue une mesure de résilience que le secteur concerné est libre d'adopter ou non. Réseaux Thermiques Suisse (RETS) – auparavant l'Association suisse du chauffage à distance (ASCAD) – ainsi que la société suisse de l'industrie du gaz et des eaux (SSIGE) recommandent, à l'ensemble de leurs membres, d'implémenter la norme minimale TIC pour l'approvisionnement des réseaux thermiques, dans son intégralité.

1.2 Situation initiale et objectifs

Pour le secteur des réseaux thermiques, comme pour la grande majorité des domaines industriels, la dépendance vis-à-vis des systèmes TIC est avérée. La numérisation croissante permet de gagner en efficacité mais complexifie le processus d'approvisionnement. La défaillance des systèmes TIC critiques peut donc avoir des répercussions considérables sur le bon fonctionnement des réseaux thermiques suisses et par conséquence impacter directement l'approvisionnement en chaleur du pays.

La présente norme émanant de l'OFAE, de RETS et de la SSIGE adopte le programme de cybersécurité du *NIST Framework Core*. Ce dernier repose sur deux concepts combinés basés sur la gestion des risques et sur la stratégie de *defense-in-depth*. L'analyse du risque acceptable est primordiale pour une organisation car cela lui permet d'adapter les mesures du *NIST Framework Core* à ses propres besoins (selon son secteur, sa taille, ses ressources et ses menaces). Quant à la stratégie *defense-in-depth*, il s'agit d'une approche dérivée du principe militaire qui veut qu'un système de défense multicouche complexe est plus difficile à franchir qu'une simple barrière. L'objectif de cette stratégie est donc d'appliquer plusieurs mesures de sécurité sur différents niveaux de protection (allant, par exemple, de la protection du réseau à la protection des éléments physiques en passant par la formation des collaborateurs) obligeant ainsi le potentiel attaquant à franchir une multitude d'obstacles de sécurité complexes.

L'objectif de ce programme de cybersécurité est d'améliorer la résilience des organisations du secteur des réseaux thermiques face aux risques TIC et, à terme, d'augmenter la sécurité globale de ce secteur afin que son processus approvisionnement puisse être assuré. Dans ce contexte, les menaces liées aux TIC sont comprises de manière globale : elles vont des dégâts physiques aux cyberattaques à visée destructrice, en passant par la perte ou la manipulation de données. Outre les mesures techniques, la norme minimale TIC englobe aussi la formation des collaborateurs et la gouvernance afin d'améliorer la résilience des systèmes TIC importants. Il est recommandé d'adopter une approche à plusieurs niveaux pour assurer la disponibilité, l'intégrité et la confidentialité des informations :

- **Disponibilité :** Garantir la disponibilité des informations lorsque c'est nécessaire. Cela suppose que les systèmes de traitement et de transmission soient opérationnels et disponibles.
- **Intégrité :** Faire en sorte que les informations soient en tout temps complètes et exactes.
- **Confidentialité :** Garantir que les informations sont accessibles uniquement aux personnes ou aux systèmes autorisés.

1.3 Champ d'application et délimitations

La présente norme minimale TIC se concentre sur la protection des systèmes TIC nécessaires au bon fonctionnement des réseaux thermiques suisses afin d'éviter que leurs dysfonctionnements n'impactent trop fortement le processus d'approvisionnement des réseaux thermiques ainsi que l'approvisionnement en chaleur de la Suisse. La portée de ce document est définie comme suit :

Champ d'application

- La présente norme englobe toutes les technologies de l'information et de la communication nécessaires à l'exploitation des systèmes et de l'infrastructure des réseaux thermiques (par ex : centrales d'énergie, gazoduc, sous-stations, etc.).
- La résilience des systèmes doit être améliorée au sein de tout le secteur. L'objectif du niveau minimal de protection doit permettre de limiter les effets d'un cyberincident sur le processus d'approvisionnement des réseaux thermiques ainsi que sur l'approvisionnement en chaleur du pays.

- La présente norme se concentre sur les systèmes de contrôle industriel (ICS), les logiciels de gestion intégrée (ERP)[10], les outils de communication ainsi que sur tous les systèmes TIC qui permettent de contrôler des installations. Cela comprend notamment : les ordinateurs portables et fixes, les téléphones, les logiciels de maintenance, les interfaces SCADA[11], les imprimantes, le *Smart Metering,* les appareils connectés *(Internet of Things)* ou encore les réseaux et systèmes installés dans les entreprises.
- Cette norme s'adresse à toutes les entreprises suisses travaillant dans le secteur des réseaux thermiques. Chaque organisation a la possibilité, selon ses ressources disponibles, de faire implémenter ce document en interne par ses collabora teurs ou en externe par un cabinet de consulting spécialisé.

Délimitation

- Le cas où une entreprise peut aussi faire fonctionner ses infrastructures sans systèmes TIC, soit en mode manuel, n'a pas été abordé. Cependant, il est recommandé de sauvegarder ou de (ré)introduire cette possibilité si les conditions s'y prêtent. Pour les infrastructures critiques, le mode manuel est capital a minima, la déconnexion en bon ordre des infrastructures devrait toujours être possible.
- Cette norme minimale TIC ne concerne pas l'approvisionnement en électricité. Il est néanmoins recommandé de prévoir, pour chaque infrastructure, un plan d'urgence afin d'affronter une pénurie ou une panne généralisée. La dépendance vis-à-vis de la fourniture d'électricité est importante. Sans électricité, les systèmes TIC et les activités qui en dépendent (ex : gestion des unités de production de la chaleur, contrôle du niveau de pression ou de température, fonctionnement du système d'alarme, etc.) ne pourraient être exécutés que manuellement, nécessitant une capacité humaine importante dans le cas où l'activité en question peut s'effectuer sans système TIC.
- Ce document se concentre uniquement sur le secteur des réseaux thermiques. Cependant, les entreprises de ce secteur ayant recourt au processus industriel de rejet de chaleur, ne produisent pas elles-mêmes la chaleur. De ce fait, une relation de dépendance se crée entre l'entreprise qui effectue l'activité productrice de chaleur et celle responsable des réseaux thermiques qui la récupère. Il est donc nécessaire de protéger la totalité du processus d'approvisionnement et pas uniquement la partie « réseau thermique ». Afin de protéger convenablement l'ensemble du processus, il est recommandé de se référer aux documents spécifiques des différents secteurs comme par exemple la norme minimale TIC pour la traitement des déchets[12] si les rejets de chaleur sont produits par une usine de valorisation thermique et électrique des déchets (UVTED). De plus amples informations sur les rejets de chaleur sont disponibles au chapitre 2.4.5.8.
- La présente recommandation ne comporte pas de mesures concernant la sécurité au travail.

1.4 Nécessité d'avoir une norme minimale pour les TIC

Bien que l'évolution du monde numérique permette l'amélioration des systèmes TIC, les cybermenaces se développent aussi et pèsent de plus en plus sur toutes les organisations. Les cyberattaques n'ont rien à voir avec la taille ou l'importance de l'entreprise et résultent souvent d'un concours de circonstances ou d'un effet d'aubaine. Ces situations se multiplient avec la généralisation de la numérisation.

Les entreprises responsables des réseaux thermiques sont nombreuses à ne pas isoler correctement leur système de contrôle industriel (ICS) du reste de l'activité ce qui entraîne de nouvelles vulnérabilités. Ces failles peuvent, par exemple, être exploitées par des pirates informatiques pour voler des données, utiliser des ressources TIC externes voire prendre le contrôle d'infrastructures industrielles. En cas d'attaque de *ransomware,* par exemple, une partie ou la totalité des systèmes TIC d'une organisation peuvent être cryptés. Il n'est alors plus possible d'accéder aux données à moins de payer la rançon demandée ou de relancer les installations grâce à des sauvegardes *(backup)* saines. Ces attaques peuvent donc entrainer d'importants dégâts autant financiers qu'industriels et en fonction de l'importance de l'organisation ou du secteur, cela peut impacter l'approvisionnement du pays. Il est donc essentiel de protéger les infrastructures dites critiques pour un pays.

[10] Enterprise-Resource-Planning-System : le système ERP est une application complexe voire une multitude de systèmes informatiques ou de logiciels d'application en interaction, aidant à planifier les ressources dans toute l'entreprise.

[11] SCADA : Supervisory Control And Data Acquisition (système de contrôle et d'acquisition de données).

[12] Norme minimale pour garantir la sécurité des technologies de l'information et de la communication (TIC) dans les usines de traitement des déchets. Association suisse des exploitants d'installations de traitement des déchets (ASED), Office fédéral pour l'approvisionnement économique du pays (OFAE), Suisse 2022.

Tous les domaines ainsi que tous les pays peuvent être touchés par des cyberattaques. Dans le secteur des réseaux thermiques et plus globalement de l'énergie, il existe plusieurs exemples d'entreprises qui ont dû affronter des cybermenaces. En 2016, une attaque DDOS *(Distributed Denial of Service)*[13] contre la société finlandaise Valtia en charge de réseaux thermiques, a rendu inaccessible les systèmes TIC de deux de ses immeubles privant ainsi les habitants de chauffage et d'eau chaude pendant plusieurs jours. Heureusement, cette attaque ne s'est pas produite lors du rude hiver finlandais évitant ainsi aux personnes affectées de risquer leur vie à cause des bases températures. Bien qu'il s'agit d'un incident mineur qui a touché uniquement deux bâtiments, il est facile d'imaginer les conséquences à grande échelle d'une telle situation pouvant priver de chaleur des quartiers ou de villes entières lors des grands froids.[14]

Un autre exemple qui met, cette fois, en avant une cyberattaque de grande envergure est celle subie par l'entreprise Colonial Pipeline en mai 2021. Il s'agit d'un oléoduc d'environ 8'900 km reliant Houston à New York. Les systèmes TIC de l'entreprise ont été infectés par une *ransomware* l'obligeant à suspendre momentanément son activité. Selon les indications, les responsables de Colonial Pipeline auraient payé 5 millions de dollars de rançon pour récupérer leurs données et la gestion de leurs installations. En plus de la rançon et du vol de données, l'oléoduc a interrompu son service pendant 5 jours ce qui a accentué la perte financière pour l'entreprise. De plus, cela a aussi eu des répercussions sur l'approvisionnement de plusieurs régions américaines engendrant une forte hausse des prix et une raréfaction des hydrocarbures. Le président américain Biden a même dû rassurer les citoyens du sud-est du pays car un début de crise était en train d'émerger. En effet, la population commençait à paniquer en voyant une grande partie des stations-services fermées pour cause de rupture de stock. Cela démontre bien comment un dysfonctionnement des systèmes TIC d'infrastructures critiques impacte l'approvisionnement d'un pays ainsi que sa population pouvant même dans les cas les plus importants créer une situation de panique.[15]

Les cyberattaques qui ont lieu dans les secteurs industriels sont toujours délicates car il est important qu'un *hacker* ne puisse pas prendre le contrôle des systèmes opérationnels liés à la réalisation des tâches industrielles de l'entreprise. En 2021, une entreprise de traitement des eaux basée en Floride a été victime d'une manipulation de son système de contrôle industriel (ICS). Les pirates informatiques ont réussi à en prendre le contrôle et étaient en train de multiplier par 100 la teneur en hydroxyde de sodium rendant ainsi l'eau impropre à la consommation et dangereuse pour la santé. L'attaque a été découverte par hasard lorsqu'un employé qui surveillait les moniteurs a remarqué que le curseur de la souris se déplaçait seul et modifiait des paramètres. Il a donc pu réagir rapidement et bloquer l'action malveillante évitant ainsi une pollution de l'approvisionnement en eau et une intoxication de la population.[16]

La Suisse ne fait pas exception à la règle et plusieurs entreprises ont aussi subi des cyberattaques. Pour citer quelques-uns des cas les plus connus, il y l'attaque DDoS contre l'usine d'eau potable d'Ebikon qui a échoué grâce à l'amélioration de son niveau de cybersécurité effectuée quelques mois auparavant.[17] L'entreprise Meyer Tobler a perdu l'accès à ses systèmes TIC permettant sa gestion administrative ce qui l'a complétement paralysé pendant plusieurs jours engendrant une perte de plusieurs millions de francs.[18] Ou encore le cas Ruag qui a subi pendant plusieurs mois du cyber-espionnage se faisant ainsi

[13] Il s'agit d'une attaque qui submerge les systèmes TIC d'une entreprise en les sollicitant avec un énorme volume de requêtes jusqu'à ce qu'ils ne puissent plus les traiter et deviennent inaccessibles.

[14] Forbes. « Hackers Use DDoS Attack to Cut Heat to Apartments », 7 novembre 2016. https://www.forbes.com/sites/leemathews/2016/11/07/ddos-attack-leaves-finnish-apartments-without-heat/?sh=2c8083c41a09 [consulté le 13.12.21].

[15] BBC. « US fuel pipeline 'paid hackers $5m in ransom », 14 mai 2021. https://www.bbc.com/news/business-57112371 [consulté le 13.12.21].

[16] Zerowaterloss. « D'autres attaques en Suisse – les producteurs d'eau potable investissent dans les systèmes de sécurité », 24 mars 2021. Hacker-Attacke auf Wasserversorgung in Ebikon LU – Blick [consulté le 04.01.22].

[17] Blick. « Hacker-Attacke auf Wasserversorgung in Ebikon LU », 19 décembre 2018. Hacker-Attacke auf Wasserversorgung in Ebikon LU – Blick [consulté le 04.01.22]

[18] ICTjournal. « La cyberattaque coûte des millions au suisse Meier Tobler », 21 mars 2019. La cyberattaque coûte des millions au suisse Meier Tobler | ICTjournal [consulté le 04.01.22]

dérober un quantité importante de données sensibles.[19] De plus, depuis la crise liée au Coronavirus, la situation dans le monde entier s'est détériorée. En Suisse, le nombre de cyberattaques a augmenté de manière significative. Le Centre national de cybersécurité (NCSC) a reçu deux fois plus de signalements de cyberattaque pour le premier semestre 2021 que pour la même période de l'année précédente.[20] Tous les types de cyberattaques ont suivi cette tendance. Selon les chiffres du NCSC[21], les principales menaces de 2021 ont été :

- *Phishing* : les victimes sont amenées à divulguer leurs mots de passe et d'autres informations personnelles,
- *Fake Sextorsion* : un maître chanteur menace de divulguer des photos ou d'autres informations compromettantes,
- *CEO-Fraud* : un ordre de paiement urgent mais factice est transmis par un pirate informatique se faisant passer pour membre de la direction qui souvent est injoignable à ce moment,
- *Ransomware* : les données sont cryptées et inaccessibles pour son propriétaire.

Ces exemples démontent que de telles menaces sont bel et bien réelles. Afin de limiter au maximum ces risques, les systèmes TIC requis pour la gestion des réseaux thermiques doivent présenter un niveau de sécurité élevé. L'instauration d'une procédure normalisée en matière de cybersécurité permet aux entreprises d'optimiser la protection de leurs systèmes TIC et d'améliorer leur protection en continu. La présente norme fournit des instructions pratiques pour mettre en œuvre ce programme de cybersécurité. Les entreprises en charges des réseaux thermiques sont encouragées, à l'aide de la norme minimale TIC, à identifier les risques auxquels elles sont exposées ainsi qu'à évaluer leur propension au risque. Elles peuvent adapter la présente norme en fonction de leur taille, de leurs ressources et des menaces auxquelles elles sont confrontées. C'est en fonction de ces considérations qu'elles seront en mesures d'estimer ce que leur coûtera la mise en œuvre de ce programme de cybersécurité. En finalité, c'est aux entreprises du secteur des réseaux thermiques d'assumer leurs responsabilités quant à la sécurité de fonctionnement de leurs installations.

1.5 Mise en œuvre de la norme minimale

Cette norme minimale TIC a pour vocation de couvrir le secteur des réseaux thermiques suisses. RETS et la SSIGE recommandent à l'ensemble de leurs membres d'implémenter cette norme minimale TIC dans son intégralité. Ils sont tenus de déterminer leur degré de maturité avec l'outil d'évaluation et de l'améliorer en continu. Les entreprises responsables d'importants réseaux thermiques sont encouragées à viser un niveau de sécurité supérieur au minimum recommandé.

Le présent document sert de guide et d'aide à la mise en œuvre. Le niveau minimum est considéré comme atteint si la notation globale de la maturité en matière de cybersécurité (cf. outil d'évaluation au chapitre 5) correspond au moins aux valeurs minimales prescrites (conformément à leur propre approche basée sur les risques). La cybersécurité n'est pas considérée ni abordée comme un état, mais comme un processus, et doit être dynamique. La sécurité des systèmes TIC n'est jamais acquise. Elle constitue un objectif permanent qui doit faire l'objet de contrôles réguliers et d'un processus d'amélioration continue. Ceux-ci doivent reposer sur la norme minimale TIC.

[19] Le Temps. «La cyberattaque de RUAG a réveillé la Suisse», Artikel in der Ausgabe vom 15. Januar 2017 (Stand: 4.1.2022).

[20] RTS. «Le nombre de cyberattaques a doublé au premier semestre en Suisse», Artikel publiziert auf der Website rts.ch am 2. November 2021 (Stand: 4.1.2022).

[21] Rapport semestriel 2021/1 (de janvier à juin). Centre national pour la cybersécurité NCSC, Bern 2021.

L'outil d'évaluation reprend pour l'essentiel les exigences du *NIST Framework Core*. Il permet une auto-évaluation à partir de 5 fonctions (identifier, protéger, détecter, réagir et récupérer). Ces fonctions sont ensuite réparties en 23 catégories, elles-mêmes subdivisées en 106 activités (voir Figure 1). Avant de commencer à utiliser l'outil d'évaluation, les fonctions et les catégories du cadre de cybersécurité peuvent être priorisées en fonction de la propension au risque de l'organisation. À cet effet, conformément à l'approche basée sur les risques, une note (entre 0 et 4)[22] est attribuée à chacune des 5 fonctions et 23 catégories. Les entreprises des réseaux thermiques déterminent quelles sont les fonctions et les catégories qui revêtent une importance particulière pour leur organisation (priorité élevée), et celles qui sont moins pertinentes en s'aidant des activités critiques définies au chapitre 2.4.

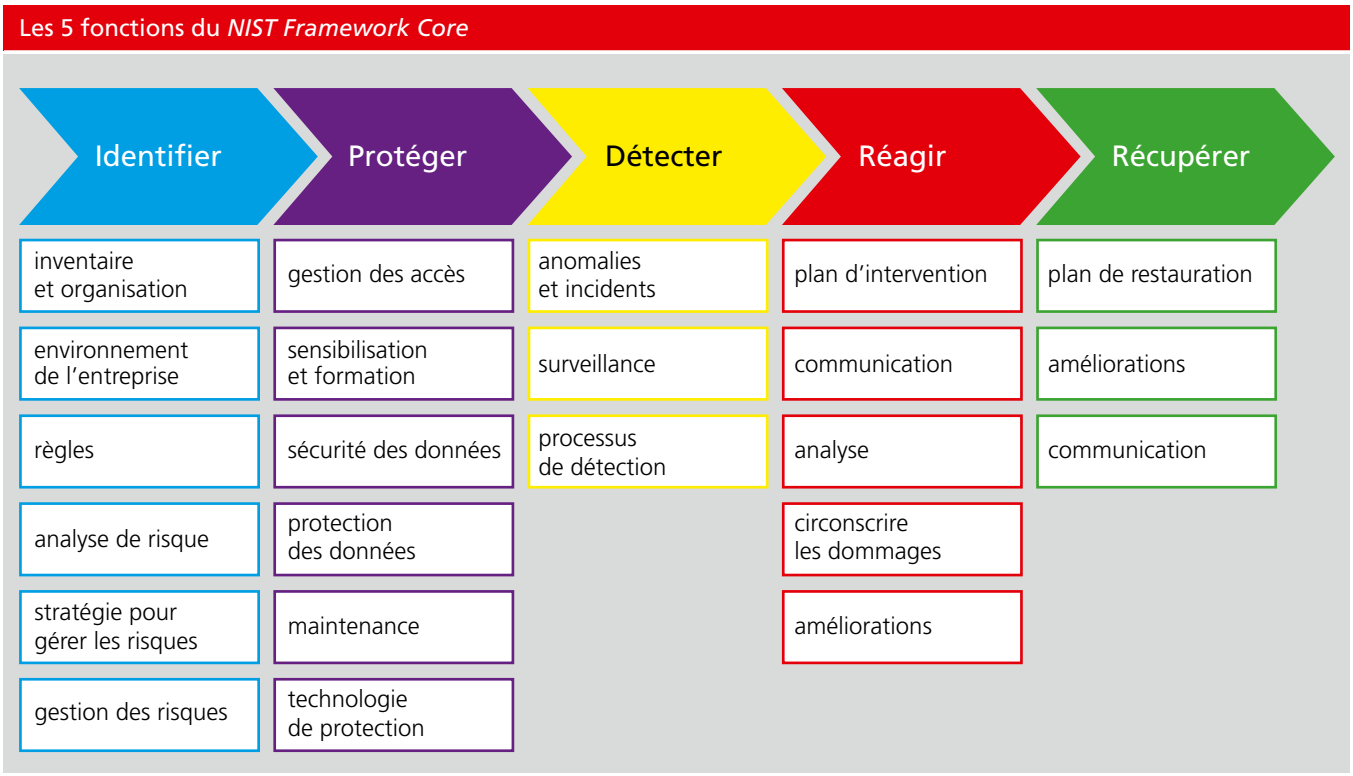

Figure 1: Fonctions et catégories du NIST Framework Core

[22] *Plus d'informations dans le chapitre 5 « Les mesures du NIST Framework Core »*

2 Présentation générale du secteur des réseaux thermiques

Ce chapitre consacré au secteur des réseaux thermiques, permet d'identifier la structure du marché, les processus d'approvisionnement ainsi que les activités critiques spécifiques à ce domaine. Le but étant d'adapter de manière optimale la norme minimale TIC à ce secteur offrant ainsi l'opportunité aux entreprises de prioriser certaines mesures du programme de cybersécurité selon les ressources disponibles, les besoins identifiés et les menaces encourues.

2.1 Définition d'un réseau thermique

Avant de rentrer dans le vif du sujet, il est important de définir ce qu'est un réseau thermique. Pour ce faire, il convient d'expliquer son fonctionnement, de dresser son contexte et son évolution possible par rapport aux besoins en chaleur de la Suisse ainsi que de mettre en avant les multiples sources d'énergies et processus industriels associés qui sont utilisés au sein de ce secteur.

2.1.1 Principe et contexte suisse

Les réseaux thermiques permettent de transporter à distance du chaud ou du froid. Dans le cas d'un réseau de chauffage à distance, une ou plusieurs centrales thermiques fournissent de la chaleur au fluide caloporteur (principalement de l'eau). Cette dernière est alors transmise au réseau afin d'être acheminée jusqu'à son lieu de consommation permettant principalement de chauffer un bâtiment. Il en va de même pour un réseau de froid à distance à l'exception que l'activité industrielle produit du froid et non du chaud. En ce qui concerne la température du réseau, elle oscille entre 60° C et 170° C pour un réseau de chauffage à distance classique. En dessous de 60° C, il s'agit de réseaux de chaleur à basse température permettant par exemple de chauffer que de petites structures à des températures avoisinant les 30° C. Lorsque la température que fournit le réseau est inférieure à la température ambiante, il s'agit de réseau de froid à distance.[23]

Les réseaux thermiques modernes existent depuis plusieurs décennies notamment dans les milieux urbains. Presque toutes les grandes villes suisses possèdent un ou plusieurs réseaux thermiques. Ces derniers étaient à l'origine alimentés par les rejets de chaleurs des usines de valorisation thermique et électrique des déchets (UVTED). Par la suite, des chaudières à bois ainsi que des pompes à chaleurs (PAC) approvisionnées principalement par l'eau des rivières ou par des rejets de chaleur industriels à plus faible émission thermique, sont venues compléter la production. Dans le milieu rural, les réseaux thermiques étaient, à l'origine, prévus pour être alimentés par la biomasse disponible dans ces régions, le plus souvent sous forme de bois et de biogaz fermentable provenant notamment des stations d'épuration des eaux usées (STEP). Bien que la majorité des réseaux thermiques fonctionnent avec des énergies renouvelables, il n'est pas rare de voir des installations équipées de chaudières à gaz ou à mazout (pouvant représenter jusqu'à 20 % de la production selon les périodes). L'objectif principal de ces énergies fossiles est de couvrir les pics de consommation mais elles permettent aussi aux organisations de disposer de systèmes de production redondants en cas de dysfonctionnement des installations principales. Toujours dans une optique de sécurité, il est donc courant de voir plusieurs systèmes de production différents pour alimenter un réseau thermique.[23]

2.1.2 Introduction au contexte industriel : sources énergétiques, processus industriels et températures produites

Comme cela a déjà été implicitement énoncé, les réseaux thermiques peuvent être alimentés par plusieurs sources énergétiques. Ces dernières sont transformées par le biais de différents processus industriels en chaleur pouvant atteindre des températures diverses et donc des utilités spécifiques. La production de chaleur est donc, pour le secteur des réseaux thermiques, un concept particulièrement hétéroclite. Afin de clarifier cette situation, la Figure 2 illustre les différentes combinaisons de production de chaleur possibles.

[23] *Fiche d'information Réseaux thermiques. Suisse Energie, Office fédéral de l'énergie OFEN, Ittigen 2021.*

Sources énergétiques combinées avec leurs processus industriels ainsi que la température produite pour le réseau thermique

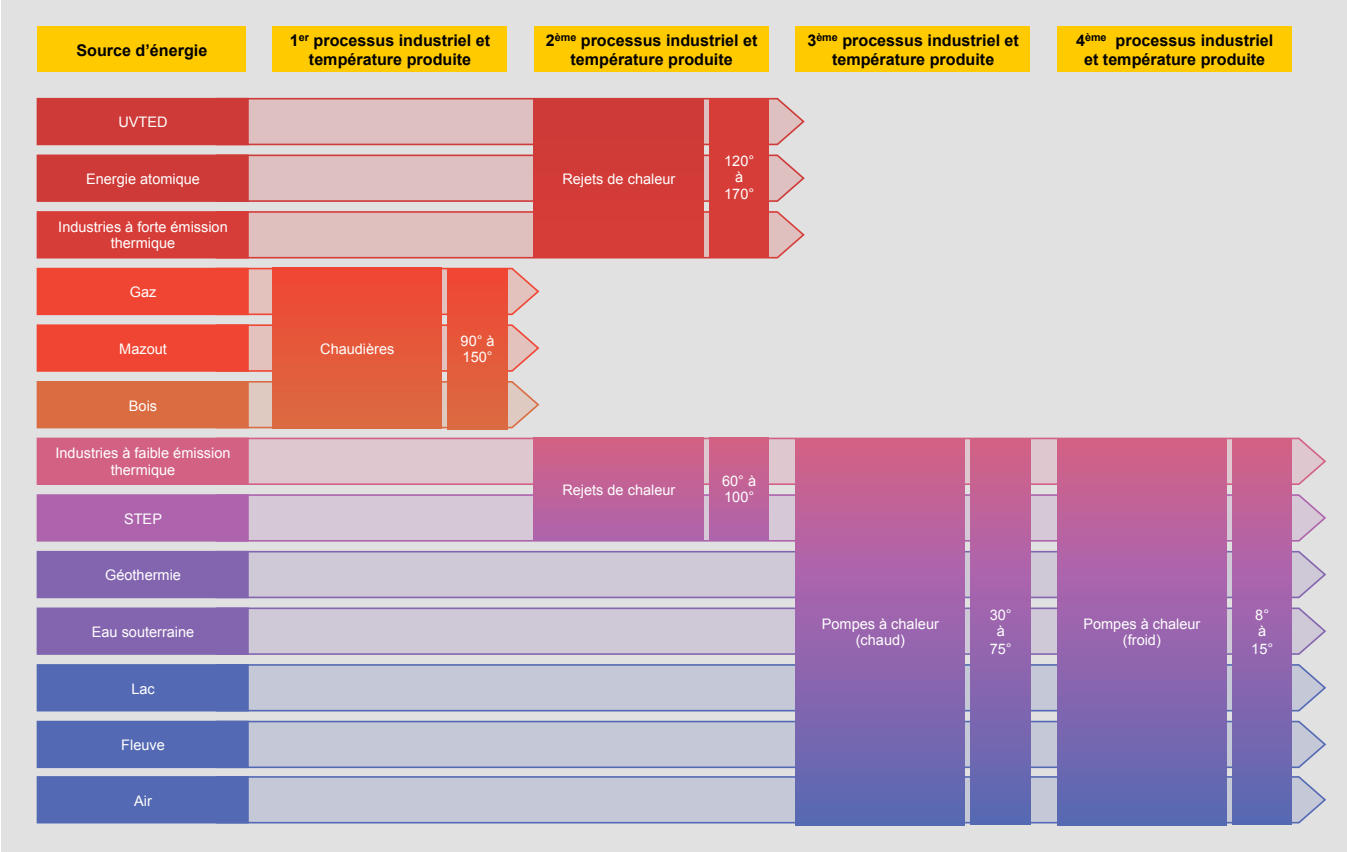

Figure 2 : Sources énergétiques, processus industriels et températures produites

Le premier processus industriel est exécuté par des « chaudières » qui peuvent fonctionner au bois, au mazout ou encore au gaz. Bien qu'il y ait une différence de température entre les trois sources énergétiques, il s'agit d'un processus dégageant une température élevée. Le deuxième processus industriel concerne les rejets de chaleur et permet d'obtenir différents niveaux de chaleur suivant l'activité industrielle qui produit la chaleur initiale. Il est possible d'atteindre des températures élevées par le biais d'activités industrielles à forte émission thermique telles que les UVTED et les centrales nucléaires mais aussi des températures plus modestes avec des activités industrielles à plus faible potentiel thermique comme les STEP. Le troisième processus industriel est effectué par des pompes à chaleur (PAC) et produit une chaleur limitée (le plus souvent ≤ 75° C). Les sources énergétiques alimentant les PAC proviennent des sols (géothermie et eau souterraine), des eaux (lac, fleuve, activités industrielles à faible émission de chaleur) ou de l'air. Le dernier processus industriel concerne le froid à distance produit par des pompes à chaleur (à froid) et obtenu selon les mêmes procédés que ceux mentionnés pour les pompes à chaleur produisant du chaud.

2.1.3 Perspectives d'évolution du secteur des réseaux thermiques

Ces dernières années, plusieurs engagements environnementaux ont été pris par la Suisse et ont fortement influencé l'avenir des réseaux thermiques. Il s'agit de l'Accord de Paris sur le climat de 2015 précisant qu'en 2030, les émissions de CO2 doivent avoir diminué de moitié par rapport à 1990, de la décision du Conseil Fédéral d'atteindre la neutralité carbone d'ici 2050 (projet zéro émission nette) et surtout de la stratégie énergétique 2050 qui est entrée en vigueur en 2018 et dont les trois objectifs principaux sont la réduction de la consommation d'énergie, l'amélioration de l'efficacité énergétique et la promotion des énergies renouvelables.[24]

Ces décisions politiques ont un impact sur l'évolution future des réseaux thermiques et pourraient en faire un acteur important de la transition énergétique suisse. Selon les projections des spécialistes[25], une augmentation significative de la production de chaleur provenant de ce secteur serait attendue. Conformément au rapport de l'OFEN intitulé « fiche d'information : réseaux thermiques »[26], la Suisse a consommé, en 2020, pour ses besoins en chaleur environ 100TWh/an dont 60 % provenaient encore des énergies fossiles. La part du chauffage à distance (réseau thermique) représentait approximativement 9 %. En se basant sur les engagements susmentionnés, l'OFEN estime que pour 2050, les besoins en chaleur du pays devraient avoisiner les 74 TWh/an et la part du chauffage à distance oscillerait entre les 14 % et 24 % selon les différentes hypothèses d'évolution. En plus d'augmenter les capacités de ce secteur, sa production devra se passer des énergies fossiles (gaz et mazout) ainsi que des énergies non-renouvelables (nucléaire) utilisées actuellement pour combler les pics de consommation ou comme réserve de sécurité en cas de panne des installations principales de production.

[24] Office fédéral de l'énergie. « Qu'est-ce que la Stratégie énergétique 2050 ». https://www.bfe.admin.ch/bfe/fr/home/politique/strategie-energetique-2050/qu-est-ce-que-la-strategie-energetique-2050.html [consulté le 10 janvier 2020].

[25] Guide Chauffage à distance / froid à distance. Association suisse du chauffage à distance, Bern 2020.

[26] Fiche d'information Réseaux thermiques. Suisse Energie, Office fédéral de l'énergie OFEN, Ittigen 2021.

Besoin en chaleur de la Suisse et proportion des réseaux thermiques en 2050

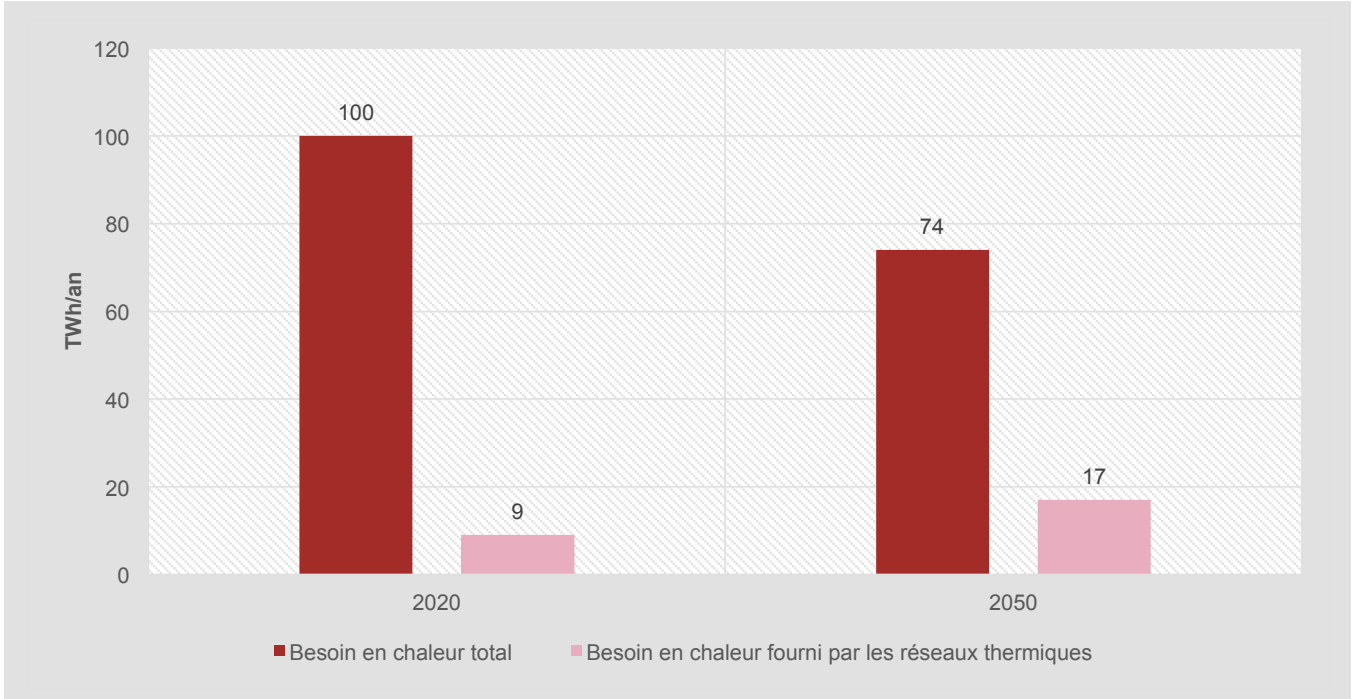

Figure 3 : Besoin en chaleur de la Suisse et capacité des réseaux thermiques pour 2020 et 2050

Estimation de l'évolution des sources d'énergies utilisées par les réseaux thermiques en 2020 et en 2050

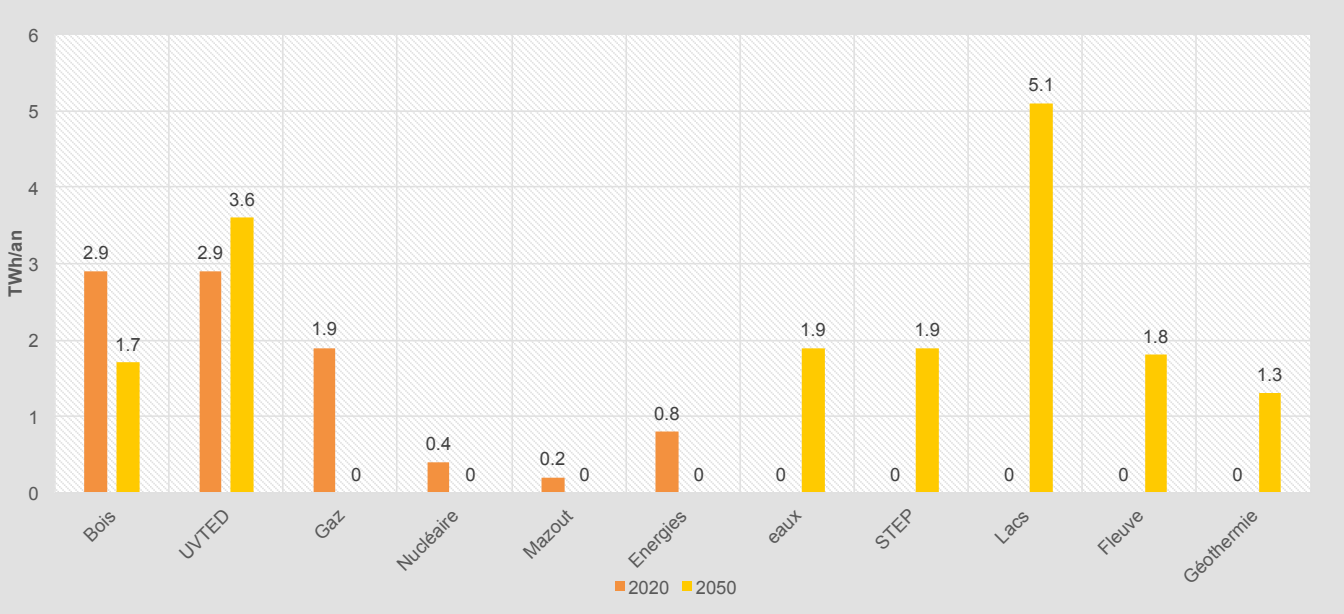

Figure 4 : Évolution des sources énergétiques pour 2050

Afin de mieux comprendre le futur développement des réseaux thermiques, il est nécessaire d'analyser plus en détail l'énergie produite par les différentes sources énergétiques. En se basant sur les chiffres de RETS provenant de son « rapport annuel 2021 »[27], il est possible d'estimer la répartition entre les différentes sources de chaleur. En prenant en compte les données d'Energie-Bois Suisse additionnées à celles de RETS, les réseaux thermiques ont vendu pour environ 9 TWh en 2020 dont 32,3 % de la production provient du bois, 31,8 % des usines de valorisation thermique et électrique des déchets (UVTED), 20,7 % du gaz naturel, 8,5 % des énergies renouvelables diverses, 4,6 % des centrales nucléaires et 2,1 % du mazout.

En ce qui concerne les projections pour 2050 basées exclusivement sur les énergies renouvelables comme le prévoit la stratégie énergétique 2050, RETS[28] estime que la part des réseaux thermiques passerait donc à 17.3 TWh (voir Figure 3) dont 29 % produits par les lacs, 21 % par les UVTED, 11 % pour les eaux souterraines, 11 % pour les STEP, 10 % par les fleuves, 10 % par le bois et 8 % pour la géothermie. La Figure 4 représente en TWh/an la production d'énergie produite par les différentes sources énergétiques. Elle illustre aussi la fin des énergies fossiles ainsi que le développement des énergies renouvelables notamment celles provenant des lacs. Selon les estimations de RETS, les lacs disposent d'un potentiel de développement très important, envisageant même qu'ils puissent devenir la source d'énergie principale des réseaux thermiques devant les UVTED qui reste une source essentielle d'énergie en augmentant aussi significativement.[29]

[27] *Rapport annuel 2021. Association suisse du chauffage à distance, Bern 2022.*

[28] *Livre blanc : le chauffage à distance en Suisse – Stratégie ASCAD. Association suisse du chauffage à distance, Eicher+Pauli SA, Bern 2014.*

[29] *Guide Chauffage à distance/froid à distance. Association suisse du chauffage à distance, Bern 2020.*

2.2 Acteurs des réseaux thermiques

Au sein de ce secteur, il existe plusieurs centaines d'acteurs aux profils particulièrement variés. Comme expliqué précédemment, les sources d'énergie ainsi que les processus industriels divergent fortement d'une installation à l'autre. Il en est de même pour la longueur des conduits thermiques ainsi que pour la quantité d'énergie produite. Afin d'illustrer cette hétérogénéité, il suffit de comparer l'une des plus grandes entreprises de ce secteur dont le réseau s'étend sur plus de 160 km et dont la production s'élève à environ 755'000 MWh/an, à une petite structure qui possède un réseau de 200m de long et qui produit 600 MWh/an.[30]

Malgré cette diversité, la composition du marché est plutôt simple. La plupart des acteurs du secteur sont représentés par les deux associations industrielles du domaine à savoir Réseaux Thermiques Suisse (RETS) et la société suisse de l'industrie du gaz et des eaux (SSIGE). La régulation et la surveillance sont effectuées par l'OFEN, comme pour la majorité des secteurs du domaine de l'énergie. Afin de disposer d'une vision représentative de ce secteur, l'OFEN et RETS ont élaboré une carte interactive recensant la quasi-totalité des réseaux thermiques du pays. La Figure 5 permet de représenter chaque acteur par un point de couleur correspondant à la source énergétique utilisée. Pour disposer des dernières mises à jour de cette carte et obtenir des informations détaillées sur l'ensemble des acteurs répertoriés, il est recommandé de se rendre sur le site Internet de RETS.[31]

Aperçu de la composition des réseaux thermiques suisses

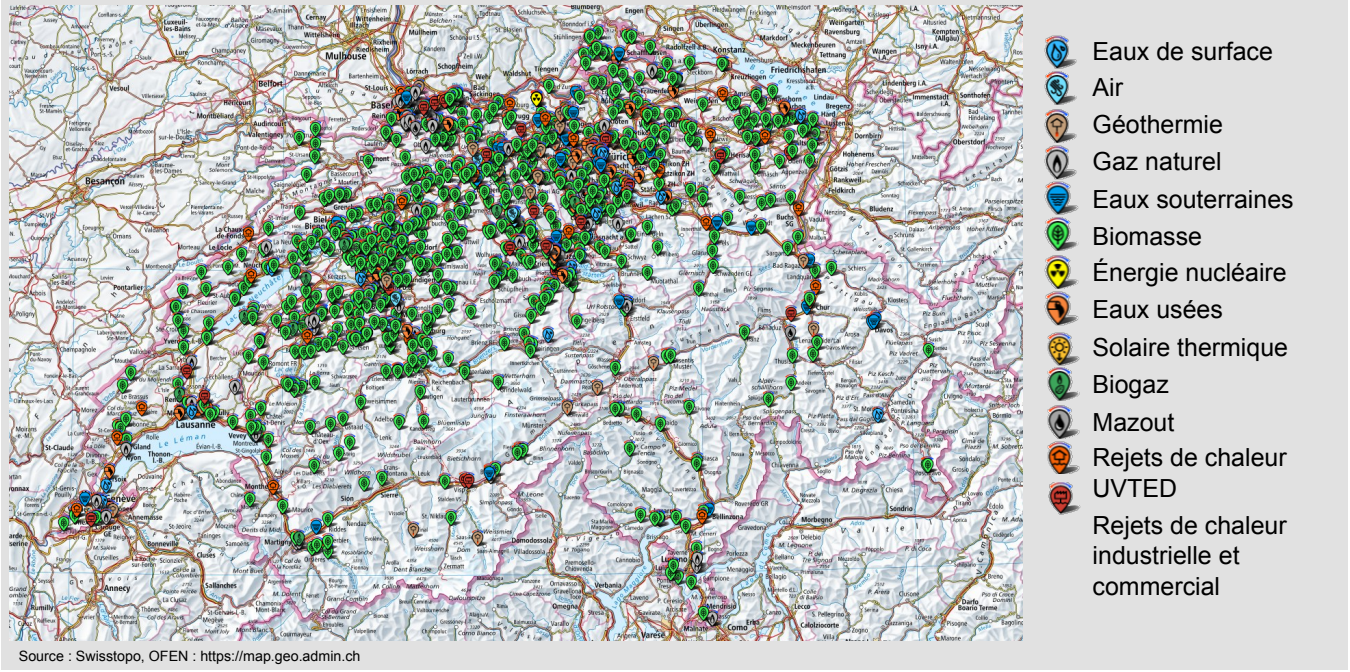

Figure 5 : Aperçu de la composition des réseaux thermiques suisses

[30] *Réseaux Thermiques Suisse. « Carte réseaux CAD ». Détails : ERZ Entsorgung Recycling Zürich et CAD Bevaix. https://s.geo.admin.ch/925f2fecea [consulté le 10 janvier 2022].*

[31] *Lien de la carte interactive de RETS : https://s.geo.admin.ch/925f2fecea*

2.3 Processus d'approvisionnement

Comme l'illustre la Figure 2, le processus d'approvisionnement des réseaux thermiques ne peut pas être identique pour l'ensemble du secteur car les sources énergétiques utilisées ainsi que les processus industriels de production de la chaleur diffèrent d'une infrastructure à l'autre. Afin de respecter cette diversité et selon les données récoltées, il a été possible de déterminer trois processus d'approvisionnement principaux. Chacun est divisé en quatre sous-processus comprenant les activités principales qui y sont effectuées.

2.3.1 Processus d'approvisionnement 1 : chaudière

Selon la Figure 6, le premier sous-processus « alimentation en matière première » répertorie les activités liées à la production, au transport et à l'achat des manières premières (bois[32], gaz[33] ou mazout[34]) qui sont nécessaires à l'alimentation de la chaudière. Les entreprises des réseaux thermiques sont dépendantes des fournisseurs de matières premières et n'ont pas réellement d'impact sur ces activités. Leur responsabilité commence une fois qu'elles ont accès aux combustibles. Le deuxième sous-processus concerne la production de chaleur ce qui comprend notamment le fonctionnement de la chaudière et l'ensemble des systèmes TIC permettant la gestion de ces tâches. La combustion

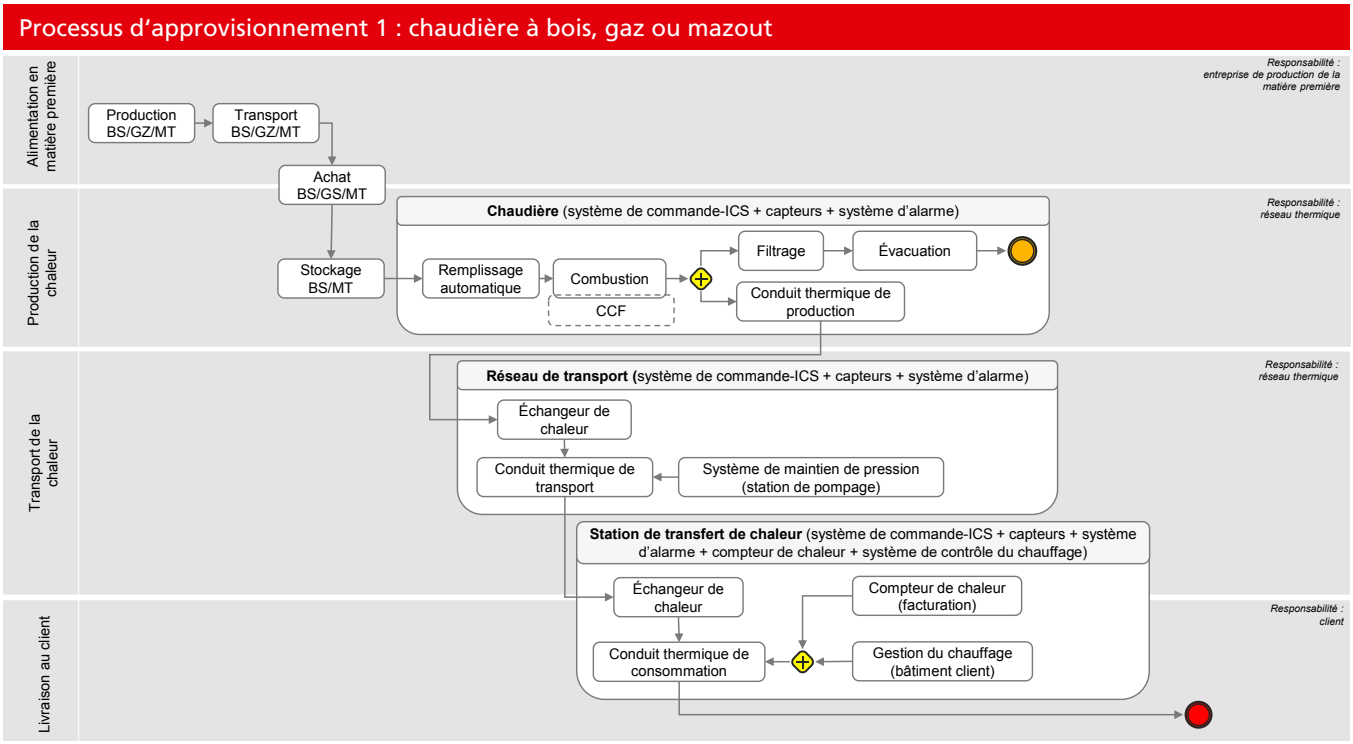

Figure 6 : Processus d'approvisionnement des chaudières

au sein de la chaudière crée une température élevée permettant d'une part de faire chauffer le fluide caloporteur (principalement de la vapeur ou de l'eau) présent dans les conduits thermiques de production et d'autre part de faire fonctionner une installation de cogénération (couplage chaleur-force) si cette dernière est présente au sein de l'infrastructure (plus de détails dans le sous-chapitre 2.3.4). Le troisième sous-processus se concentre sur le transport de la chaleur. L'échangeur permet de transmettre la chaleur des conduits thermiques de production aux conduits thermiques de transport afin qu'elle puisse être acheminée

[32] Energie-environnement.ch. « Le chauffage au bois ». https://www.energie-environnement.ch/maison/renovation-et-chauffage/installations/chauffage-au-bois, [consulté le 20.12.21].

[33] Energie-environnement.ch. « Le chauffage au Gaz naturel (non renouvelable) et au Biogaz (renouvelable) https://www.energie-environnement.ch/maison/renovation-et-chauffage/installations/chauffage-au-gaz, [consulté le 20.12.21].

[34] Energie-environnement.ch. « Le chauffage au Mazout ». https://www.energie-environnement.ch/maison/renovation-et-chauffage/installations/chauffage-au-mazout, [consulté le 20.12.21].

jusqu'aux échangeurs des clients. Les systèmes TIC permettent de commander à distance l'ensemble du réseau de transport incluant en plus les sous-stations chez les clientes et clients ainsi que les niveaux de pressions globaux afin de garantir un transport optimal au sein des conduites. Le dernier sous-processus renvoie à la livraison et à la consommation de la chaleur par le client. La responsabilité de l'organisation en charge du réseau thermique à distance s'arrête typiquement aux stations de transfère de chaleur des clients, mais il peut y avoir d'autres accords contractuels concernant certaines interfaces du processus. Dès ce moment, le client est en charge de son système de chauffage. Les systèmes TIC sont néanmoins encore présents afin de collecter les données liées à la consommation du client ainsi qu'à la facturation. De plus, le client a aussi la possibilité de régler ses besoins en chaleur à l'aide de l'unité de gestion du chauffage.

L'ensemble du processus d'approvisionnement est géré par le système de commande (ICS) qui permet de centraliser l'acquisition, la surveillance, le contrôle et le traitement des données provenant des capteurs disséminés sur l'ensemble de l'infrastructure. Il offre la possibilité de contrôler et de surveiller à distance toutes les activités qui y sont liées. Si le système de contrôle industriel s'aperçoit que les données examinées ne correspondent pas à l'intervalle de sureté prédéfini, il déclenche le système d'alarme qui va permettre de prévenir les responsables que le fonctionnement est altéré et qu'il est nécessaire de le corriger et de réagir.

Afin de facilité la lecture des Figure 6, Figure 7, Figure 8 et Figure 9, le parcours « retour » n'a pas été illustré. En effet, tous les conduits thermiques sont des circuits fermés. Le fluide caloporteur qui transmet la chaleur ne disparait pas du réseau une fois que la chaleur a été consommée mais il parcourt le chemin inverse jusqu'au prochain échangeur de chaleur afin d'être à nouveau chauffé.[35] Pour une meilleure lisibilité, toutes les figures des processus d'approvisionnement sont au format A4 dans les annexes de ce document.

2.3.2 Processus d'approvisionnement 2 : rejet de chaleur

Dans le cas des rejets de chaleur, l'entreprise en charge des réseaux thermiques ne produit pas elle-même la chaleur mais la récupère. En effet, une autre activité industrielle effectuée en amont comme par exemple l'incinération des déchets (UVTED)[36] ou la fission nucléaire permet de créer cette chaleur. Il y a donc une relation de dépendance entre le processus d'approvisionnement des réseaux thermiques et celui de l'activité productrice de chaleur. La structure organisationnelle entre ces deux activités n'est pas prédéfinie, il n'existe aucun standard. Il se peut qu'une seule entreprise soit responsable de l'activité principale et du réseau thermique ou alors que deux organisations se partagent distinctement les tâches ou encore que la délimitation entre les deux entreprises ne soit pas si évidente. Cette dépendance oblige l'entreprise qui a la charge des réseaux thermiques de prendre aussi en compte le processus d'approvisionnement élargi comprenant les tâches de l'activité productrice de chaleur et celles des rejets de chaleur. Il en va de même pour la protection des systèmes TIC qui peuvent suivant la structure organisationnelle, être communs ou encore complétement distincts. Dans le sous-chapitre 2.4.5.8 lié aux activités critiques, la dépendance des rejets de chaleur est traitée de manière plus approfondie afin de mettre en avant les éléments qui nécessitent une attention particulière.

[35] Energie-environnement.ch. « Chauffage à distance (CAD) et réseau de chaleur ». Chauffage à distance (CAD) – energie-environnement.ch, [consulté le 20.12.21

[36] Energie-environnement.ch. « Usine d'incinération ». https://www.energie-environnement.ch/dechets-recyclage/1430, [consulté le 20.12.21].

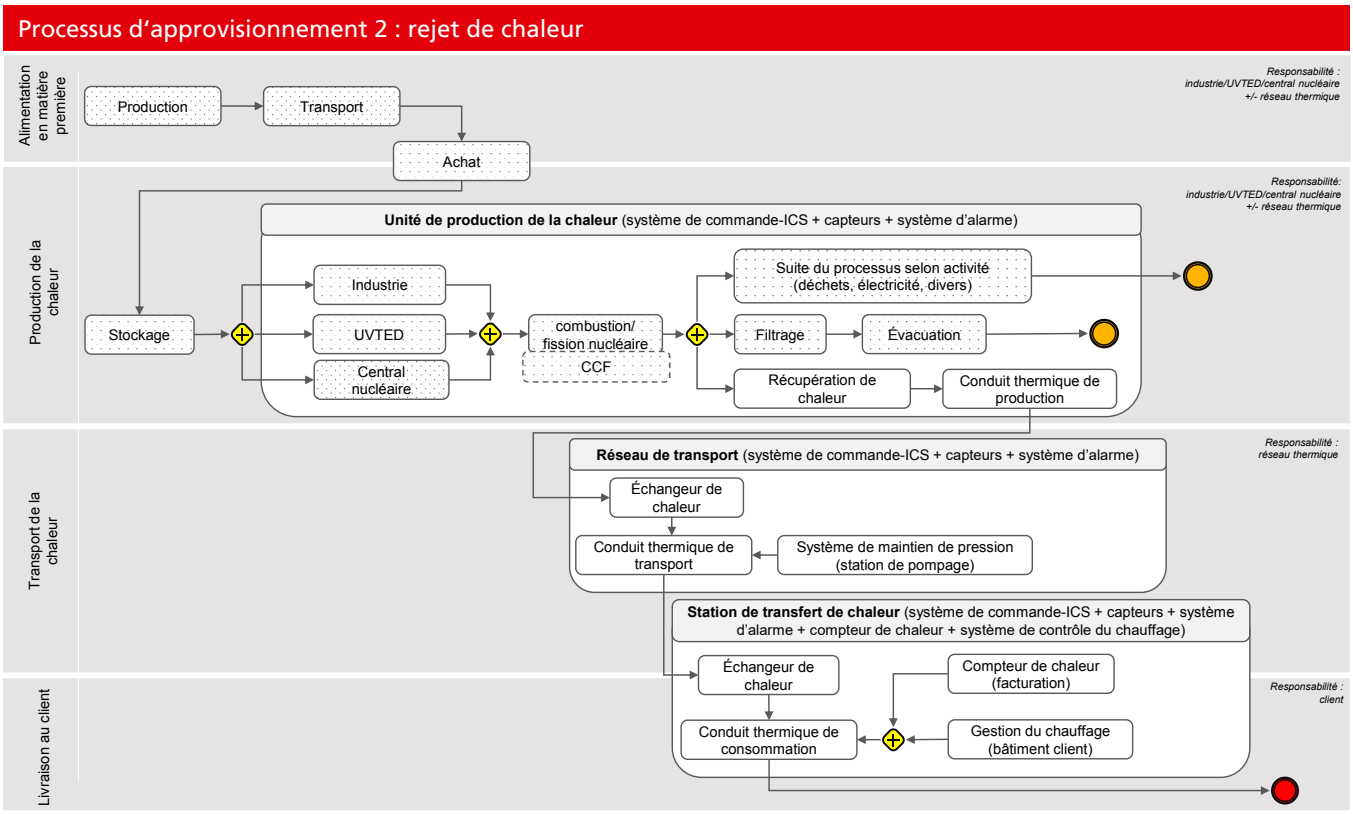

Figure 7 : Processus d'approvisionnement des rejets de chaleur

Cette dépendance vis-à-vis de l'activité productrice de chaleur est représentée, dans le processus d'approvisionnement des rejets de chaleur (Figure 7), par les activités dont le fond est pointillé. Il s'agit donc d'activités nécessaires pour la production de chaleur mais qui ne sont pas forcément (selon la structure organisationnelle) sous la responsabilité de l'organisation en charge des réseaux thermiques. La production de chaleur est alors effectuée par diverses unités de production dont principalement les usines de valorisation thermique et électrique des déchets (UVTED) mais aussi les centrales nucléaires ou d'autres industries à forte émission thermique. La suite du processus d'approvisionnement de l'activité principale n'est pas détaillée dans cette figure mais est représentée par l'activité « suite du processus selon activité » qui permet l'élimination des déchets, la production d'électricité ou encore d'autres finalités selon l'industrie. Quant à l'activité « récupération de chaleur », elle consiste à récupérer les rejets de chaleur afin de chauffer les conduits thermiques de production permettant ainsi d'approvisionner les réseaux thermiques. La suite du processus d'approvisionnement (transport de la chaleur et livraison aux clients) ainsi que l'utilisation des systèmes TIC sont exactement les mêmes que pour le processus d'approvisionnement des chaudières.[37]

[37] *Energie-environnement.ch. « Chauffage à distance (CAD) et réseau de chaleur ». Chauffage à distance (CAD) – energie-environnement.ch, [consulté le 20.12.21].*

2.3.3 Processus d'approvisionnement 3 : pompe à chaleur (PAC)

Dans le cas du processus d'approvisionnement des pompes à chaleur (PAC), l'entreprise en charge du réseau thermique est responsable dès le premier sous-processus permettant d'alimenter les PAC en matière première (Figure 8). Il existe trois différents types de PAC en fonction du milieu dans lequel la chaleur est puisée. Les PAC air-eau[38] qui à l'aide d'un compresseur aspirent l'air et sa chaleur, les PAC eau-eau[39] qui pompent de l'eau dans différents milieux (lacs, rivières, eaux souterraines mais aussi provenant des différentes installations comme par exemple les STEP) afin de lui prélever sa chaleur et les PAC sol-eau[40] qui grâce à des sondes géothermiques vont soutirer la chaleur du sol selon la profondeur du forage.

Une fois la chaleur captée, la pompe à chaleur va permettre de décupler cette chaleur par le biais d'un système qui comprime et détend (changement de phase) un gaz réfrigérant synthétique. De manière plus concrète, la source de chaleur primaire (air, sol ou eau) va transmettre sa chaleur au gaz réfrigérant dans l'évaporateur. Le gaz réfrigérant passe donc à l'état gazeux et avance jusqu'au compresseur qui va le comprimer. En augmentant la pression, cela va produire une réaction qui va considérablement élever la température du gaz. Il passe ensuite dans le condensateur pour qu'il puisse transmettre sa chaleur aux conduits thermiques de production. Le gaz continue jusqu'au détendeur qui va permettre de diminuer la pression pour que le gaz passe à l'état liquide et qu'il puisse récupérer de la chaleur au sein de l'évaporateur et recommencer son cycle. En ce qui concerne les ICS, ils participent aux bons fonctionnements des PAC. Le système de commande contrôle le fonctionnement de l'installation, s'assure que la pression des conduits soit optimale, récupère et traite les données des capteurs et déclenche le système d'alarme en cas d'irrégularité.

Contrairement au deux autres processus d'approvisionnement, les pompes à chaleurs produisent des températures moins élevées (le plus souvent ≤ 75° C). Cependant, les PAC ont la possibilité de produire du froid. Le principe est exactement le même que ce qui a été expliqué ci-dessus mais le fonctionnement est inversé et c'est le froid qui est injecté dans le réseau thermique.[41] Le reste du processus d'approvisionnement est identique aux deux autres précédemment développés.

[38] Energie-environnement.ch. « Pompe à chaleur (PAC) « air/eau », https://www.energie-environnement.ch/maison/renovation-et-chauffage/installations/pac-air-eau, [consulté le 19.01.2022].

[39] Energie-environnement.ch. « Pompe à chaleur (PAC) « eau/eau », https://www.energie-environnement.ch/maison/renovation-et-chauffage/installations/pac-eau-eau, [consulté le 19.01.2022].

[40] Energie-environnement.ch. « Géothermie et pompe à chaleur (PAC) « sol/eau »« , https://www.energie-environnement.ch/maison/renovation-et-chauffage/installations/geothermie-et-pac-sol-eau, [consulté le 19.01.2022].

[41] Energie-environnement.ch. « Généralités sur les pompes à chaleur (PAC) », https://www.energie-environnement.ch/maison/renovation-et-chauffage/installations/generalites-sur-les-pac, [consulté le 20.12.21].

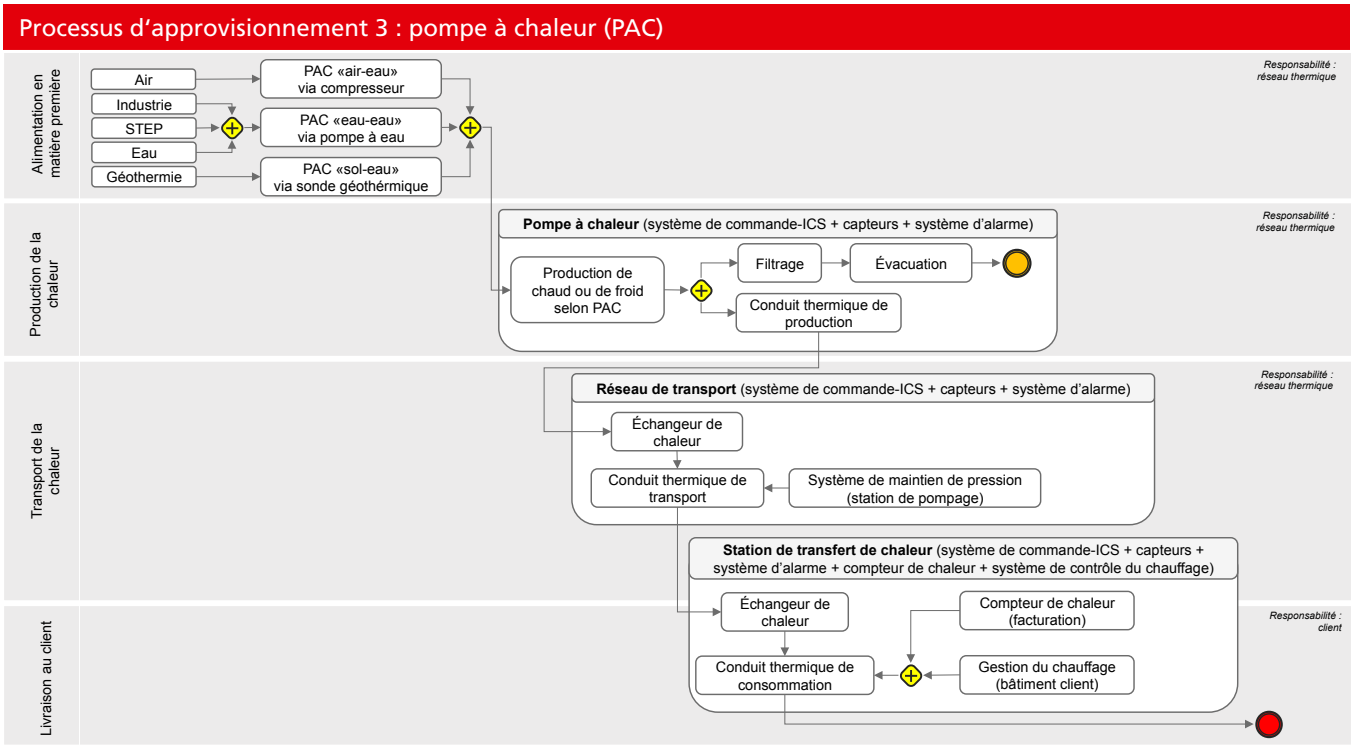

Figure 8 : Processus d'approvisionnement des pompes à chaleur

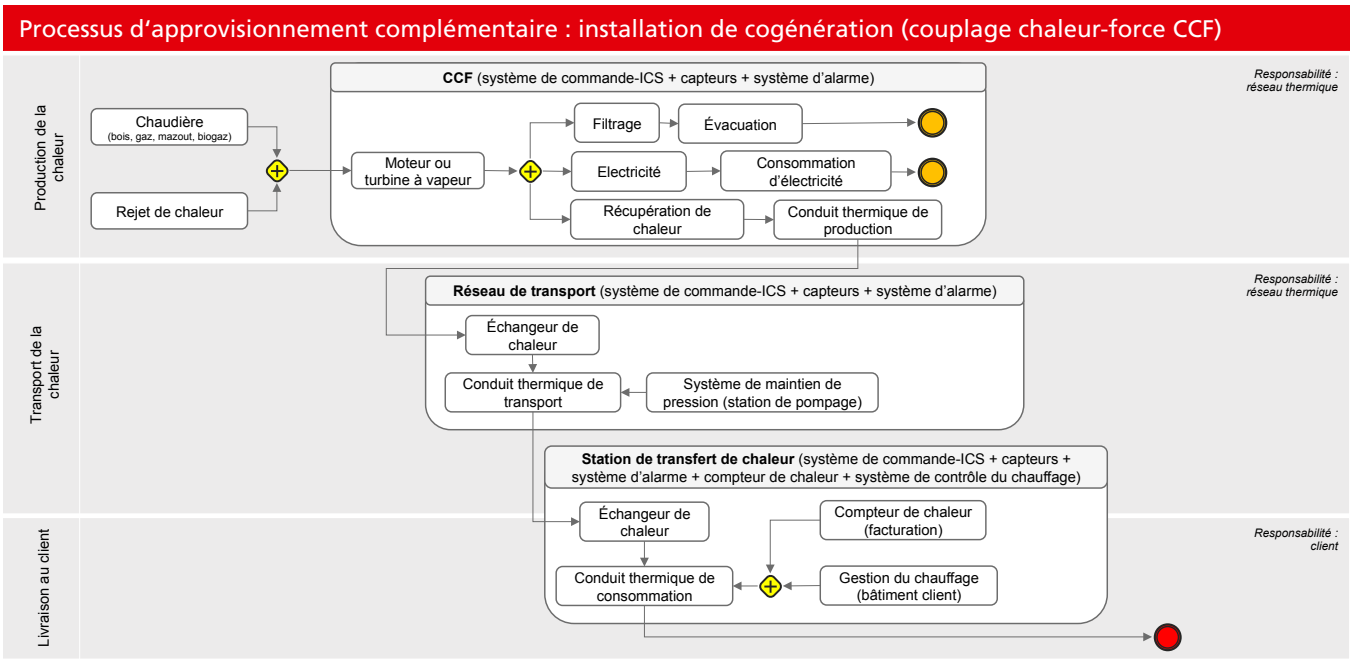

Figure 9 : Processus d'approvisionnement complémentaire sur le couplage chaleur-force

2.3.4 Processus d'approvisionnement complémentaire : installation de cogénération – couplage chaleur-force (CCF)

Une installation de couplage chaleur-force n'est pas réellement un processus industriel à part entière, il est plutôt combiné avec un moyen de production. Cependant, comme il est assez commun d'en trouver sur une infrastructure productrice de chaleur, il est tout de même pertinent de détailler son fonctionnement. Il s'agit donc d'un procédé complémentaire qui permet de créer simultanément de la chaleur et de l'électricité offrant ainsi une utilisation plus efficiente des installations thermiques. L'exemple classique d'une installation de couplage chaleur-force consiste à utiliser du gaz, du mazout, du bois ou du biogaz pour faire fonctionner un moteur à piston ou une turbine à vapeur. La combustion de ces éléments permet de créer de la chaleur afin de chauffer un circuit d'eau. Quant au mouvement du piston ou de la turbine, il est couplé à une génératrice qui va produire de l'électricité.[42]

Dans le cadre des réseaux thermiques, il s'agit d'une installation qui est présente dans les processus industriels des chaudières et des rejets de chaleur. La haute température produite ou récupérée par ces installations permet de créer de la vapeur. Cette dernière permet d'actionner une turbine reliée à une génératrice produisant ainsi de l'électricité et parallèlement de chauffer les conduits thermiques de production. Un exemple plus démonstratif d'une installation de cogénération est illustré au sous-chapitre 2.4.5.8 à l'aide de la Figure 12 démontrant par la même occasion les différentes combinaisons d'installations possibles afin de le rendre une infrastructure thermique plus efficiente (UVTED + CCF + STEP + réseaux thermiques).

Pour revenir sur le processus d'approvisionnement complémentaire du couplage chaleur-force, il est représenté par la Figure 9. Le sous-processus « alimentation en matière première » n'a pas été détaillé car il est identique à celui du processus industriel qu'il complète (chaudière et rejet de chaleur). En ce qui concerne la production de chaleur, il est intéressant de relever que ces installations sont souvent approvisionnées en biogaz provenant de la fermentation des boues d'épuration (STEP), des déchets organiques ou encore de déchets verts (domaine agricole)[43]. Mise à part la production d'électricité qui est propre à ce type d'installation, le reste du processus est identique aux autres processus d'approvisionnement dont il fait partie.

[42] *Energie-environnement.ch. « CCF – Couplage chaleur-force (ou cogénération », https://www.energie-environnement.ch/maison/renovation-et-chauffage/installations/couplage-chaleur-force-ccf, [consulté le 19.01.2022].*

[43] *Fiche d'information Réseaux thermiques. Suisse Energie, Office fédéral de l'énergie OFEN, Ittigen 2021.*

2.4 Activités critiques

L'objectif de ce chapitre 2 est d'implémenter la norme minimale TIC en se basant sur les spécificités d'un secteur. Pour ce faire, différentes thématiques allant du contexte actuel, aux acteurs du marché, en passant par les processus d'approvisionnement sont abordées et détaillées. La finalité de ce procédé est de pouvoir définir des activités dites critiques afin de sensibiliser les organisations de ce secteur sur leurs composants essentiels et leur permettre d'adapter la norme minimale TIC à leurs besoins. Cette démarche offre donc la possibilité de prioriser certaines mesures du programme de cybersécurité en tenant compte des ressources disponibles, du risque acceptable et des menaces encourues propres à chaque organisation de ce secteur.

2.4.1 Définition d'une activité critique

Pour qu'une activité soit considérée comme critique, elle doit remplir deux conditions : être dépendante des systèmes TIC et être indispensable au processus d'approvisionnement. Cependant, afin de garantir un niveau de sécurité suffisant, il a été nécessaire d'ajouter une troisième notion. En effet, il est possible que le dysfonctionnement TIC d'une activité n'empêche pas le bon déroulement du processus d'approvisionnement mais qu'elle soit quand même considérée comme critique pour des raisons de *safety.* Cette notion anglaise permet de faire la distinction entre la sécurité des systèmes TIC *(security)* et la protection des vies humaines *(safety).* Afin de garantir un niveau de sécurité globale, il a été décidé que toutes activités pouvant mettre en danger des vies humaines à la suite d'une panne TIC sont automatiquement considérées comme critique. De ce fait, pour qu'une activité TIC soit considérée comme critique, elle doit : 1) dépendre des systèmes TIC et 2) empêcher le bon fonctionnement du processus d'approvisionnement ou mettre en péril des vies humaines.

2.4.2 Pyramide d'automatisation

Pour une meilleur compréhension, les activités critiques ont aussi été combinées avec la pyramide de l'automatisation[44] qui représente de manière conceptuelle les différents niveaux des outils et des systèmes d'informatiques selon une hiérarchie fonctionnelle (voir Figure 10). Cette représentation permet donc de mieux cerner l'intégration des différentes technologies qui sont utilisées au sein d'un secteur industriel tout en tenant compte des concepts génériques de l'automatisation. La pyramide est divisée en cinq couches qui représentent chacune un type d'informations, de systèmes et de temporalité spécifiques.

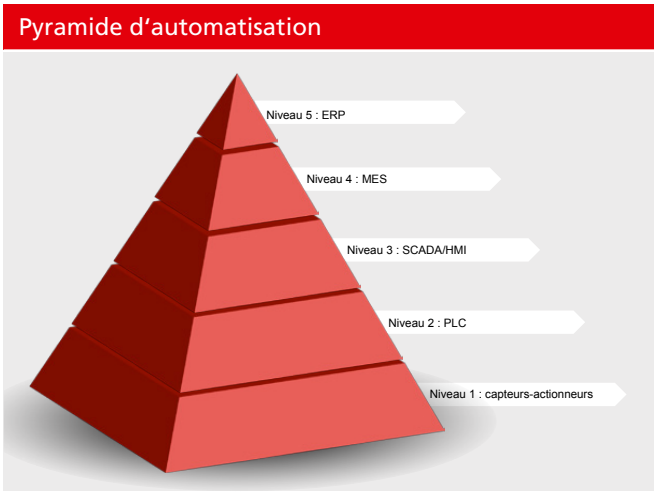

Figure 10 : Pyramide d'automatisation

- Niveau 1 : comprend l'ensemble des éléments physiques nécessaires au bon fonctionnement de l'activité industrielle. Il s'agit essentiellement des capteurs et des actionneurs (vérin, moteur, pompe, vanne, etc.) qui ont un impact direct sur le monde physique (matériel).

- Niveau 2 : est associé au contrôle. Les PLC[45] reçoivent les signaux des capteurs et commandent les actionneurs afin qu'ils effectuent physiquement leur travail.

- Niveau 3 : correspond au niveau de la supervision qui est effectuée par le biais des systèmes SCADA. Ces derniers permettent d'accéder aux données et aux systèmes de commande à distance. Plus concrètement, ils permettent de contrôler depuis un seul endroit plusieurs PLC. De plus, les systèmes SCADA sont souvent associés à des HMI[46] qui permettent d'avoir une interface graphique simplifiant la gestion à distance.

[44] Realpars. «What ist the Automation Pyramid ?», 11 juin 2018. https://realpars.com/automation-pyramid/, [consulté le 07.07.2022].

[45] Programmable Logic Controller (PLC). Une définition détaillée est donnée au chapitre 3.1.

[46] Human Machine Interface (HMI)

- Niveau 4 : gère la planification et les contrôles d'exécution à l'aide des systèmes MES[47] qui permettent de surveiller l'ensemble du processus industriel de la matière première jusqu'à livraison du produit fini. Grâce à ces systèmes, la direction sait exactement ce qui se passe au niveau de la production et peut prendre des décisions à l'échelle d'une usine entière en fonction de ces informations.

- Niveau 5 : est lié au management et associé aux ERP[48] qui permettent de combiner les informations opérationnelles des niveaux inférieurs avec les données de gestion. Ce niveau d'intégration permet donc à la direction de commander stratégiquement tous les niveaux de l'entreprise, de l'achat à la fabrication en passant par la vente ainsi que les finances, les ressources humaines etc.

[47] *Manufacturing Execution System (MES)*

[48] *Enterprise Resource Planning (ERP)*

2.4.3 Représentation graphique des activités critiques

Pour mieux appréhender les différentes activités critiques du secteur des réseaux thermiques (voir Figure 11), elles ont été réparties dans deux catégories. La première regroupe toutes les activités critiques dites organisationnelles, c'est-à-dire celles qui ont un impact sur le fonctionnement administratif d'une organisation. Quant à la deuxième plus spécifique, il s'agit des activités critiques opérationnelles liées aux processus industriels. Cette distinction entre les tâches organisationnelles et opérationnelles n'est pas anodine car elle fait partie d'une problématique plus globale traitant de la convergence entre les technologies de l'informatique (IT) et les technologies opérationnelles (OT) qui est à l'origine des problèmes de cybersécurité rencontrés par les organisations industrielles. Cette thématique est traitée de manière plus détaillée dans le sous-chapitre 3.6 de ce document. Afin d'être explicite, il est indiqué pour chaque activité critique de quels systèmes TIC elles dépendent, si elles sont considérées citriques pour des raisons liées à la *safety* et sur quel niveau de la pyramide d'automatisation elles se situent. De plus, pour comprendre le rôle de chaque activité sans avoir recours à d'autres supports, une brève description de ces dernières est donnée. Pour améliorer le confort de lecture, la Figure 11 se trouve aussi dans l'annexe 7.3 de ce document, en format A4.

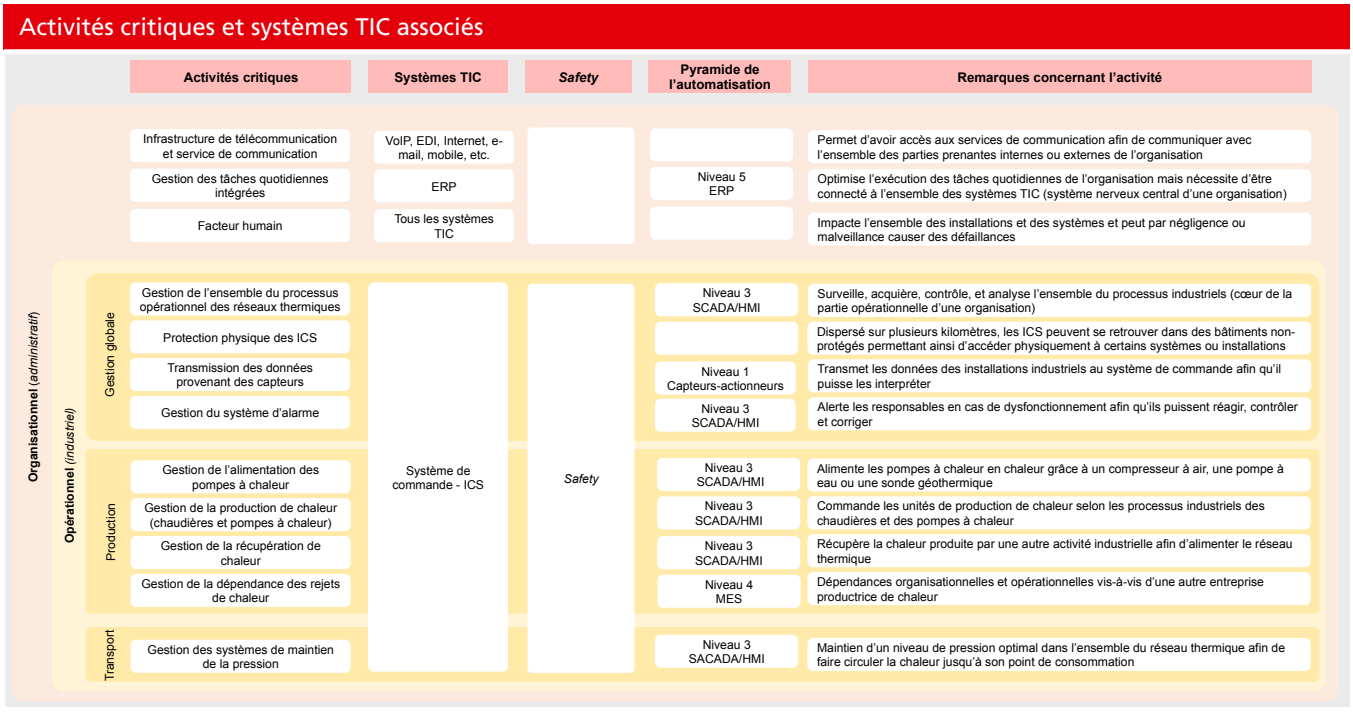

Figure 11 : Activités critiques et systèmes TIC

2.4.4 Activités critiques organisationnelles

Comme expliqué précédemment, il s'agit d'activités permettant à l'organisation de gérer une partie de ses tâches administratives. Le dysfonctionnement TIC d'une de ces activités critiques peut entrainer une paralysie partielle ou totale des infrastructures. Cependant, aucune d'entre-elles n'est considérée critique pour des raisons de *safety*.

2.4.4.1 Infrastructure de télécommunication et services de communication

Pour qu'une organisation puisse utiliser l'ensemble de ses systèmes TIC, elle doit avoir accès à des infrastructures de télécommunication. Pour ce faire, il est nécessaire qu'elle passe par un fournisseur *(provider)* créant ainsi une relation de dépendance. Il est donc important de choisir un fournisseur offrant un bon niveau de protection de ses infrastructures, proposant des services adaptés aux besoins de l'organisation et disposant d'un support efficace en cas d'incident. Afin d'augmenter le niveau de résilience d'une organisation, il est aussi recommandé d'avoir recours à plusieurs fournisseurs d'infrastructure de télécommunication. Cela permet de limiter le niveau de dépendance vis-à-vis d'un fournisseur et de disposer d'installations redondantes pouvant faire face à la déconvenue d'un des prestataires.

Les infrastructures de télécommunication donnent accès à une multitude de services de communication qui sont essentiels au bon fonctionnement. Il peut s'agir par exemple de la téléphonie vocale *(Voice over IP)*, de l'échange de données informatisé *(Electronic Data Interchange, EDI)*, de l'accès à Internet, des messageries électroniques, de la communication mobile ou encore de l'accès au cloud. Les services de communication jouent un rôle essentiel dans les relations internes et externes des entreprises. Sans ces outils, l'échange d'information entre les différentes parties n'est plus assuré paralysant ainsi le fonctionnement global de l'entreprise. Sans moyen de communiquer, il n'est pas aisé de gérer convenablement les activités organisationnelles et opérationnelles immobilisant ainsi l'organisation. Si l'organisation n'a plus accès aux infrastructures de télécommunication ainsi qu'à ses services de communication, elle perd l'usage de la totalité de ses systèmes TIC l'empêchant ainsi de poursuivre son activité.

2.4.4.2 Gestion intégrée des tâches quotidiennes

Ce système TIC, plus connus sous le terme d'enterprise *resource planning* (ERP), est souvent décrit comme le « système nerveux central d'une entreprise ». Il permet d'automatiser, d'intégrer et de fournir l'intelligence nécessaire à la réalisation de toutes les tâches de gestion du quotidien. Presque toutes les données de l'organisation sont stockées dans le système ERP afin qu'il puisse fournir une version exacte et unique de la réalité du fonctionnement de l'entreprise. Il est en charge de tâches diverses et variées liées par exemple à la facturation, aux ressources humaines, à la production, à la chaine d'approvisionnement, aux achats, aux stocks et à plein d'autres encore. Pour fonctionner efficacement, l'ERP peut être connecté avec des systèmes TIC de l'organisation ce qui lui confère une place névralgique au sein de l'infrastructure. En effet, une défaillance de l'ERP peut entraîner des dysfonctionnements dans plusieurs secteurs de l'entreprise. Il est donc primordial que l'ERP ne puisse pas être utilisé comme vecteur d'attaque (en le protégeant avec par exemple des *Air Gap*, *Demilitarized Zones* (DMZ), etc.) pour infecter les systèmes TIC critiques d'une organisation comme le système de commande (ICS). Pour protéger au mieux un ERP, il est nécessaire de réaliser régulièrement des sauvegardes *(backup)* de ses données afin de pouvoir le relancer sur des bases saines. Il est aussi important de créer une architecture réseau segmentée (voir sous-chapitre 4.2.4) efficace afin de protéger convenablement le système de contrôle industriel d'un défaut de l'ERP. De plus, il aussi essentiel de choisir un prestataire capable de garantir un support efficace et un développement permanent du logiciel afin qu'il soit le plus résilient possible.

2.4.4.3 Facteurs humains

Malgré les meilleures mesures techniques de protection, aucun système TIC n'est à l'abri d'une mauvaise manipulation humaine. Il s'agit du risque le plus courant, pouvant engendrer des pannes systèmes de grandes envergures. L'organisation doit se prémunir contre les erreurs humaines effectuées par négligence ou par malveillance. Dans le premier cas figure, il est obligatoire pour l'entreprise de former suffisamment ses employés sur la sécurité des systèmes TIC. Pour ce faire, il est recommandé de documenter la progression de la formation pour tous les collaborateurs et de répéter régulièrement la formation. Il s'agit de sensibiliser, instruire et responsabiliser les employés aux bonnes pratiques (cyberhygiène) afin qu'ils puissent accomplir leurs tâches dans le respect des normes de sécurité et ce pendant la totalité de leur rapport de travail. Les règles ainsi que les directives de sécurité TIC doivent être claires et réalistes afin de pouvoir développer un cadre et un mode opératoire appropriés pour les employés. De plus, les tâches et les responsabilités en cas de dysfonctionnement TIC doivent être définies clairement et attribuées de manière transparente entre les différents collaborateurs. Pour minimiser les risques liés aux employés, l'entreprise peut par exemple limiter les droits d'accès en les octroyant uniquement à certains responsables. Il est aussi pertinent de définir différents types de profils avec des droits spécifiques et adaptés aux besoins selon les systèmes TIC (ex : profil administrateur, modificateur, lecteur, etc.). De plus, afin de renforcer la sécurité des certaines tâches critiques, il est recommandé de mettre en place un principe de double identification. En ce qui concerne les actes malveillants, ils sont majoritairement effectués par des ex-employés. Afin de lutter contre ces attaques, les organisations doivent suivre un processus rigoureux en supprimant les accès des anciens collaborateurs et en modifiant régulièrement les protocoles d'accès aux infrastructures.

2.4.5 Activités critiques opérationnelles

Contrairement aux activités organisationnelles dont l'impact concerne l'ensemble de l'entreprise, les activités opérationnelles sont plus spécifiques et se rapportent aux processus industriels. Dans le chapitre 2.3 consacré aux processus d'approvisionnement, se sont ces activités qui sont majoritairement illustrées au travers des différents figures (Figure 6, Figure 7, Figure 8 et Figure 9). Le dysfonctionnement d'une de ces activités critiques met en péril la production, le transport ou la livraison de chaleur. Dans certains cas, une défaillance peut même mettre en danger la totalité du processus d'approvisionnement des réseaux thermiques. Comme il s'agit d'activités industrielles gérant divers systèmes de combustion atteignant de hautes températures ainsi que des conduits sous pression, la majorité d'entre-elles sont considérées comme critique parce qu'elles sont nécessaires au processus d'approvisionnement et pour des questions de *safety.*

2.4.5.1 Gestion de l'ensemble du processus opérationnel des réseaux thermiques :

La gestion des processus opérationnels des réseaux thermiques s'effectue principalement par le biais des ICS (système de commande, PLC, *Direct Digital Control* [DDC], etc.). Le système de commande a pour tâches de centraliser l'acquisition, la surveillance, le contrôle et le traitement des données provenant des unités de terrains dispersées géographiquement sur plusieurs kilomètres. Il offre la possibilité de contrôler à distance plusieurs opérations locales telles que le démarrage, le fonctionnement et l'arrêt des unités de productions, la collecte de données provenant de différents capteurs, la pression des conduits thermiques ou encore la surveillance de l'ensemble de l'infrastructure. Il s'agit donc de l'élément central de la gestion des processus opérationnels. En cas de dysfonctionnement du système de commande, l'organisation n'est plus en mesure de surveiller et de contrôler ses installations. Cependant, les installations doivent continuer à fonctionner de manière autonome, même en cas de panne du système de commande. De plus, comme le système de contrôle industriel a accès à presque toutes les activités industrielles, la prise de contrôle sur ce logiciel par des personnes malveillantes entrainerait des dommages conséquents pouvant également menacer la sécurité de vies humaines *(safety)* faisant

de cette activité l'une des plus critiques. De plus, comme il s'agit de systèmes spécifiques, ils sont développés et améliorés par des entreprises spécialisées entrainant une fois encore une relation de dépendance vis-à-vis d'un prestataire externe. Il est donc essentiel de choisir un fournisseur capable de garantir un support sans faille et un développement constant du système afin qu'il soit le plus sécurisé et résilient possible. L'architecture réseau du système de commande est aussi un élément essentiel à prendre en compte. Afin de limiter le plus possibles les accès à ce système et donc renforcer sa résilience, il est important de l'isoler des autres. Ce point est développé de manière plus détaillée dans le sous-chapitre 4.2.4 de ce document.

2.4.5.2 Protection physique des ICS

Comme les ICS sont utilisées pour contrôler des réseaux physiques répartis sur plusieurs kilomètres, il est nécessaire de prendre aussi en compte leur protection physique. Les points d'accès physiques principaux (PLC) se trouvent souvent dans les caves (chaufferies) des bâtiments privés. Comme il s'agit d'endroits souvent à l'écart et pas forcément bien sécurisés, les potentiels attaquants disposent des beaucoup de temps pour précéder à une telle attaque. De plus, la protection physique de tous ces points d'accès possibles (vecteurs d'attaque possibles) n'est donc pas possible. Selon la technologie utilisée, une éventuelle attaque peut se produire via WLAN, *Bluetooth* ou fibre optique. Il est donc nécessaire de procéder à une protection globale du réseau en appliquant une stratégie de *defense-in-depth* (voir chapitre 4.2).

2.4.5.3 Transmission des données provenant des capteurs

L'ensemble du processus opérationnel des réseaux thermiques est couvert de capteurs qui permettent de collecter ainsi que de transmettre les données liées au fonctionnement des différentes installations, au système de commande (ICS). Il s'agit donc d'éléments TIC qui sont physiquement présents sur l'ensemble des infrastructures du processus d'approvisionnement et en communication permanente avec le système de commande. Ils lui permettent d'obtenir des données diverses allant de la température de l'unité de production de chaleur, au niveau de pression des conduits thermiques, en passant par la quantité d'énergie consommée par le client. Une panne des capteurs de grande envergure ne permettrait plus de contrôler correctement l'installation car les PLC/DDC ne disposerait plus de données sur cette dernière. De ce fait, l'organisation perd la vue d'ensemble et ne peut plus contrôler cette infrastructure à distance. De plus, si les capteurs sont manipulés et transmettent des données erronées, les actions effectuées par l'organisation ne seraient plus en adéquation avec la réalité pouvant ainsi aggraver la situation réelle au lieu de l'améliorer. Selon l'importance de l'infrastructure à laquelle les capteurs sont connectés, une panne ou une transmission de données falsifiées peut déboucher sur une paralysie du processus d'approvisionnement ou/et sur la mise en danger de vies humaines *(safety)*. Il est donc important que les capteurs soient convenablement protégés afin de sécuriser l'ensemble du processus d'approvisionnement.

2.4.5.4 Gestion du système d'alarme

Les données collectées par les capteurs et analysées par le système de commande permettent de surveiller l'ensemble des installations. Afin de garantir un niveau de sécurité suffisant, un système d'alarme est combiné au système de commande permettant ainsi de détecter rapidement une anomalie sur l'ensemble de l'infrastructure. En effet, si le système de contrôle industriel s'aperçoit que les données examinées ne correspondent pas à l'intervalle de sureté prédéfini, il déclenche le système d'alarme qui va permettre de prévenir les responsables que le fonctionnement est altéré et qu'il est nécessaire de le corriger et de réagir. Un dysfonctionnement du système d'alarme empêche une organisation de réagir de manière appropriée ce qui peut entrainer un aggravement de la situation pouvant déboucher sur la mise en danger de vies humaines *(safety)* ou sur une blocage partiel ou complet des installations. Pour éviter cela, d'autres mesures de sécurité analogiques et physiques doivent être prises sur l'installation, telles que des soupapes de surpression, des pressostats, des thermostats, etc.

2.4.5.5 Gestion de l'alimentation des pompes à chaleur

Les pompes à chaleur sont approvisionnées en chaleur selon trois procédés, un compresseur pour l'air, une pompe à eau pour l'eau et une sonde pour la géothermie. La défaillance des systèmes TIC (capteurs, système de commande ou encore système d'alarme) ne permettrait plus aux pompes à chaleur d'être alimentées mettant ainsi en défaut l'ensemble de ce processus d'approvisionnement. De ce fait, si aucun système de production redondant permet de chauffer le réseau thermique, celui-ci n'est plus approvisionné en chaleur.

2.4.5.6 Gestion de la production de chaleur (chaudière et pompe à chaleur)

Comme cela a été expliqué précédemment, les infrastructures des réseaux thermiques sont couvertes de capteurs et connectées au système de commande (ICS). Les unités de production de chaleur ne font pas exception et peuvent être commandées sur place via l'interface machine (PLC)[49] ou à distance grâce au système de commande. Les systèmes TIC contrôlent donc différentes tâches comme par exemple, la mise en marche ou l'arrêt de l'installation, la quantité de combustible à brûler, la température à atteindre, la pression des systèmes ou encore le niveau d'énergie à produire. Un dysfonctionnement TIC sur une chaudière ou une pompe à chaleur engendre un arrêt de la production bloquant ainsi le processus d'approvisionnement des réseaux thermiques. De plus, si aucun système de production redondant n'existe, cette coupure empêcherait les clients d'être approvisionnés en chauffage pouvant, suivant la taille du réseau et la saison, provoquer leur mise en danger *(safety)*. Dans le cas où les systèmes TIC sont manipulés par une entité malveillante, cette dernière pourrait pousser l'unité de production à la limite de ses capacités ce qui pourrait engendrer des dégâts matériels et mettre en péril des vies humaines *(safety)*, à moins que d'autres mesures de sécurité physique ne soient en place (voir ci-dessus).

2.4.5.7 Gestion de la récupération de chaleur (rejet de chaleur)

À la différence des processus industriels fonctionnant avec les chaudières ou les pompes à chaleur, les rejets de chaleur ne produisent pas la chaleur mais la récupèrent. Pour l'entreprise en charge des réseaux thermiques sa responsabilité débute avec la récupération de chaleur. Il s'agit donc de capter la chaleur fournie par une autre activité industrielle et de la transférer aux conduits thermiques. Les systèmes TIC permettent de contrôler différents paramètres (quantité, température, pression, etc.) afin que les réseaux thermiques disposent de la chaleur nécessaire pour leur bon fonctionnement. En cas de défaillance des systèmes TIC, il pourrait ne plus être possible de récupérer la chaleur nécessaire pour chauffer les différents conduits des réseaux thermiques entravant le processus d'approvisionnement et pouvant priver de chauffage les clients ce qui peut avoir des répercussions funestes selon la taille du réseau et la saison *(safety)*.

2.4.5.8 Gestion de la dépendance des rejets de chaleur

Contrairement aux chaudières et aux pompes à chaleur, un élément supplémentaire doit être pris en compte pour les rejets de chaleur. En effet, l'entreprise responsable des réseaux thermiques ne produit pas elle-même la chaleur ce qui la rend dépendante du processus d'approvisionnement lié à l'activité principale productrice de chaleur et à l'entreprise qui en a la responsabilité. Cette spécificité met en évidence trois éléments qu'il est important de prendre en compte lors de la mise en œuvre de la stratégie de cybersécurité.

Structure organisationnelle

Le premier élément est organisationnel et concerne la répartition des tâches et des responsabilités entre les deux organisations. Il n'existe aucun standard prédéfini, la structure choisie dépend du contexte. Il se peut, par exemple, qu'une seule entreprise soit responsable de l'activité principale et du réseau thermique ou alors que deux organisations se partagent les tâches de manières bien délimitée en séparant soigneusement leurs infrastructures ou encore que la délimitation des tâches entre les deux entreprises ne soit pas si évidente et qu'elles partagent une partie de leurs installations ou systèmes. Cette distinction organisationnelle a un impact sur le fonctionnement mais aussi sur la protection des organisations car, plus deux entreprises sont dépendantes, plus elles doivent être protégées conjointement afin que le dysfonctionnement TIC de l'une n'entraine pas la défaillance de l'autre.

Architecture réseau

Le deuxième élément se concentre sur l'architecture réseau utilisée par les entreprises afin de limiter leur interdépendance. En effet, une bonne architecture réseau permet de segmenter les différents réseaux TIC et d'isoler les plus importants afin qu'il soit difficile pour un attaquant de les atteindre. L'objectif principal étant généralement de confiner les systèmes TIC de la partie « opérationnelle » afin de renforcer la protection des infrastructures liées à la production et d'éviter leur manipulation.

[49] *Explications au chapitre 3.1*

Il est donc primordial d'utiliser une architecture réseau efficace lorsque des entreprises sont dépendantes l'une de l'autre. Une mauvaise architecture réseau peut donc entrainer des défaillances en chaîne pouvant entrainer la mise en danger physique de l'ensemble des installations et mettre en danger des vies humaines *(safety).* Plus d'informations sur l'architecture réseau sont disponibles dans le chapitre 4.2.4.

Activités critiques

Quant au troisième élément, il est lié à la gestion des activités critiques. Dans le cas des rejets de chaleur, l'entreprise en charge des réseaux thermiques peut se protéger convenablement contre les cyberrisques en sécurisant correctement ses activités critiques. Cependant, cela ne sera pas suffisant car pour chauffer ses conduits thermiques, elle utilise de la chaleur provenant d'une autre activité potentiellement gérée par une autre entreprise et dont les activités citiques dépendent d'un autre processus d'approvisionnement. De ce fait, les activités critiques des entreprises ayant recourt aux rejets de chaleur ne se limitent pas uniquement à celles énoncées dans ce document mais comprend aussi toutes celles liées à l'exécution de l'activité principale. Il est donc primordial que les deux entreprises travaillent conjointement pour atteindre un niveau de sécurité suffisant. Il en va de même dans la situation où une seule entreprise est responsable de l'activité principale et du réseau thermique. Elle doit prendre en compte les activités critiques des deux secteurs pour se protéger efficacement.

Synthèse de la dépendance

Pour mieux représenter cette relation de dépendance, il est intéressant de se référer à la Figure 12 qui illustre le fonctionnement d'une usine de valorisation thermique et électrique des déchets (UVTED) dont la chaleur est récupérée pour alimenter une installation de cogénération produisant de l'électricité et alimentant un réseau thermique. De manière simplifiée, cette illustration identifie les différentes activités permettant de faire fonctionner cette infrastructure. Le processus industriel global est, dans cet exemple, divisé en quatre. Ils représentent différents secteurs industriels qui sont couverts par des normes minimales TIC sectorielles spécifiques. La première se rapporte aux réseaux thermiques, la deuxième à l'électricité[50], la troisième à l'élimination des déchets[51] et la dernière au traitement des eaux usées[52]. Cette image permet de mieux se rendre compte des effets de dépendance entre l'activité principale (élimination des déchets) et la récupération de la chaleur pour le réseau thermique. Elle montre aussi que dans le cas des rejets de chaleur, le secteur des réseaux thermiques ne doit pas être pris séparément mais qu'il fait partie d'un ensemble composé de plusieurs secteurs industriels. Lors de la mise en œuvre d'un programme de cybersécurité, il est nécessaire de protéger la totalité des infrastructures afin de limiter les effets de dépendance. Il est donc recommandé aux entreprises d'avoir une vision globale afin qu'elles puissent identifier la totalité des activités critiques qui composent leur processus d'approvisionnement, déterminer leurs responsabilités ainsi que celles des organisations dont elles sont dépendantes, élaborer une architecture réseau pertinente et utiliser à bon escient les différentes normes minimales TIC sectorielles existantes afin de sécuriser convenablement l'ensemble des systèmes TIC dont elles dépendent.

[50] Norme minimale pour garantir la sécurité des technologies de l'information et de la communication (TIC) pour l'approvisionnement en électricité. Association des entreprises électriques suisses (AES), Office fédéral pour l'approvisionnement économique du pays (OFAE), Suisse 2018.

[51] Norme minimale pour garantir la sécurité des technologies de l'information et de la communication (TIC) dans le domaine de l'élimination des déchets. Association suisse des exploitants d'installations de traitement des déchets (ASED), Office fédéral pour l'approvisionnement économique du pays (OFAE), Suisse 2022.

[52] Norme minimale pour garantir la sécurité des technologies de l'information et de la communication (TIC) dans les stations d'épuration des eaux usées. Association suisse des professionnels de la protection des eaux (VSA), Office fédéral pour l'approvisionnement économique du pays (OFAE), Step by STEP, Suisse 2021.

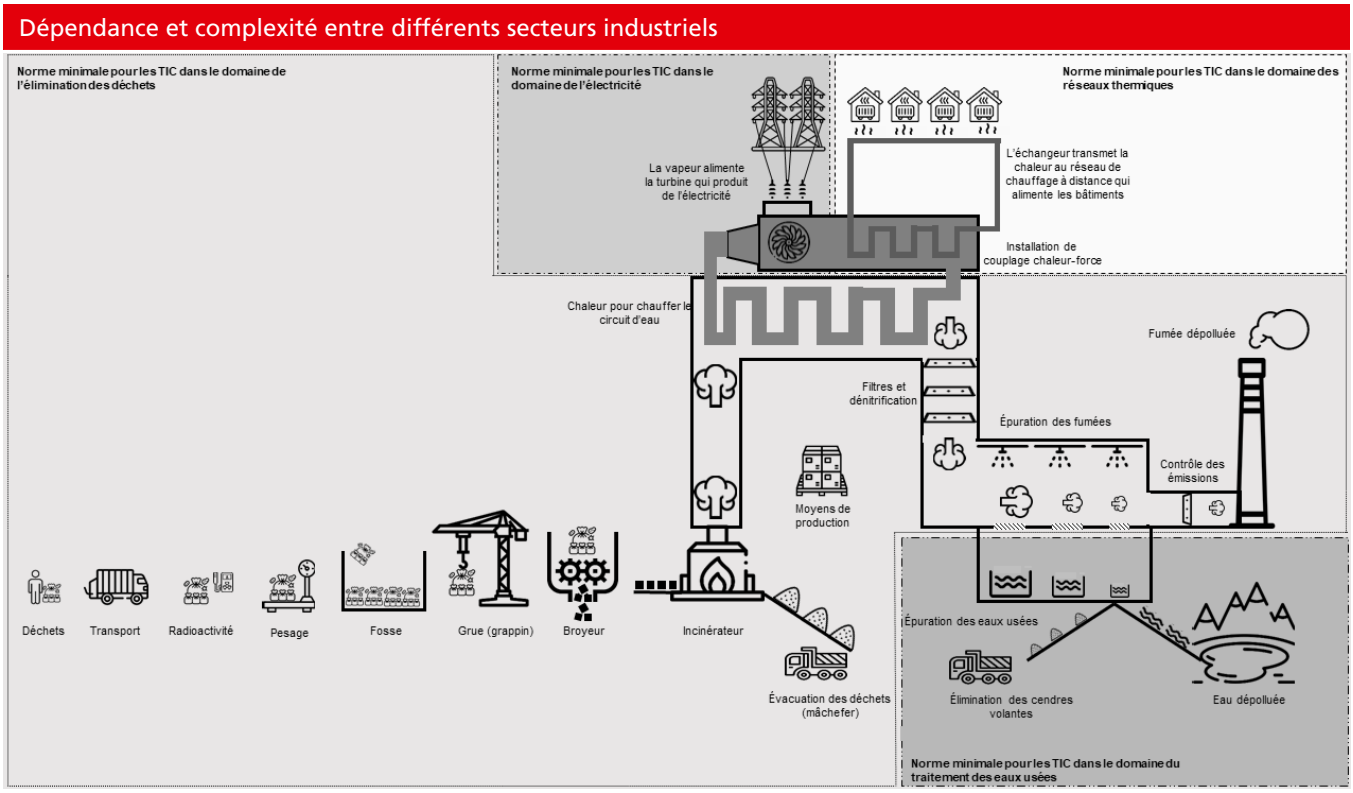

Figure 12 : Dépendances entre UVTED, réseau thermique, électricité et eau usée

2.4.5.9 Gestion des systèmes de maintien de la pression

Afin de permettre à la chaleur d'être livrée jusqu'au client, les conduits thermiques sont mis sous pression. Le fluide caloporteur (principalement eau ou vapeur) peut ainsi transporter la chaleur jusqu'aux stations de transfert de chaleur des différents clients. Afin de maintenir un niveau de pression optimal, des stations de pompage connectées aux systèmes de commande s'attèle à cette tâche. Un dysfonctionnement TIC lié à cette activité entrainerait une défaillance du système de pression. En cas de sous-pression, le fluide caloporteur ne pourrait plus circuler correctement dans l'ensemble des conduits empêchant d'approvisionner la totalité des clients. Alors qu'en cas de surpression, les conduits thermiques peuvent céder ce qui déboucherait sur une panne physique bloquant aussi l'approvisionnement. Dans les deux cas, un problème de pression entraine un arrêt partiel voire total du processus d'approvisionnement. De plus, si la taille du réseau est importante (beaucoup de clients) et que la saison est particulièrement froide (hiver), le manque de chauffage peut entrainer la mise en danger de vies humaines classant cette activité comme critique aussi pour des raisons de *safety*.

3 Besoins et contraintes liés aux ICS

Dans les précédents chapitres, le terme ICS a été introduit brièvement en expliquant qu'il s'agissait d'équipements permettant de contrôler des systèmes industriels. Cependant, pour protéger efficacement ces systèmes, il est important de connaître plus en détail leur composition, leur fonctionnement, leur évolution ainsi que leurs spécificités.

3.1 Différents types d'ICS

Un système de contrôle industriel (ICS) est composé de plusieurs éléments de contrôle pouvant être électriques, mécaniques, hydrauliques ou encore pneumatiques, et qui interagissent ensemble afin d'atteindre un objectif commun, comme par exemple, gérer le processus de production de chaleur d'une chaudière à pellets. La tâche de ce système consiste à collecter des données provenant de processus variables ou des statuts de machines industrielles mais aussi à contrôler ces machines sur place ou à distance.[53] Ce terme générique englobe plusieurs types de systèmes de contrôle dont les plus importants sont les systèmes SCADA, DCS et PLC.[54]

La spécificité d'un système de contrôle et d'acquisition de données (SCADA) est d'effectuer des contrôles opérationnels sur de longues distances en utilisant les ondes radio, la transmission satellite, le réseau téléphonique ou encore le réseau WAN.[55] Ce type d'ICS est donc principalement utilisé dans la distribution industrielle. Il permet de centraliser l'acquisition, la surveillance, le contrôle et le traitement des données provenant des unités de terrains dispersées géographiquement sur des centaines ou des milliers de kilomètres. Il offre aussi la possibilité de contrôler à distance plusieurs opérations locales telles que l'ouverture et la fermeture de vannes ou de disjoncteurs, la collecte de données provenant de différents capteurs ainsi que la surveillance des unités de terrain et la possibilité de réagir si nécessaire.[56]

Contrairement à un système SCADA, les DCS *(Distributed Control System)* et les PLC *(Programmable Logic Controller)* communiquent principalement par le biais d'un réseau local (LAN)[57] et sont utilisés pour contrôler les systèmes de production dans un même lieu géographique. Un DCS permet de décomposer un processus en plusieurs tâches distinctes (modules de production) et de contrôler individuellement chaque tâche permettant ainsi de limiter l'impact d'un défaut sur l'ensemble du système de production. Les DCS sont connectés à des capteurs et des actionneurs qui adaptent, en temps réel, les processus industriels pour que les données de production restent comprises dans un intervalle *(setpoint control)* défini.[58]

Le PLC était, à l'origine, un petit ordinateur industriel conçu pour exécuter des fonctions logiques de base (relais, interrupteurs ou encore minuterie). Aujourd'hui, les PLC ont évolué et sont capables de contrôler des processus complexes. Ils sont largement utilisés en tant que composant de contrôle dans les systèmes SCADA et DCS, mais également comme contrôleur principal dans des petits systèmes de contrôle (comme par exemple dans les chaînes de montage automobile ou les commandes de souffleurs de suie des centrales électriques).[59]

[53] National Institute of Standards and Technology. « Glossary : industrial control system ICS ». https://csrc.nist.gov/glossary/term/industrial_control_system [consulté le 17 avril 2020].

[54] Falco, J., Scarfone, k. & Stouffer, K. (2013). NIST Special Publication 800-82, Guide to Industrial Control Systems (ICS) Security. National Institute of Standards and Technology.

[55] Il s'agit d'un réseau étendu qui permet la transmission de données à un grand nombre d'utilisateurs sur une zone géographique bien plus étendue que le réseau LAN

[56] National Institute of Standards and Technology. « Glossary : Supervisory Control and Data Acquisition SCADA ». https://csrc.nist.gov/glossary/term/Supervisory_Control_and_Data_Acquisition [consulté le 17 avril 2020].

[57] Local Area Network : réseau local reliant des appareils se situant dans le même endroit géographique.
National Institute of Standards and Technology. « Glossary : Local Area Network LAN ». https://csrc.nist.gov/glossary/term/Local_Area_Network [consulté le 17 avril 2020].

[58] National Institute of Standards and Technology. « Glossary : Distributed Control System DCS ». https://csrc.nist.gov/glossary/term/Distributed_Control_System [consulté le 17 avril 2020].

[59] National Institute of Standards and Technology. « Glossary : Programmable Logic Controller PLC ». https://csrc.nist.gov/glossary/term/Programmable_Logic_Controller [consulté le 17 avril 2020].

3.2 Évolution des ICS

Les ICS sont, aujourd'hui, utilisés dans de nombreuses industries, notamment dans la production et la distribution. Pour les entreprises de production, les systèmes ICS sont généralement centralisés en un seul endroit (DCS et PLC) alors que pour les entreprises de distribution (p. ex. le gaz, l'eau ou l'électricité), ils sont répartis géographiquement sur plusieurs sites (SCADA).

Historiquement, les ICS ont été implémentés sur la technologie opérationnelle (OT). Au début, cette technologie opérationnelle était principalement mécanique et dépendait des opérateurs, dont la tâche consistait à actionner des sélecteurs, leviers et autres éléments mécaniques afin de permettre le bon fonctionnement de l'installation. La demande croissante et la nécessité d'augmenter les capacités opérationnelles ont accéléré l'automatisation des processus industriels. Dès 1950, les processus industriels ayant recourt à des processeurs informatisés pour le contrôle des leurs activités étaient déjà d'actualité, particulièrement pour les secteurs de production et les services publics.

Le terme « système de contrôle et d'acquisition de données » (SCADA) est apparu dans les années 70 pour désigner une combinaison entre *hardware* et *software* permettant de superviser (de manière automatisée) un processus industriel. A leurs débuts, les systèmes SCADA étaient de grande taille et entièrement propriétaires. Ils ne possédaient pas ou que très peu de moyens de communication, en dehors du périmètre d'action lié au fournisseur spécifique. Dans les années 1990 et 2000, les fournisseurs de SCADA ont commencé à adopter des architectures ouvertes pour leurs produits, permettant ainsi à leurs systèmes d'être interconnectés.[60]

3.3 Convergence entre IT et OT au sein d'un ICS

Afin de réduire les coûts et d'améliorer le fonctionnement de ces systèmes, notamment par le biais d'une meilleure connectivité, surveillance et analyse, les technologies opérationnelles (OT) ont commencé à fusionner avec les technologies de l'information (IT). Cette convergence entre OT et IT a permis de rendre « intelligents » les systèmes industriels, c'est-à-dire connectés et automatisés. L'avènement de « l'industrie intelligente » est généralement désigné sous le terme « d'industrie 4.0 ».[61] De ce fait, les équipements actuels sur lesquels repose la technologie opérationnelle et les systèmes SCADA qui y sont implémentés, permettent de contrôler ces outils numériquement à distance en utilisant des protocoles de communication IT standard. Cette convergence OT-IT implique donc que dans tous les secteurs, les systèmes IT exploitent, de plus en plus, les données des systèmes OT soutenant ainsi la tendance générale à l'automatisation, qui est caractéristique de la quatrième révolution industrielle.[62]

Bien qu'il existe une convergence entre IT et OT, ces deux technologies restent conçues pour des tâches différentes. Les technologies de l'information regroupent l'ensemble des systèmes informatiques qui soutient le travail quotidien d'une entreprise. Il s'agit d'ordinateurs, d'équipements auxiliaires, de logiciels, de microprogrammes ou encore de services qui sont utilisés pour l'acquisition, le stockage, la manipulation, le contrôle, la transmission et la réception automatisée des données ou de l'information.[63] Quant aux technologies opérationnelles, elles sont utilisées pour le travail opérationnel, lié aux processus industriels, d'une organisation. Elles englobent tous les équipements qui interagissent avec l'environnement physique et qui permettent de détecter ou de provoquer, par le biais de la surveillance et du contrôle de certains dispositifs, un changement impactant directement un processus industriel.[64]

[60] Balmelli, Laurent. « Build a Cyber Security Program for Industrial Control Systems ». Medium, 14 février 2020. https://medium.com/@laurentbalmelli/bui ld-a-cyber-security-program-for-industrial-control-systems-5026064aa633 [consulté le 20 février 2020].

[61] Marr, Bernard. « What is Industry 4.0 ? Here's a super easy explanation for anyone ». Forbes, 2 septembre 2018. https://www.forbes.com/sites/bernardmarr/2018/09/02/what-is-industry-4-0-heres-a-super-easy-explanation-for-anyone/#3c395f7e9788 [consulté le 2 mars 2020].

[62] World Economic Forum. « What is the fourth industrial revolution ? ». https://www.weforum.org/agenda/2016/01/what-is-the-fourth-industrial-revolution/ [consulté le 2 mars 2020].

[63] National Institute of Standards and Technology. « Glossary : information technology IT ». https://csrc.nist.gov/glossary/term/information_technology [consulté le 17 avril 2020]

[64] National Institute of Standards and Technology. « Glossary : Operational Technology OT ». https://csrc.nist.gov/glossary/term/operational_technology [consulté le 17 avril 2020].

3.4 De nouveaux besoins pour la sécurité des ICS

Comme expliqué précédemment, cette convergence des technologies OT et IT a amélioré la productivité des processus industriels, mais elle a aussi apporté son lot d'inconvénients. En effet, cette nouvelle interdépendance a rendu la technologie opérationnelle vulnérable à des perturbations externes, fragilisant ainsi la fiabilité et la sécurité des systèmes industriels. Néanmoins, cette nouvelle vulnérabilité a été rapidement identifiée et est, depuis les années 2000, un sujet de préoccupation pour les chercheurs et les experts en cybersécurité.

En 2007, l'expérience « *Aurora Generator Test* »[65], menée par l'*Idaho National Laboratory,* a permis de démontrer comment une cyberattaque pouvait détruire physiquement des composants d'un réseau électrique. Il aura suffi de quelques lignes de code pour pousser le générateur à « s'autodétruire ». Aujourd'hui, la sécurité de l'OT est toujours un besoin réel en constante évolution. Les enjeux sont tels, que certains grands noms de l'informatique (Microsoft, ABB, BlackBerry Cylance, Fortinet…)[66] se sont associés pour essayer d'y répondre.

L'un des avantages de cette convergence entre OT et IT est l'amélioration et la standardisation de la connectivité TCP/IP. Cependant, en contrepartie, cela expose aussi les ICS aux attaques basées sur les adresses IP. Il est donc important de sécuriser les différents points d'accès *(endpoint security),* c'est-à-dire d'avoir la certitude que tous les éléments connectés à un réseau restreint soient sécurisés et conformes. Comme pour un réseau TIC, les informations industrielles telles que les données opérationnelles et financières doivent aussi être sécurisées dans le cas d'un ICS. L'accès à ces informations sont d'un grand intérêt pour un attaquant car il est facile de les monétiser par le biais, par exemple, d'un *ransomware* mais elles peuvent être d'un intérêt encore plus grand pour des cyberattaques plus sophistiquées dont le but est la destruction physique de l'infrastructure industrielle.

En plus de ces quelques exemples, la sécurité d'un ICS comporte aussi une dimension physique. La fiabilité et la sécurité du processus doivent être garanties car, comme le démontre le cas du générateur Aurora mentionné en dessus, une faille de sécurité numérique peut entraîner la destruction d'éléments physiques, ce qui peut avoir des conséquences directes sur la vie humaine, la production ou la distribution.[67]

À plus large échelle, les ICS de distribution qui font partie des infrastructures critiques de la Suisse sont fortement interconnectés et interdépendants. De ce fait, la défaillance d'un élément important peut entraîner des défaillances en cascade et donc des pannes de plus en plus graves. Il est donc primordial de les protéger.

3.5 Contraintes de sécurité pour les ICS

Un système ICS fonctionne selon des besoins spécifiques liés à la nature des processus physiques des différents contrôleurs (p. ex. PLC) présents au sein des unités de terrain. Il est donc important de prendre en compte ces contraintes lors de l'élaboration d'un programme de sécurité afin d'utiliser les mesures de sécurité adaptées.

Un système ICS est construit sur des systèmes opérationnels fonctionnant en temps réel ce qui induit une contrainte de temps et de performance pouvant poser problème lorsque des mesures de sécurité actives sont appliquées. En effet, ces mesures actives peuvent influencer l'exécution du système en fonction des événements liés à la sécurité. Afin d'éviter cette problématique, les mesures passives sont privilégiées dans les solutions actuelles de surveillance des ICS.

[65] CNN. Staged cyber attack reveals vulnerability in power grid. https://edition.cnn.com/2007/US/09/26/power.at.risk// [consulté le 2 mars 2020].

[66] Businesswire. New Operational Technology Cyber Security Alliance Launches to Deliver Comprehensive Cyber Security Guidelines for Operational Technology. https://www.businesswire.com/news/home/20191021005857/en/New-Operational-Technology-Cyber-Security-Alliance-Launches [consulté le 2 mars 2020].

[67] Balmelli, Laurent. « Build a Cyber Security Program for Industrial Control Systems ». Medium, 14 février 2020. https://medium.com/@laurentbalmelli/build-a-cyber-security-program-for-industrial-control-systems-5026064aa633 [consulté le 20 février 2020].

L'une des autres exigences d'un système ICS est la nécessité de fonctionner en continu. C'est pourquoi les interruptions sont souvent planifiées des jours ou des semaines à l'avance. Les pratiques informatiques (IT) courantes, telles que le redémarrage d'un composant, ne sont pas possibles et auraient un impact négatif sur la fiabilité du système ainsi que sur sa disponibilité et sa maintenabilité. Ce fonctionnement en continu a un impact direct sur tout le processus de gestion des changements et fait de la gestion des correctifs et de la vulnérabilité une tâche difficile dans un ICS. La durée de vie typique des composants, qui est de l'ordre de 10 à 15 ans, rend cette tâche encore plus difficile. Une durée de vie aussi longue est généralement en contradiction avec le rythme rapide de l'évolution technologique.

Un système ICS a aussi des contraintes de ressources notamment à cause de l'exigence d'exécution en temps réel. Les composants d'un système ICS ne disposent donc pas de toutes les fonctionnalités IT typiques telles que le cryptage, l'enregistrement des erreurs ou la protection par mot de passe rendant les systèmes ICS vulnérables. Toutefois, la prise de conscience de la nécessité de la sécurité s'est accrue depuis la découverte de certains *malwares* (notamment Stuxnet)[68] et a commencé à faire évoluer les mentalités, tant du côté des clients que du côté des fournisseurs.[69]

[68] Ce malware a été découvert en 2010. Il s'agissait de la première cyber-arme conçue pour attaquer une cible industrielle. Il était capable d'espionner un système ICS et de reprogrammer les PLC, tout en camouflant les modifications effectuées.

[69] Balmelli, Laurent. « Build a Cyber Security Program for Industrial Control Systems ». Medium, 14 février 2020. https://medium.com/@laurentbalmelli/build-a-cyber-security-program-for-industrial-control-systems-5026064aa633 [consulté le 20 février 2020].

3.6 Différences de protection entre les composants IT et OT d'un ICS

Précédemment, il a été expliqué que depuis plusieurs années, il existait une convergence entre les technologies de l'information et opérationnelles. Cette convergence se produit dans la partie OT du réseau d'un ICS sous la forme d'équipements industriels supportant les normes informatiques *(IT standards)* ainsi que la présence croissante d'ordinateurs à usage général fonctionnant sous une OS commune.

Cependant, bien qu'il y a une convergence, ces deux technologies ne peuvent pas être protégées de la même manière. En effet, il est nécessaire d'adapter les moyens de sécurité utilisés pour protéger les technologies OT et IT. Les composants de la partie IT d'un réseau, liée aux tâches organisationnelles d'une organisation, fonctionnent comme la plupart des appareils informatiques communs avec une solution antivirus classique, des mises à jours régulières et un cycle de vie plutôt court de deux à trois ans. Alors que les composants de la partie OT d'un réseau, liée au travail opérationnel et industriel, nécessitent quant à eux des mesures de sécurité particulières (cf. chapitre 3.5). Afin d'appliquer des mesures de sécurité adaptées, le Tableau 1 décrit les principales différences de sécurité entre la partie OT et IT d'un ICS.

Thématique sécuritaire	IT (p. ex. gestion des e-mails, imprimantes, téléphones, etc.)	OT (p. ex. SCADA, DCS, PLC, etc.)
Antivirus	Largement répandu. Facile à distribuer et à actualiser. Possibilité de personnalisation par les utilisateurs. Possibilité de configurer la protection antivirus au niveau des appareils ou à l'échelle de l'entreprise.	Les besoins de stockage et le ralentissement des échanges de données par le processus de scannage des logiciels antivirus peuvent avoir une influence négative sur un système ICS. Les organisations ne peuvent protéger les anciens éléments de l'ICS qu'avec des solutions après-vente. Les solutions antivirus recourent souvent à des dossiers « d'exception » dans les environnements ICS afin d'éviter la mise en quarantaine des fichiers stratégiques.

Tableau 1 : Différences relatives à la sécurité entre IT et OT

Thématique sécuritaire	IT (p. ex. gestion des e-mails, imprimantes, téléphones, etc.)	OT (p. ex. SCADA, DCS, PLC, etc.)
Mise à jour de sécurité *(Update Management)*	Clairement définies, effectuées à l'échelle de l'entreprise, automatisées grâce à des accès à distance.	Longueur des délais et des périodes de planification jusqu'à l'installation réussie du patch correctif ; toujours propres au fabricant ; peuvent provoquer un arrêt (temporaire) du système ICS. Nécessité de définir le risque acceptable à cet égard.
Cycle de vie de la technologie *(Technology Support Lifecycle)*	2 à 3 ans, plusieurs fournisseurs, développement et mises à niveau continus.	10 à 20 ans, généralement un seul fournisseur ou prestataire de service sur tout le cycle de vie, la fin du cycle de vie génère de nouvelles mises en danger de la sécurité.
Méthodes de test et d'audit *(Testing and Audit Methods)*	Recours à des méthodes modernes (si possible automatisées). Les systèmes sont généralement suffisamment résilients et fiables pour supporter des évaluations au cours de l'exploitation.	Les méthodes d'évaluation automatisées peuvent ne pas être adaptées, notamment en raison du caractère très personnalisé des solutions. Il existe une forte probabilité d'erreur durant les évaluations. Il est donc généralement plus difficile de les réaliser au cours de l'exploitation.
Gestion des modifications *(Change management)*	Rythme régulier et planifié. Adapté aux exigences de l'entreprise, pour la durée minimale et maximale du fonctionnement de l'appareil.	Processus complexe avec un impact possible sur les activités de l'entreprise. Une planification stratégique et individuelle est indispensable.
Classification des actifs *(Asset Classification)*	Exécution courante et annuelle. Dépenses et investissements planifiés conformément aux résultats.	Effectuée uniquement lorsque cela est nécessaire et obligatoire. Sans inventaire, les contre-mesures ne sont généralement pas adaptées à l'importance de l'élément du système.
Réaction et analyse aux incidents *(Incident Response and Forensics)*	Facile à développer et à mettre en œuvre. Au besoin, se conformer aux prescriptions réglementaires (protection des données).	Principalement axées sur le redémarrage du système. Processus d'analyse peu réglementés.
Sécurité physique *(Physical Security)*	Varie de faible pour les outils de bureautique à forte pour les centres de données sécurisés.	Varie de faible (maison individuelle) à élever (centres de données sécurisés).
Développement des logiciels sécurisés *(Secure Software Development)*	Partie intégrante du processus de développement.	Historiquement, les systèmes ICS étaient conçus comme des systèmes distincts. Il n'était pas prévu d'intégrer la sécurité dans leur développement. Les fournisseurs des systèmes ICS ont fait des progrès, mais moins que dans le domaine IT. Il n'existe guère de solutions pour sécuriser a posteriori les éléments centraux des systèmes ICS.
Règle de sécurité *(Safety Rules)*	Prescriptions réglementaires générales, selon le secteur (pas tous les secteurs).	Normes réglementaires propres au secteur (mais pas tous les secteurs).

Tableau 1 : Différences relatives à la sécurité entre IT et OT

3.7 Attaques récurrentes envers les ICS

Dans ce chapitre 3, la définition, le fonctionnement, l'évolution et les spécificités de sécurité des ICS ont été abordés. Le dernier élément à prendre en compte concerne les attaques contre les ICS. En raison de leur architecture complexe, les ICS font face à certaines vulnérabilités *(vulnerabilities)* qui peuvent, dans les cas les plus graves, rester insoupçonnées pendant très longtemps. Si ces vulnérabilités sont exploitées, elles peuvent se transformer en une *Advanced Persistent Threat*[70]. Pour l'illustrer, voici quelques méthodes d'attaque caractéristiques des systèmes ICS contre lesquelles le programme de sécurité de la norme minimale offre une protection appropriée :

- attaque en provenance d'Internet à l'encontre d'un système ICS accessible en ligne, dans le but d'établir un accès à distance longue durée,
- accès à distance au système ICS via l'utilisation de données d'accès volées,
- attaques envers le système ICS à travers l'exploitation des failles de l'*interface web,*
- contamination d'un système ICS par des logiciels malveillants provenant de supports corrompus (p. ex. clés USB, *smartphones,* etc.),
- attaque via les systèmes IT (p. ex. via des courriels d'hameçonnage *(« phishing »)* ou infection par téléchargement furtif *(« Drive-by Download »)*, etc.) visant à pénétrer dans un système ICS par n'importe quelle interface.

[70] Il s'agit d'une cyberattaque discrète et ciblée qui est effective sur une longue durée. Généralement, le but d'une Advanced Persistent Threat est de surveiller l'activité d'un réseau ou/et de voler des données sans impacter le réseau.

4 Programme de cybersécurité

Lors de l'élaboration de la norme minimale TIC, le choix du programme de cybersécurité s'est porté sur le *NIST Framework Core.* Cette méthodologie[71] américaine, élaborée par le *National Institute of Standards and Technology* (NIST), permet de disposer d'une protection globale et surtout continue des équipements TIC. L'objectif du *NIST Framework Core* et de ses recommandations est de fournir aux opérateurs d'infrastructures critiques et aux autres organisations dépendantes des TIC, un instrument leur permettant d'accroître de manière indépendante et autonome leur niveau de résilience face aux risques des TIC. Il offre aussi une combinaison de sécurité équilibrée entre la technologie commune de l'IT et les contrôles de sécurité spécifiques de l'OT, tout en étant technologiquement neutre. De plus, le *NIST Framework Core* est compatible avec les normes ISO 2700x.

Dans son programme de sécurité, le *NIST Framework Core* combine une approche basée sur le risque et une stratégie de *defense-in-depth.* L'analyse du risque acceptable est primordiale pour une organisation car cela lui permet d'adapter les mesures du *NIST Framework Core* à ses propres besoins (selon son secteur, sa taille, ses ressources et ses menaces). Après cette analyse, chaque organisation est en mesure de déterminer, selon ses ressources, le niveau de protection optimale à atteindre. Quant à la stratégie *defense-in-depth,* il s'agit d'une approche dérivée du principe militaire qui veut qu'un système de défense multicouche complexe est plus difficile à franchir qu'une simple barrière. L'objectif de cette stratégie est donc d'appliquer plusieurs mesures de sécurité sur différents niveaux de protection (allant, par exemple, de la protection du réseau à la protection des éléments physiques en passant par la formation des collaborateurs) obligeant ainsi le potentiel attaquant à franchir une multitude d'obstacles de sécurité complexes.

Le dernier élément de ce programme de sécurité concerne les mesures du *NIST Framework Core.* Il s'agit d'une centaine de mesures réparties sous cinq fonctions : identifier, protéger, détecter, réagir et rétablir. Chaque organisation doit évaluer (entre 0 et 4) l'ensemble de ces mesures afin qu'elle puisse identifier ses faiblesses et appliquer les solutions de sécurité correspondantes. L'évaluation de ces mesures offre un cadre de sécurité complet permettant aux organisations d'adapter en continu leur programme de sécurité à leurs besoins. De plus amples informations ainsi que les détails de toutes les mesures de sécurités du *NIST Framework Core* sont approfondis au chapitre 5.

4.1 Gestion des risques

Il s'agit d'une étape préalable à la *defense-in-depth* qui aide chaque organisation à identifier ses risques ainsi que sa propension au risque (risque acceptable). L'objectif étant de définir correctement quelles ressources engager, pour quel niveau de protection et contre quel risque.

4.1.1 Programme de gestion des risques

Il faut comprendre les risques auxquels une entreprise est exposée (menaces informatiques) pour mettre en œuvre une stratégie de *defense-in-depth.* Ils doivent être gérés en fonction de la propension au risque de l'entreprise. Les responsables de l'exploitation et de la maintenance des systèmes TIC doivent pouvoir identifier, évaluer et traiter les *cyber*-risques. Cela exige une bonne connaissance des scénarios de menace, des processus opérationnels et techniques, ainsi que des technologies en jeu. On ne peut intégrer dans les tâches quotidiennes une stratégie de *defense-in-depth* qu'après avoir analysé ces paramètres. La direction de l'entreprise doit définir la sécurité comme un prérequis à toutes ses activités informatiques.

[71] *National Institute of Standards and Technology. An Introduction to the Components of the Framework. https://www.nist.gov/cyberframework/online-learning/components-framework [consulté le 9 janvier 2020].*

Les règles énoncées ci-dessus ne sont que des principes généraux. Certaines applications TIC sont particulièrement importantes, voire critiques, notamment dans les systèmes de contrôle industriels (ICS). Pour concevoir une architecture de sécurité ICS efficace, il faut que les risques de l'entreprise soient rapportés aux exigences fonctionnelles (opérationnelles) du ICS. Cela peut avoir des incidences dans le monde réel (par ex. un périmètre de sécurité autour d'un centre de calcul). Les décideurs, à tous les niveaux de l'entreprise, doivent saisir l'importance des cyberrisques et être activement impliqués dans leur processus de gestion. Il est nécessaire d'effectuer régulièrement des analyses de risques pour les systèmes, applications et processus cruciaux, y compris pour les réseaux associés. Elles doivent être effectuées selon des règles strictes, suivant une approche structurée et systématique.

4.1.2 Cadre pour gérer les risques

Les analyses des risques informatiques devraient être intégrées dans la gestion globale des risques et être effectuées régulièrement sur des objets de recherche clairement définis. Il s'agit par exemple de systèmes, de processus et d'applications stratégiques (même en cours de développement) ainsi que d'autres systèmes, réseaux et services dont ils dépendent. Ce cadre de gestion des risques permet d'affecter aux risques identifiés des responsables/rôles qui vont surveiller (monitorage), évaluer et mettre en œuvre des mesures permettant de circonscrire les risques dans des limites préalablement définies comme acceptables (= propension au risque).

4.1.3 Analyse des risques

Il est nécessaire de définir clairement la portée de l'analyse des risques informatiques, de décrire les processus opérationnels et les éléments techniques pertinents (et d'éventuels facteurs externes), puis de pondérer ces facteurs et éléments. Ainsi on aura défini le contenu et les limites de l'analyse.

4.1.4 Analyse de l'impact sur les affaires *(business impact analyse)*

Cette analyse permet d'évaluer quel serait l'impact (réaliste voire extrême) d'une composante TIC corrompue (y compris les personnes, les données, les processus, les services ou les réseaux) sur les activités d'une entreprise, et ce, à divers titres (financier, opérationnel, juridique, réputationnel, sanitaire). Il est nécessaire de déterminer l'impact sur les activités que l'entreprise est prête à assumer en cas d'absence de ses ressources informatiques. Par conséquent, il convient de définir les exigences et les niveaux de protection nécessaires pour assurer la disponibilité, l'intégrité et la confidentialité des ressources TIC choisies en fonction d'un risque jugé acceptable.

4.1.5 Mesures contre le risque

Identifier, examiner et valider les mesures à prendre est nécessaire pour se prémunir contre les risques décrits dans l'analyse d'impact. La direction de l'entreprise doit les valider en même temps que les plans précisant la marche à suivre. Il est aussi indispensable d'évaluer le risque résiduel pour tous les équipements dans l'environnement considéré et à le gérer de manière adéquate (l'atténuer, le contourner, le transférer ou l'accepter), selon la propension au risque de l'entreprise. Il est nécessaire de déterminer le risque maximal acceptable pour chaque équipement *(asset)*, permettant ainsi de calculer les risques informatiques (cumulés).

4.2 Stratégie de *defense-in-depth*

4.2.1 Application de la stratégie de *defense-in-depth*

Une entreprise doit axer sa stratégie de sécurité informatique sur la protection des équipements TIC indispensables aux processus opérationnels. Il est donc important d'avoir une approche à plusieurs niveaux. Dans le secteur de la cybersécurité, la stratégie de *defense-in-depth* vise à détecter les atteintes à la sécurité des systèmes TIC et à réagir en réduisant leurs effets. La *defense-in-depth* poursuit une approche globale qui vise à protéger toutes les ressources TIC contre n'importe quel risque. Une entreprise devrait consacrer ses ressources à se protéger des risques connus et à cerner les risques potentiels. Des mesures appropriées doivent protéger l'intégralité des systèmes TIC. Cela comprend les personnes, les processus, les bâtiments, les données et les appareils. Un agresseur ne constitue une menace pour un système TIC que s'il parvient à détecter et exploiter une faille dans l'un de ces éléments. Les entreprises doivent régulièrement contrôler l'efficacité des mesures de protection et les adapter aux nouvelles menaces si nécessaire.

Afin de limiter les menaces qui pèsent sur les systèmes ICS, les facteurs suivants doivent être pris en en compte lors de l'application de la stratégie de *defense-in-depth :*

- les coûts liés à la sécurisation des systèmes anciens conformément aux besoins actuels,
- la tendance croissante à connecter les systèmes ICS aux réseaux d'entreprise,
- la possibilité d'autoriser les accès à distance pour les utilisateurs et les fournisseurs (prestataires de services), tant dans l'environnement IT qu'OT,
- la nécessité de se fier à sa chaîne d'approvisionnement *(« supply chain »)*,
- les possibilités actuelles de surveillance et de protection des protocoles spécifiques aux systèmes ICS,
- la possibilité d'actualiser en permanence les connaissances spécialisées au sujet des nouvelles menaces à l'encontre des systèmes ICS.

La stratégie de *defense-in-depth* complique donc les attaques directes envers les systèmes TIC et augmente la probabilité de déceler rapidement un comportement étrange ou inhabituel au sein d'un système. Cette approche aide également à créer des zones séparées pour la mise en place des technologies destinées à reconnaître une intrusion dans le système *(Intrusion Detection Technology)*.
Afin d'offrir une vision plus globale de ce concept, une sélection de différentes couches de protection de la stratégie de *defense-in-depth* appliquée par le *NIST Framework Core* est représentée dans le Tableau 2 et détaillée dans les sous-chapitres suivants.

Éléments représentatifs d'une stratégie de *defense-in-depth*	
Protection des applications *(monitoring)*	• *Intrusion Detection Systems IDS* • sécurité des *Audit-Logging* • problèmes de sécurité et contrôle des incidents
Protection des *Hosts* (terminaux)	• gestion des correctifs et des points faibles • terminaux • appareils virtuels
Protection du réseau	• normes/recommandations • lignes directrices et mode opératoire • zones de sécurités standards • réseaux locaux (LAN) virtuels
Protection du périmètre réseau	• zones démilitarisées (DMZ) et pare-feu *(firewall)* • accès à distance et authentification • serveurs intermédiaires/hôtes
Protection des éléments physiques	• protection des terminaux • surveillance des accès au centre de contrôle • vidéosurveillance, contrôle des accès et barrières
Gestion des fournisseurs	• gestion et contrôle de la chaîne des fournisseurs • services d'infogérance et externalisation • utilisation de services *cloud* • gestion des accès à distance
Gestion des collaborateurs	• lignes directives • mode opératoire • formation et conscientisation
Gestion de la politique de sécurité informatique	• ligne directrice claire • application de la politique de sécurité • contrôle de la politique de sécurité

Tableau 2 : Éléments représentatifs d'une stratégie de defense-in-depth

4.2.2 Protection des applications *(monitoring)*

L'utilisation de systèmes de *monitoring* (surveillance) et de composants réseau qui permettent de détecter une intrusion par exemple par anomalies[72] ou par signatures[73] ajoute de la complexité à un environnement informatique ou à un ICS. Les fonctions de surveillance et de détection selon le plan de *defense-in-depth* sont toutefois indispensables pour protéger les équipements critiques. Une barrière électronique autour du réseau ICS ne suffit pas à protéger les ressources critiques contre une intrusion. Le plan de la *defense-in-depth* prévoit qu'une entreprise soit alertée dès que possible par son système de surveillance en cas de problème de sécurité. La plupart des entreprises ont une surveillance standard dans leur environnement informatique, mais elles oublient parfois de le faire pour leurs réseaux ICS.

Il est donc indispensable d'effectuer des audits de sécurité exhaustifs, indépendants et réguliers (secteurs critiques dans l'entreprise, processus, applications et systèmes/réseaux supportés) ; de surveiller les flux de données dans les systèmes ICS afin de détecter tout comportement inadéquat ; de surveiller les risques informatiques, de respecter les exigences légales, réglementaires et contractuelles importantes pour la sécurité et d'informer régulièrement la direction de l'entreprise de la sécurité informatique.

4.2.3 Protection des *hosts* (terminaux)

Un degré de sécurité supplémentaire doit être apporté au niveau des hosts ou postes de travail. Les *firewalls* protègent la plupart des appareils contre les intrusions extérieures, mais un bon système de sécurité exige des défenses à plusieurs niveaux. Une sécurisation complète du réseau implique de sécuriser tous les serveurs, toutes les connexions et tous les *endpoints.* Cette couche de sécurité doit permettre à un opérateur d'utiliser divers systèmes d'exploitation et différentes applications tout en assurant une protection correcte des équipements.

Les directives sur les mots de passe doivent être identiques pour tous les utilisateurs d'un système. Les noms de comptes classiques (p. ex. administrateur) doivent être modifiés et les mots de passe initiaux doivent être changés. Les utilisateurs auront tendance à contourner des pratiques trop restrictives en notant leur mot de passe (p. ex. sur des post-it) ou en utilisant systématiquement des chaînes de caractères semblables. La complexité relative aux mots de passe doit être adaptée selon le niveau d›autorisation des utilisateurs. Il est aussi possible d'exiger des changements de mots de passe à intervalles réguliers.

Les recommandations générales suivantes devraient être mises en œuvre par les entreprises pour chaque *host* ICS et chaque appareil doté d'un accès au réseau de l'entreprise (quel que soit le système d'exploitation) :

- installer et configurer un *firewall* spécifique pour les *hosts*
- désactiver les autologin
- régler si possible les écrans de veille à intervalles très courts, obligeant de redonner le mot de passe (activer les *autologout*)
- installer régulièrement les correctifs *(patches)* des systèmes d'exploitation et mettre à jour les micrologiciels
- configurer les logs et les activer sur tous les appareils
- désactiver les services et les comptes non utilisés, de même que ceux qui ne sont plus utilisés
- remplacer les services non sécurisés (Telnet, *Remote Shell* ou FTP) par des solutions plus sûres (sTelnet, SSH, sFTP, etc.)
- ne pas autoriser les utilisateurs à désactiver des services
- effectuer et contrôler les sauvegardes des systèmes, surtout si elles ne sont pas gérées de manière centralisée
- activer ou remplacer les modules de sécurité fournis avec le système d'exploitation (scanners de sécurité) par des logiciels plus performants
- appliquer les mêmes stratégies aux appareils portables, qu'ils soient connectés en permanence ou pas au réseau de l'entreprise. Il est aussi recommandé de crypter les disques durs des équipements portables.

[72] Les systèmes de détection d'intrusion par anomalies analysent le flux du réseau et réagissent lorsqu'ils détectent un comportement anormal.
[73] Les systèmes de détection d'intrusion par signatures stockent des bibliothèques contenant des descriptions d'attaques et réagissent lorsqu'ils détectent l'une de ces attaques dans le réseau.

4.2.4 Protection du réseau

Une architecture de cybersécurité comprend des mesures spécifiques et leur positionnement stratégique dans le réseau afin d'instaurer les couches de sécurité requise pour une *defense-in-depth.* Elle facilite également la collecte d'informations sur les flux de données entre tous les systèmes et sur leurs connexions. L'architecture de cybersécurité devrait être en phase avec l'inventaire des installations et des ressources TIC pour garantir que les flux informatiques soient globalement identifiés dans l'entreprise.

Une architecture de cybersécurité devrait être en adéquation avec le *NIST Framework Core* et prendre en compte la protection de la confidentialité, de l'intégrité et de la disponibilité des données, des services et des systèmes. Pour ce faire, il est nécessaire d'élaborer un plan de mise en œuvre respectant la culture d'entreprise et les objectifs stratégiques, tenant adéquatement compte des besoins de sécurité et indiquant les ressources requises. En général, une architecture de cybersécurité est complétée par une liste de tâches qui détaille les résultats espérés (signalant des problèmes et l'urgence de poursuivre l'analyse en profondeur pour établir des plans plus précis), établit les agendas des projets, évalue les besoins en ressources et cerne les principaux facteurs de dépendance du projet.

4.2.4.1 Composants principaux d'une architecture réseau

Dans cette section, différents modèles de conception vont être abordés en se basant sur les ICS de distribution (principalement SCADA). Cependant, ces éléments ne sont pas tous exclusifs aux systèmes SCADA et peuvent, par conséquent, aussi être transposés à d'autres types d'ICS.

Comme cela a déjà été évoqué, l'une des spécificités d'un système SCADA réside dans sa capacité à communiquer sur de longues distances à l'aide d'un réseau WAN, d'ondes radio ou encore via le réseau téléphonique, lui permettant ainsi de rester connecté avec l'ensemble de ses unités de terrain dispersés sur plusieurs sites. Un système SCADA permet donc de centraliser la surveillance et la gestion des données qui proviennent des *field sites* (unités de terrain), au sein d'un *control center* (centre de contrôle). Le *control center* héberge généralement un *SCADA server*[74] (serveur SCADA), des *Engineering Workstations EWS* (des postes de travail d'ingénierie), des *Human Machine Interfaces HMI* (des interfaces homme-machine) ainsi qu'un *data historian*[75] qui est une base de données centralisée permettant l'analyse des données en utilisant des techniques statistiques de contrôle de processus. Le rôle du *SCADA server* est important, car il établit la liaison entre le *control center* et les *field site*s par le biais des PLC ou RTU. Ce sont ces derniers qui permettent aux opérateurs d'effectuer depuis le *control center* des diagnostics et des réparations à distance sur les *field sites,* mais aussi de contrôler des processus physiques grâce aux actionneurs et aux capteurs auxquels ils sont connectés.

L'ensemble des éléments faisant partie des *control centers* et des *field sites* sont généralement regroupés sous la dénomination *control network* (réseau de contrôle) et représentent la partie OT du réseau, car ils sont en lien direct avec le travail opérationnel. A contrario, il existe la partie IT du réseau aussi appelée *corporate network* (réseau d'entreprise) qui héberge les fonctions de *back-office* nécessaires pour gérer les aspects organisationnels et financiers de l'entreprise.[76] En général, le *corporate network* a accès à tous les *control centers* et *field sites* pour, par exemple, les opérations de dépannage et de maintenance. Pour des raisons de sécurité, le *control newtwork* est généralement séparé du *corporate network* par une technologie de *firewall* (pare-feu) et/ou une *demilitarized zone DMZ* (zone démilitarisée) afin d'éviter d'offrir un accès à l'ensemble des systèmes opérationnels. De plus amples informations sur les périmètres de sécurité réseau sont disponibles dans le sous-chapitre 4.2.5.

Enfin, il existe de multiples façons de mettre en œuvre les systèmes ICS et l'architecture utilisée dépend principalement de l'industrie et de l'ampleur des opérations. La Figure 13 illustre le fonctionnement général ainsi que les différents composants d'un système ICS qui ont été abordés dans ce chapitre. Il s'agit plus d'un modèle explicatif que réaliste et reste orienté pour les ICS de distribution.[77]

[74] Est aussi connu sous les dénominations : Control server, Master Terminal Unit (MTU) ou encore Supervisory controller.
[75] National Institute of Standards and Technology. « Glossary : data historian ». https://csrc.nist.gov/glossary/term/Data_Historian [consulté le 29 avril 2020].
[76] À noter que le data historian peut aussi se trouver dans le corporate network
[77] Falco, J., Scarfone, k. & Stouffer, K. (2013). NIST Special Publication 800-82, Guide to Industrial Control Systems (ICS) Security. National Institute of Standards and Technology.

Architecture réseau générique d'un systèmes SCADA

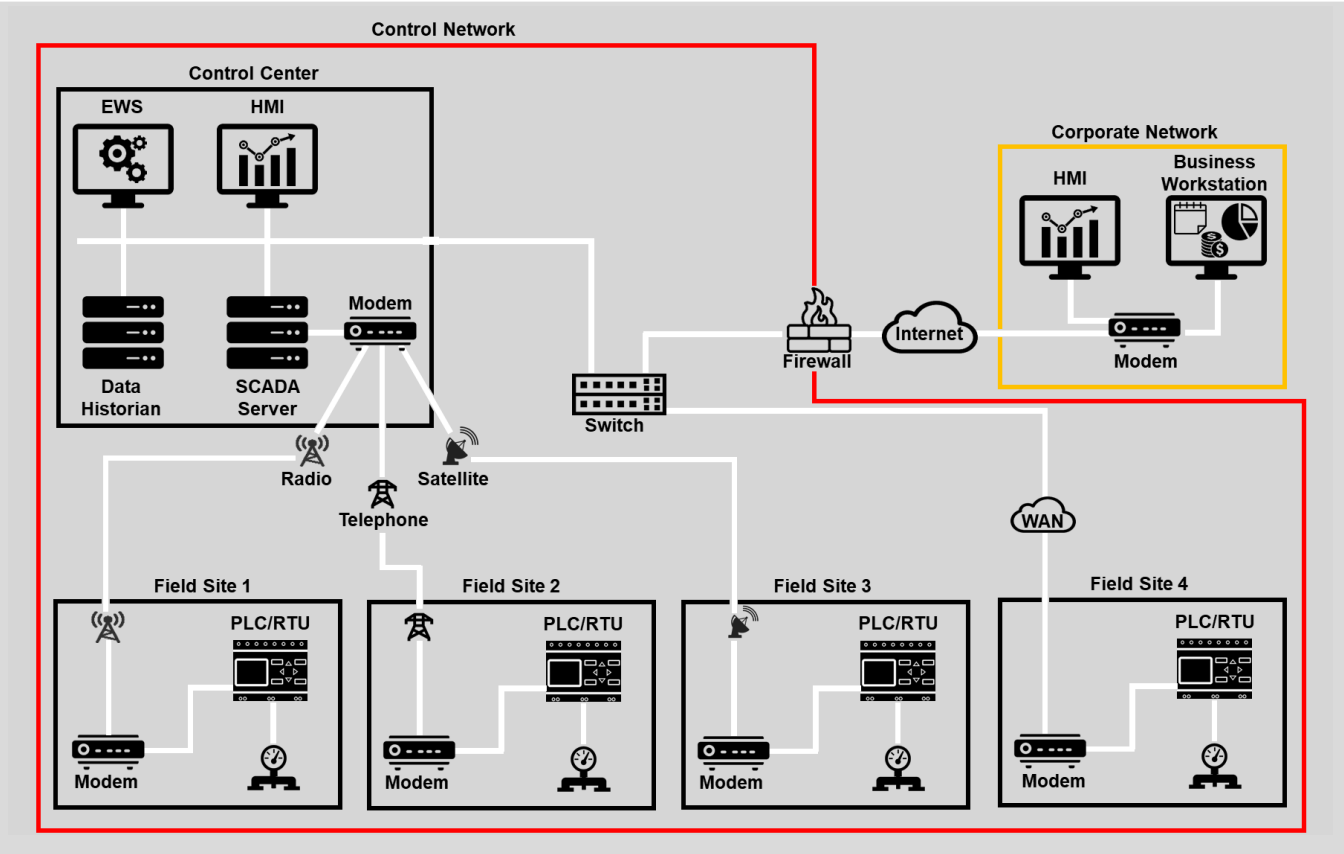

Figure 13 : Architecture réseau générique d'un système SCADA

4.2.4.2 Segmentation de l'architecture réseau

Une architecture réseau stable et sécurisée constitue l'une des principales conditions à toute défense efficace contre les attaques. Chaque interface, chaque passerelle, chaque connexion représente un danger potentiel. Il faut donc impérativement connaître et gérer en conséquence tous les processus normalement supportés par les réseaux et les équipements. Le principe de base consiste à définir une architecture réseau en groupant ou en segmentant correctement les différents réseaux. L'important est de subdiviser les réseaux en au moins deux zones de sécurité. La première zone de sécurité, dédiée aux systèmes organisationnels, englobe les systèmes informatiques de planification et de répartition des ressources (p. ex. ERP, système de gestion des achats). La seconde zone de sécurité, dédiée aux systèmes opérationnels, englobe les ICS servant à piloter le processus d'approvisionnement des réseaux thermiques. Contrairement à la figure précédente qui détaille les différents composants présents dans une architecture réseau, la Figure 14 illustre très schématiquement l'architecture réseau de la filière des réseaux thermiques, avec ses activités critiques liées au domaine IT et au domaine OT, ainsi que ses zones de sécurité montrant une fois encore une séparation claire et sécurisée entre le *corporate network* et le *control network* représentés ici respectivement par la zone « organisation » et la zone « production ».

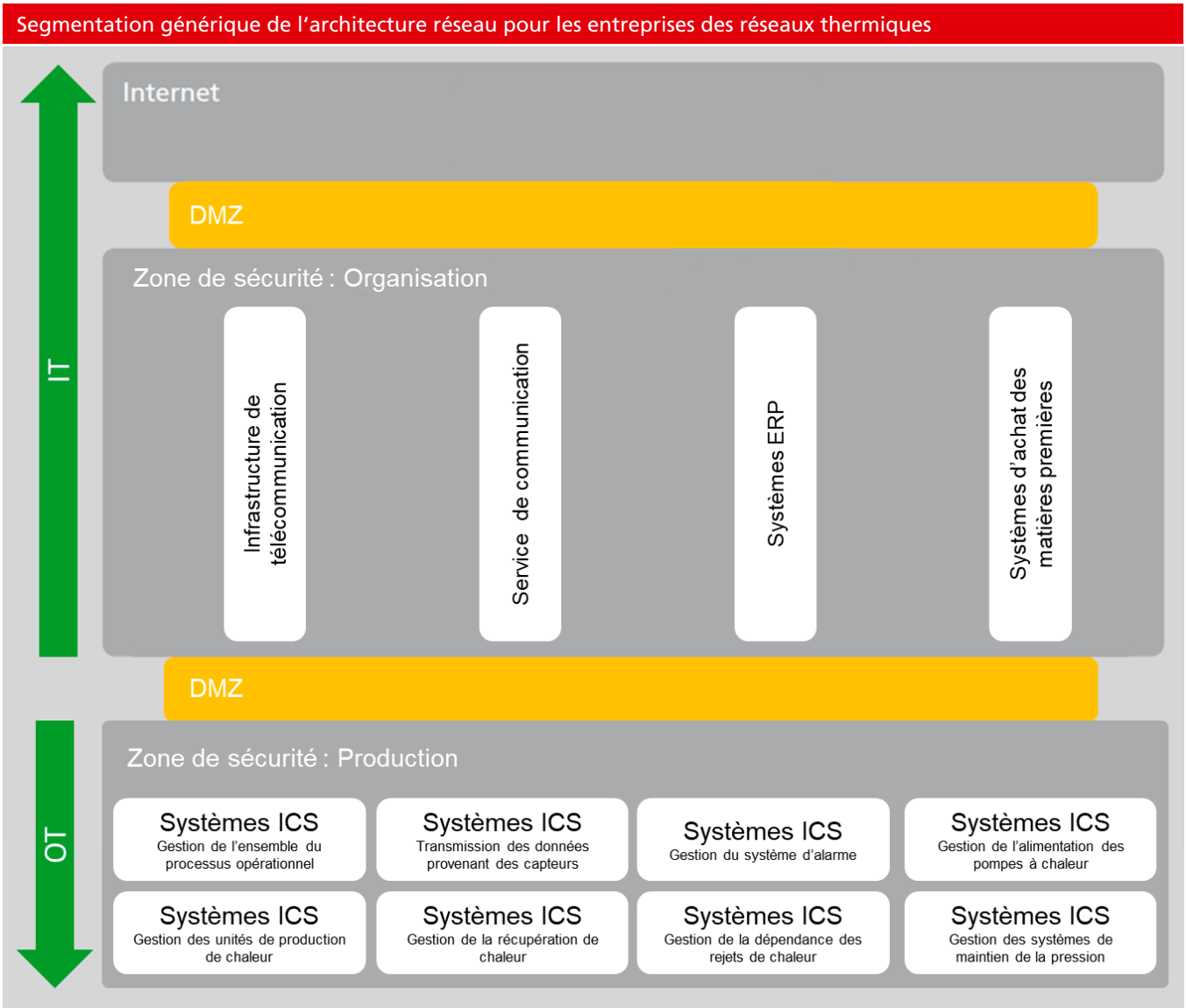

Figure 14 : Segmentation générique de l'architecture réseau pour les entreprises des réseaux thermiques

4.2.5 Périmètre de sécurité entre les réseaux

Le coût d'une installation ICS et la maintenance d'une infrastructure de réseau homogène exigent souvent une connexion entre le *corporate network* et le *control network*. Cette connexion (visible sur les Figure 13 et Figure 14) représente un important risque pour la sécurité et elle devrait être techniquement protégée. Si les réseaux doivent absolument être interconnectés, il est fortement recommandé de n'autoriser qu'un minimum de connexions (voire des connexions uniques) via un *firewall* (pare-feu) et une DMZ (segment de réseau séparé). Les serveurs ICS contenant les données du réseau d'entreprise doivent être placés dans une de ces zones « démilitarisées ». Les connexions avec l'extérieur doivent être recensées et limitées via le *firewall*. En outre, des systèmes de détection d'anomalies permettent de surveiller les échanges de données et de les valider.

4.2.6 Protection des éléments physiques

Après avoir sécurisé les éléments « techniques » en lien avec les différents réseaux utilisés par l'organisation, il est nécessaire de protéger l'accès aux équipements physiques ainsi qu'à l'environnement de travail. En plus de sécuriser physiquement certains équipements, il est aussi important de prendre en compte le cycle de vie des composants physiques. Certains éléments, OT notamment, peuvent avoir un cycle de vie particulièrement long (entre 10 et 20 ans) et il est nécessaire de s'assurer de leur sécurité pendant toute leur période d'activité. Quant aux appareils portables qui peuvent fréquemment être perdus, oubliés ou encore volés, il est nécessaire d'opter pour une configuration standard limitant au mieux les potentiels dégâts.

4.2.6.1 Protection physique des équipements et des installations

Les mesures de sécurité physique réduisent le risque de pertes accidentelles ou intentionnelles, ou de dommages causés aux appareils informatiques ou à l'environnement TIC de l'entreprise. Les équipements à protéger comprennent le matériel tout comme les outils et les installations, l'environnement (au sens écologique) et le voisinage ainsi que ce qui relève de la propriété intellectuelle, notamment les données propriétaires (paramètres de configuration ou fichiers clients). Les contrôles de sécurité doivent fréquemment répondre à des exigences spécifiques dans différents domaines : environnement, sécurité, réglementation, droit, etc. Les entreprises doivent adapter les contrôles de sécurité et les contrôles techniques à leurs besoins de protection. Pour garantir une protection globale, la sécurité physique comprend également la protection des composantes informatiques *(= security)* et des données sur l'environnement informatique. La sécurité de nombreuses infrastructures TIC est étroitement liée à la sécurité des installations *(= safety)*. L'objectif est de mettre les employés à l'abri du danger sans entraver leur travail. Les contrôles de sécurité sont des mesures actives ou passives qui limitent l'accès à toutes les composantes de l'infrastructure TIC. Ces mesures de protection doivent notamment empêcher les cas suivants :

- visiteurs indésirables aux endroits critiques
- modifications physiques, manipulations, vols ou autres disparitions voire destructions de systèmes, d'infrastructures, d'interfaces de communication, voire de sites
- observations inopportunes d'installations critiques, émanant de curieux, de photographes ou de personnes faisant d'autres sortes de relevés
- introduction ou installation non autorisée de nouveaux systèmes, infrastructures, interfaces de communication ou autre équipement informatique
- introduction illicite d'appareils (clés USB, point d'accès sans fil, *Bluetooth* ou *mobiles*), destinés à endommager des équipements, intercepter des communications ou nuire d'une autre manière.

4.2.6.2 Gestion des cycles de vie du matériel

Pour répondre aux besoins de la sécurité informatique, il faut protéger les équipements, y compris les systèmes et le matériel réseau, les outils de bureautique (imprimantes en réseau et appareils multifonctions) et les équipements spéciaux (par ex. les ICS) tout au long de leur cycle de vie, de leur acquisition (achat ou location) à leur élimination, en passant par leur maintenance. L'achat ou la location de matériel robuste et fiable doit toujours se faire en respectant les exigences de sécurité. Les éventuels points faibles du matériel doivent toujours être identifiés. L'objectif est de garantir que les équipements offrent les fonctionnalités désirées et ne compromettent pas la sécurité des informations et des systèmes critiques ou sensibles et ce, tout au long de leur cycle de vie.

4.2.6.3 Configuration des appareils portables contre le vol ou en cas de perte

Pour protéger les données contre les accès non autorisés, la perte et le vol, les appareils portables (ordinateurs portables, tablettes et smartphones) doivent toujours avoir une configuration standardisée qui réponde aux exigences de sécurité en limitant les accès, en installant des logiciels de sécurité et en gérant les appareils de manière centralisée. Le but de cette configuration standardisée est de garantir, même en cas de perte ou de vol, la sécurité informatique des données stockées ou envoyées sur l'appareil portable.

4.2.7 Gestion des fournisseurs

La gestion des fournisseurs concerne l'identification et la gestion des risques liés aux technologies de l'information pour les fournisseurs externes (matériel + logiciels, services d'externalisation, services *clouds* etc.). Définir et respecter les exigences en matière de sécurité informatique par le biais de contrats formels permet de minimiser les risques.

4.2.8 Gestion des collaborateurs-trice-s

Les erreurs humaines posent de nombreux défis aux entreprises. Les mesures techniques de protection ne peuvent jamais garantir qu'aucune erreur ne se produise, que ce soit par malveillance ou par négligence. Dans une entreprise, le risque d'erreur est directement lié au niveau de formation et de connaissance des employés dans le domaine des TIC. Lutter contre d'éventuels actes malveillants commis par ses propres collaborateurs confronte une entreprise à un autre genre de défi. Elle doit, pour ce faire, résoudre divers problèmes.

4.2.8.1 Les cycles de la vie professionnelle

La sécurité de l'information doit être un souci permanent pour l'entreprise. La sensibilisation, la formation et son suivi, ainsi que la responsabilisation des employés doit se faire en permanence, du début à la fin du rapport de travail. Les employés doivent acquérir les compétences nécessaires pour accomplir leurs tâches dans le respect de la sécurité et des valeurs d'entreprise. Les divers accès, tant physiques que digitaux, par exemple les accès aux locaux, aux bâtiments, aux serveurs et aux logiciels dont disposent les employés doivent être revus régulièrement et modifiés en cas de changement d'activité ou de transfert à l'intérieur de l'entreprise. Un processus RH doit veiller à ce que ces différents accès soient radiés au moment de la fin du rapport de travail.

4.2.8.2 Les règles et directives

Des règles et des directives claires et réalistes définissent le comportement des employés en matière de sécurité. Elles donnent un cadre et prévoient des contrôles pour protéger les systèmes en appliquant ces règles. Elles décrivent également les modes opératoires et définissent les attentes de l'entreprise envers ses collaborateurs. Les consignes et les instructions déterminent ce qui doit être respecté ainsi que la manière de sanctionner les infractions.

4.2.8.3 Les processus de sécurité

L'organisme responsable de la sécurité informatique est chargé de gérer la sécurité et les spécificités de ses processus. Sa fonction première est de protéger les informations et les données de l'entreprise. Les processus de gestion de la sécurité doivent être appliqués aux systèmes de contrôle industriels. Pour ce faire, il faut définir les processus précisant la manière d'opérer ou de configurer certains systèmes. Ces processus doivent être normalisés et reproductibles. L'entreprise formera toujours ses nouveaux collaborateurs afin de maintenir un niveau de sécurité constant, ce qui garantira qu'ils connaissent toutes les réglementations et normes requises. Le processus de détection et de réaction d'un *cyberincident (Intrusion detection and response)* est extrêmement important. Les procédures de sécurité liées au réseau sont cruciales pour les protocoles propriétaires et les systèmes patrimoniaux.

4.2.8.4 Tâches et responsabilités dans les secteurs critiques de l'entreprise

Il est nécessaire de communiquer et d'attribuer clairement à des personnes compétentes les tâches et les responsabilités dans les environnements critiques, de la gestion des processus métier à l'utilisation des applications spécifiques (y compris les systèmes et réseaux supportés), ainsi que l'accès aux informations. L'objectif est de susciter chez les employés un sentiment de responsabilité individuelle. Un tel climat dans une entreprise aide les employés à effectuer leurs tâches en respectant les prescriptions de sécurité informatique.

4.2.8.5 Communication et programmation de sensibilisation à la sécurité

Un programme de sensibilisation à la sécurité et une politique de communication ouverte responsabilisent les employés et favorisent les comportements adaptés à tous les niveaux hiérarchiques de l'entreprise. L'objectif est d'obtenir dans une entreprise un climat qui favorise les comportements de sécurité individuels. Chacun devrait pouvoir prendre des décisions en fonction du risque dans sa sphère de compétences.

4.2.9 Gestion de la politique de sécurité informatique

Une fois la stratégie globale de sécurité informatique définie, maintenue et contrôlée, la direction d'une entreprise peut fixer des lignes directrices claires et les défendre tant dans l'application des exigences que dans la gestion des risques.

5 Les mesures du NIST Framework Core

5.1 Introduction au *NIST Framework Core*

Le programme de cybersécurité de la norme minimale et ses recommandations visent à fournir aux organisations du secteur des réseaux thermiques un instrument leur permettant d'accroître leur résilience TIC de manière autonome et responsable. À cet égard, il prend également en compte la recherche d'efficacité, la confidentialité et la protection de la sphère privée en vue d'atteindre la prospérité économique. Afin de faciliter la poursuite du développement et l'innovation technique, le cadre de cybersécurité est technologiquement neutre. Il se base sur une sélection de normes, de directives et de bonnes pratiques existantes.

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

1. *Identifier (Identify)*
2. *Protéger (Protect)*
3. *Détecter (Detect)*
4. *Réagir (Respond)*
5. *Rétablir (Recover)*

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

5.2 Implémentation des « *Tiers* »

Le *NIST Framework* comprend 4 niveaux, *appelés Implementation Tiers.* Ils décrivent le niveau de protection qu'une entreprise a mis en place. Ces niveaux vont de partiel *(Tier 1)* à dynamique *(Tier 4).* Pour déterminer son niveau de protection, une entreprise doit parfaitement connaître ses pratiques de gestion des risques, son infrastructure, son architecture IT/OT, le genre de menaces possibles, les exigences légales et réglementaires, ses objectifs commerciaux et ses besoins organisationnels.

Tier 0 : pas mis en œuvre

Bien que l'organisation soit consciente que la mesure considérée devrait en fait déjà être réalisée depuis longtemps, elle n'a encore rien entrepris.

Tier 1 : partiellement mis en œuvre

Le niveau 1 signifie que les processus de gestion des risques ainsi que les exigences organisationnelles pour la sécurité des TIC ne sont pas formalisés (pas de règles fixées). Les risques informatiques sont généralement gérés au jour le jour, en mode réactif. Il existe un programme intégré pour gérer les risques au niveau organisationnel, mais on n'a pas instauré une véritable prise de conscience des risques informatiques ou une approche globale pour y faire face dans l'entreprise. Cette dernière ne dispose généralement pas de processus pour relayer en son sein les informations sur la cybersécurité. Il en va de même pour les autres risques informatiques, l'entreprise n'a le plus souvent pas prévu de processus standardisés pour communiquer ou coordonner ses activités avec ses partenaires externes.

Tier 2 : conscient des risques

Les entreprises qui optent pour un classement au niveau 2 disposent généralement de processus pour gérer leurs risques informatiques. Cependant, ces programmes ne sont pas concrètement appliqués ni obligatoires. Au niveau organisationnel, les risques informatiques sont intégrés dans un système de gestion global et tous les niveaux de l'entreprise ont été sensibilisés aux risques informatiques. On enregistre généralement dans l'entreprise un manque de volonté pour gérer et améliorer la sensibilisation aux risques informatiques, actuels et futurs. Les processus et méthodes approuvés sont définis et mis en œuvre. Les collaborateurs disposent de ressources suffisantes pour effectuer leurs tâches de cybersécurité. Les informations sur la cybersécurité sont partagées de manière informelle au sein de l'entreprise. Cette dernière est consciente de son rôle et n'hésite pas à communiquer avec ses partenaires externes (clients, fournisseurs, prestataires de services, etc.) sur les questions de cybersécurité. Il n'existe cependant aucun processus standardisé pour collaborer ou échanger des informations avec ces partenaires.

Tier 3 : reproductible

Les entreprises de niveau 3 ont formellement validé leurs plans pour gérer les risques et leurs instructions pour les faire appliquer en leur sein. La gestion des risques informatiques est définie dans les directives de l'entreprise. Les risques informatiques sont standardisés et les directives pour y remédier font l'objet de mises à jour régulières. Cette pratique tient compte des nouveaux besoins de l'entreprise, des progrès technologiques et d'un environnement où les menaces sont mouvantes, que ce soit à cause de nouveaux acteurs ou d'une nouvelle législation.

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

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

Tier 4 : dynamique

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

n/a : pas de réponse

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

5.3 Profils

Un profil est le résultat de l'ajustement aux standards, aux directives et aux bonnes pratiques du *Cybersecurity Framework,* conjugué à un scénario d'implantation individuel. Les profils peuvent servir à identifier les meilleures options d'amélioration au regard de la cybersécurité, par exemple en comparant un profil réel et un profil souhaité (voir Figure 15). L'outil d'évaluation fourni avec la présente norme minimale de sécurité numérique sert précisément à paramétrer un tel profil. L'évaluation des 106 activités répertoriées dans le questionnaire donne des résultats agrégés d'après les cinq fonctions du *Cybersecurity Framework* (identifier, protéger, détecter, réagir, récupérer). Le niveau minimal requis est réputé atteint lorsque la « cote globale de l'évaluation de la cybersécurité » indique des valeurs (sous rubrique « réalité ») correspondant au moins aux valeurs minimales requises (sous rubrique « cible »). Les instructions concernant le mode opératoire sont intégrées à l'outil d'évaluation.

Exemple d'évaluation de la cybersécurité

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

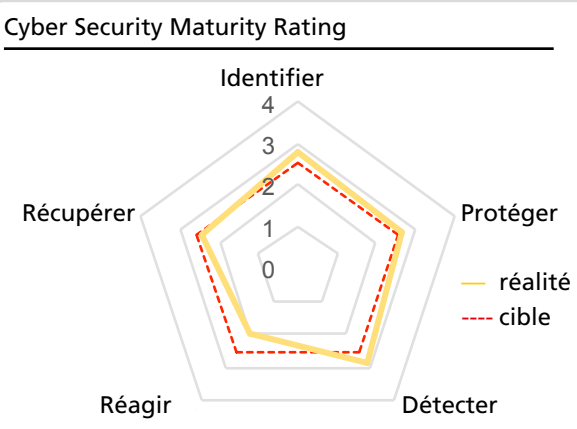

Figure 15 : Exemple de cote globale de l'évaluation de la cybersécurité

5.4 Identifier – *Identify*

5.4.1 Inventaire et organisation – *Asset Management*

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

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

Tableau 3 : Tâches ID.AM

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

Tableau 4 : Références ID.AM

5.4.2 Environnement de l'entreprise – *Business Environment*

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.

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

Tableau 5 : Tâches ID.BE

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

Tableau 6 : Références ID.BE

5.4.3 Règles – *Governance*

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

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

Tableau 7 : Tâches ID.GV

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

Tableau 8 : Références ID.GV

5.4.4 Analyse de risque – *Risk Assessment*

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

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

Tableau 9 : Tâches ID.RA

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

Tableau 10 : Références ID.RA

5.4.5 Stratégie pour gérer les risques – *Risk Management Strategy*

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

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

Tableau 11 : Tâches ID.RM

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

Tableau 12 : Références ID.RM

5.4.6 Gestion des risques liés à la chaine d'approvisionnement – *Supply Chain Risk Management*

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

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

Tableau 13 : Tâches ID.SC

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

Tableau 14 : Références ID.SC

5.5 Protéger – *Protect*

5.5.1 Gestion des accès – *Access Control*

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

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

Tableau 15 : Tâches PR.AC

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

Tableau 16 : Références PR.AC

5.5.2 Sensibilisation et formation – *Awareness and Training*

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

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

Tableau 17 : Tâches PR.AT

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

Tableau 18 : Références PR.AT

5.5.3 Sécurité des données – *Data Security*

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

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

Tableau 19 : Tâches PR.DS

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

Tableau 20 : Références PR.DS

5.5.4 Règles de protection des données – *Information Protection Processes and Procedures*

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

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

Tableau 21 : Tâches PR.IP

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

Tableau 22 : Références PR.IP

5.5.5 Maintenance – *Maintenance*

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

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

Tableau 23 : Tâches PR.MA

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

Tableau 24 : Références PR.MA

5.5.6 Technologie de protection – *Protective Technology*

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

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

Tableau 25 : Tâches PR.PT

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

Tableau 26 : Références PR.PT

5.6 Détecter – *Detect*

5.6.1 Anomalies et incidents – *Anomalies and Events*

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

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

Tableau 27 : Tâches DE.AE

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

Tableau 28 : Références DE.AE

5.6.2 Surveillance – *Security Continuous Monitoring*

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

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

Tableau 29 : Tâches DE.CM

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

Tableau 30 : Références DE.CM

5.6.3 Processus de détection – *Detection Processes*

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

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

Tableau 31 : Tâches DE.DP

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

Tableau 32 : Références DE.DP

5.7 Réagir – *Respond*

5.7.1 Plan d'intervention – *Response Planning*

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

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

Tableau 33 : Tâches RS.RP

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

Tableau 34 : Références RS.RP

5.7.2 Communication – *Communication*

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

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

Tableau 35 : Tâches RS.CO

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

Tableau 36 : Références RS.CO

5.7.3 Analyse – *Analysis*

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

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

Tableau 37 : Tâches RS.AN

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

Tableau 38 : Références RS.AN

5.7.4 Circonscrire les dommages – *Mitigation*

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

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

Tableau 39 : Tâches RS.MI

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

Tableau 40 : Références RS.MI

5.7.5 Améliorations – *Improvements*

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

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

Tableau 41 : Tâches RS.IM

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

Tableau 42 : Références RS.IM

5.8 Récupérer – *Recover*

5.8.1 Plan de restauration – *Recovery Planning*

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

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

Tableau 43 : Tâches RC.RP

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

Tableau 44 : Références RC.RP

5.8.2 Améliorations – *Improvements*

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

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

Tableau 45 : Tâches RC.IM

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

Tableau 46 : Références RC.IM

5.8.3 Communication – *Communication*

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

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

Tableau 47 : Tâches RC.CO

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

Tableau 48 : Références RC.CO

6 Conclusion

L'approvisionnement des réseaux thermiques est une tâche particulièrement complexe dû notamment à sa diversité. Les sources d'énergies ainsi que les processus industriels utilisés pour chauffer les conduits thermiques sont multiples et chacun apporte son lot de spécificités. Actuellement, les réseaux thermiques dont l'utilisation principale consiste à chauffer des bâtiments ne couvrent pas un grand pourcentage des besoins en chaleur du pays. Cependant, cette situation peut évoluer en se basant sur les changements sociaux et politiques de ces dernières années. En effet, les énergies renouvelables devront à terme remplacer complètement les énergies fossiles ce qui pourrait considérablement favoriser le développement des réseaux thermiques. De plus, ce secteur est en interaction avec une multitude d'autres secteurs industriels. Il faut concevoir les réseaux thermiques comme faisant partie d'un ensemble profitant de synergies globales et non pas comme un secteur isolé. En effet, une grande partie de la production de chaleur qui alimente les conduits thermiques provient d'autres activités industrielles créant ainsi une relation de dépendance vis-à-vis de l'activité productrice de chaleur ou de l'organisation qui en a la charge. Il est donc nécessaire de prendre en compte la totalité du processus d'approvisionnement et ne pas se limiter à celui des réseaux thermiques.

Comme pour la majorité des activités industrielles, les réseaux thermiques utilisent différents systèmes TIC pour gérer de manière efficiente leurs installations. Cependant, la défaillance de ces derniers peut avoir des répercussions considérables sur le bon fonctionnement des réseaux thermiques suisses et par conséquence impacter directement l'approvisionnement en chaleur du pays. Afin de maintenir un niveau de protection acceptable de ces infrastructures, il est nécessaire de protéger convenablement ces systèmes TIC. Pour ce faire, il est recommandé d'implémenter la présente norme minimale TIC, élaborée en collaboration entre l'OAFE, RETS et la SSIGE, et qui a pour objectif d'augmenter le niveau de résilience du secteur suisse des réseaux thermiques et ainsi de garantir son approvisionnement en cas de dysfonctionnements liés aux TIC.

Pour atteindre un niveau de sécurité adéquat, la norme minimale TIC analyse la composition, le processus d'approvisionnement et les activités critiques spécifiques au secteur des réseaux thermiques. Cette analyse permet d'identifier les éléments primordiaux des infrastructures thermiques afin de les protéger correctement. En ce qui concerne le programme de sécurité à appliquer, la norme minimale TIC se base sur le *NIST Framework Core* qui combine trois principaux aspects.

- Le premier est son approche basée sur le risque. Elle permet ainsi à chaque organisation de définir par elle-même sa sensibilité aux risques, les mesures à prendre pour réduire ces risques et leur ordre de priorité. De ce fait, chaque entreprise peut contrôler et adapter sa cybersécurité selon ses besoins.
- Le deuxième est la stratégie de *defense-in-depth*. Ce concept basé sur une défense à plusieurs niveaux permet de combiner plusieurs mesures de sécurité et ainsi protéger plus efficacement les équipements TIC.
- Le dernier aspect de ce programme de sécurité est les mesures du *NIST Framework Core*.

La présente norme minimale TIC propose un outil d'évaluation Excel[78] basé sur ces mesures, qui permet aux entreprises des réseaux thermiques de fortifier la résilience de leurs processus informatisés. À travers l'outil d'évaluation, cette norme minimale TIC permet aux acteurs de ce secteur de relever leur niveau de sécurité de façon systématique et d'atteindre un niveau de sécurité minimum suffisamment élevé et homogène. La mise en œuvre de la norme minimale TIC repose sur une méthode efficace qui a déjà fait ses preuves. D'autres secteurs d'approvisionnement, comme celui de l'électricité ou de l'eau potable, utilisent les mêmes procédés, ce qui favorise les effets de synergie, notamment pour les sociétés responsables de plusieurs domaines.

La cybersécurité n'est pas considérée ni abordée comme un état, mais comme un processus dynamique. La sécurité des systèmes TIC n'est jamais acquise. Elle constitue un objectif permanent qui doit faire l'objet de contrôles réguliers et d'un processus d'amélioration continue. La norme minimale TIC pour garantir l'approvisionnement des réseaux thermiques sert de guide afin de mettre en œuvre ce processus et ainsi atteindre cet objectif.

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

7 Annexes

7.1 Processus d'approvisionnement selon les différents processus industriels

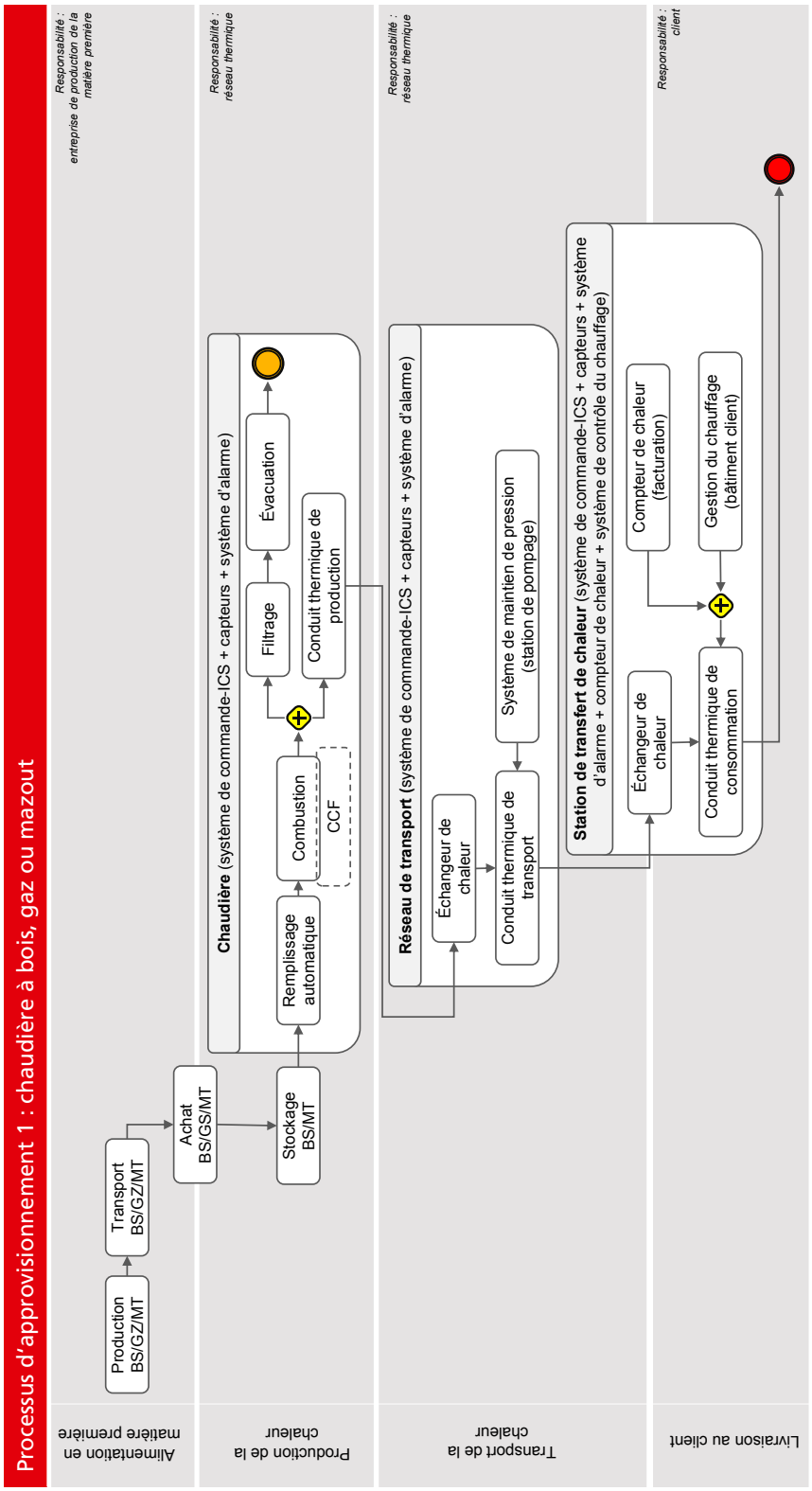

Figure 16 : Processus d'approvisionnement des chaudières

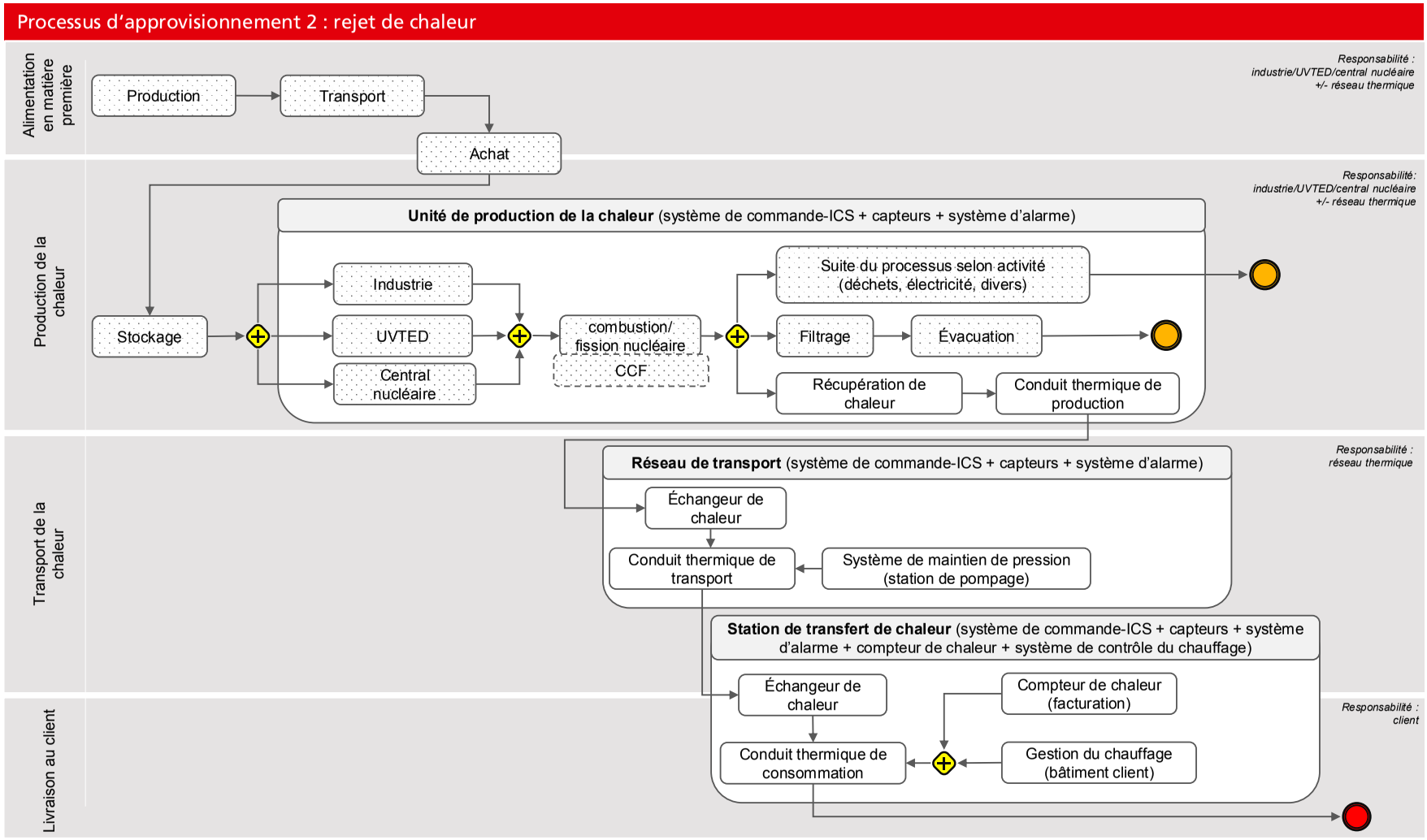

Figure 17 : Processus d'approvisionnement des rejets de chaleur

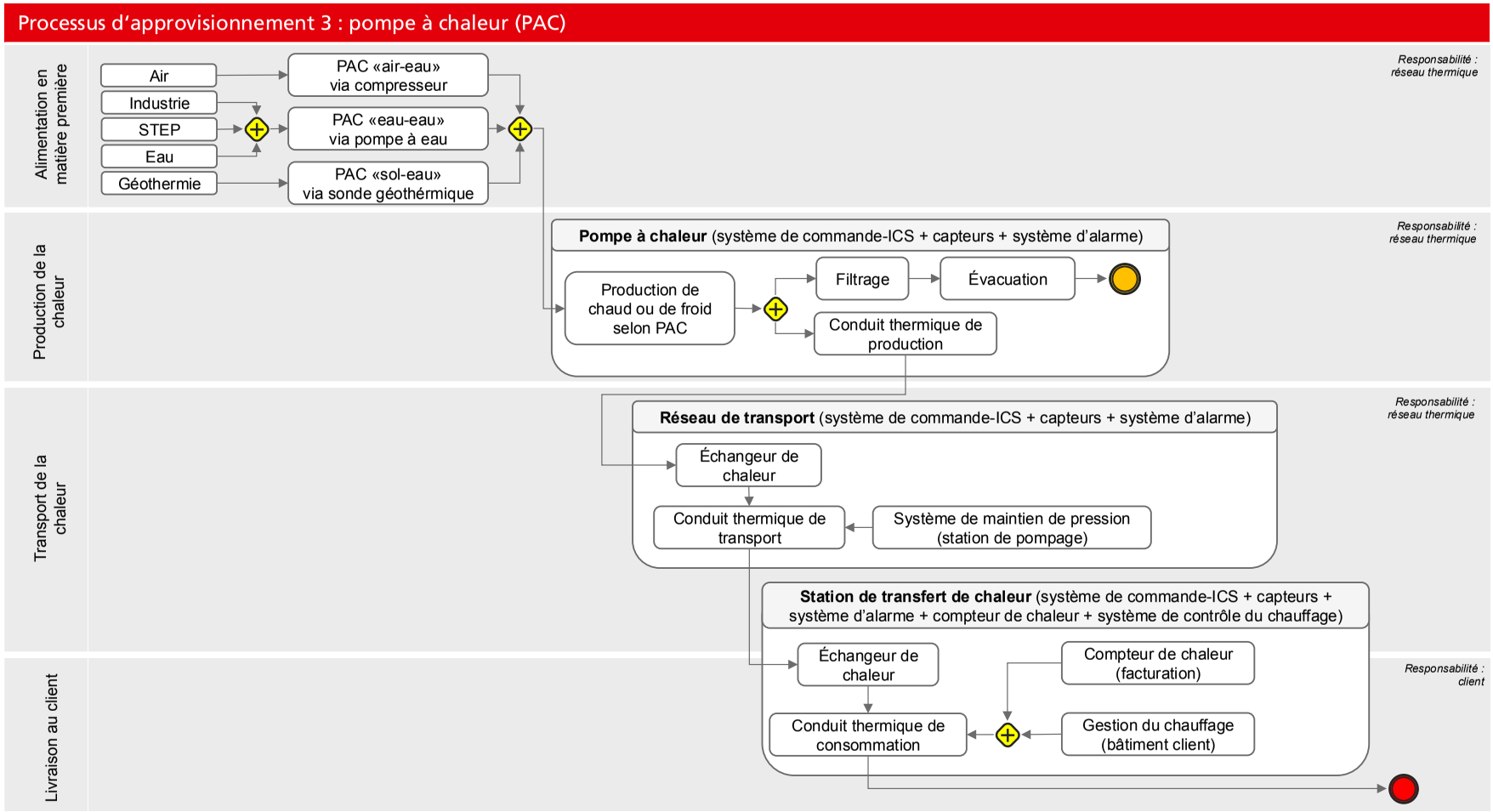

Figure 18 : Processus d'approvisionnement des pompes à chaleur

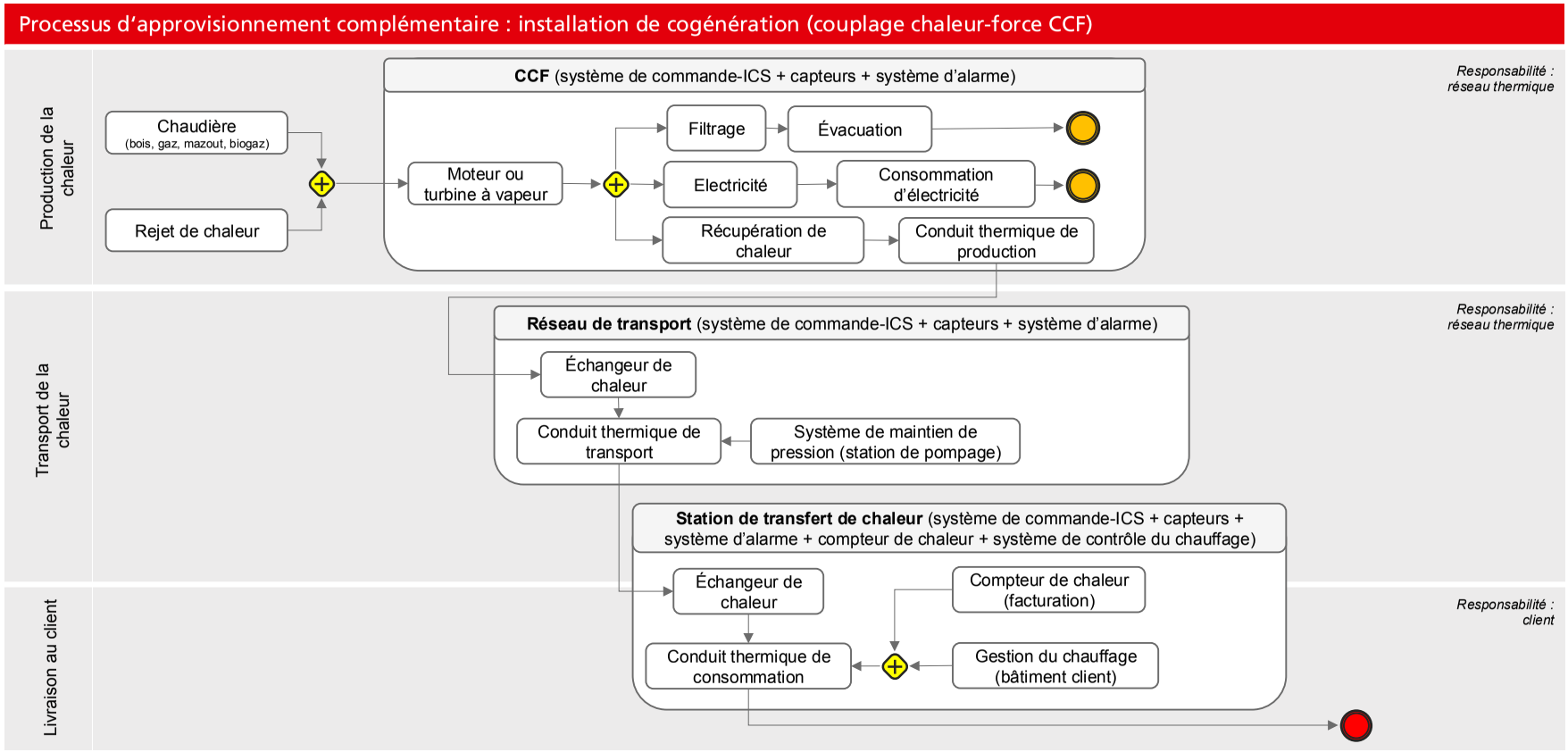

Figure 19 : Processus d'approvisionnement complémentaire sur le couplage chaleur-force

7.2 Dépendance entre différents secteurs industriels

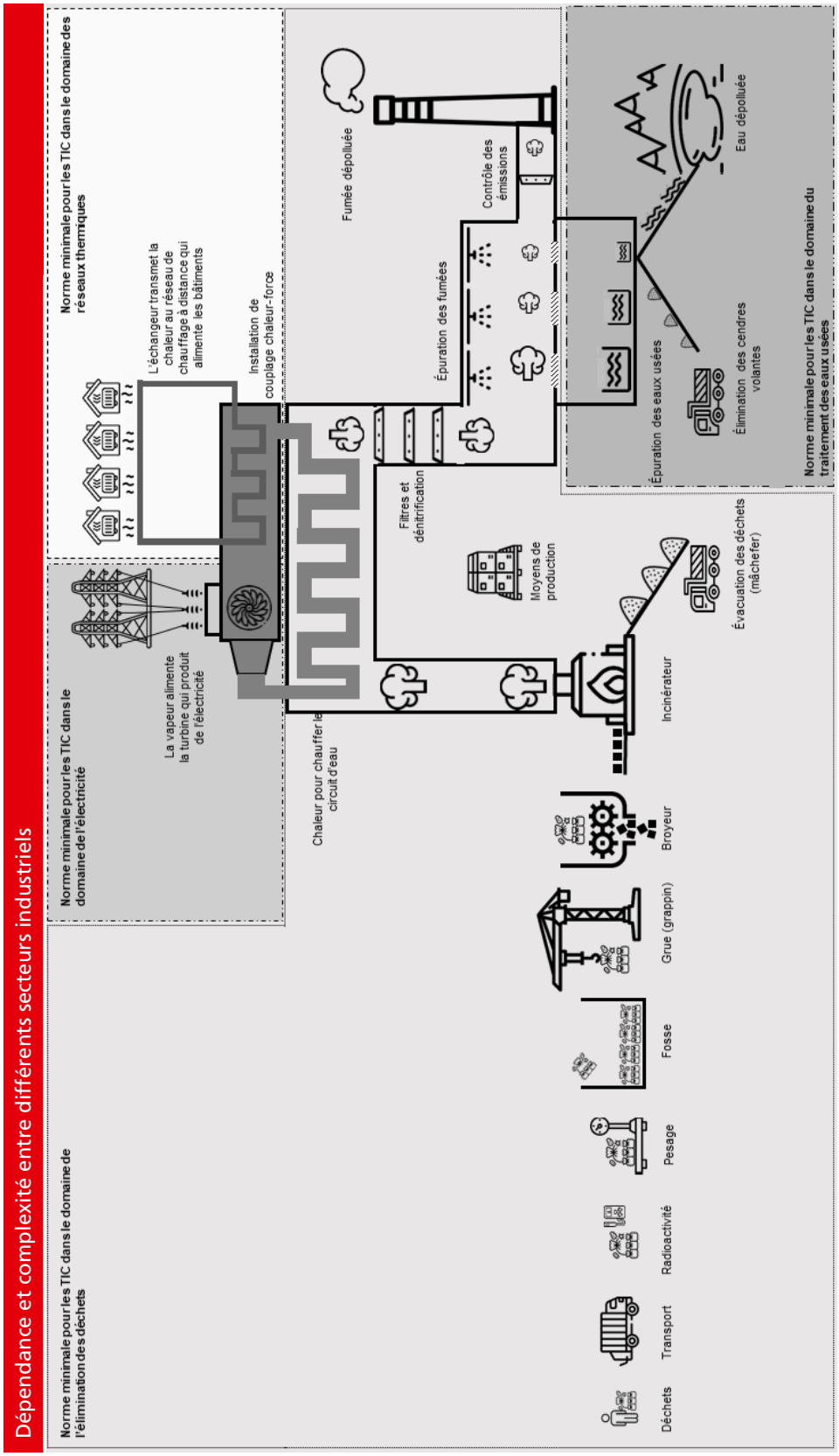

Figure 20 : Dépendances entre UVTED, réseau thermique, électricité et eau usée

Activités critiques et systèmes TIC associés

		Activités critiques	Systèmes TIC	*Safety*	Pyramide de l'automatisation	Remarques concernant l'activité
Organisationnel (*administratif*)		Infrastructure de télécommunication et service de communication	VoIP, EDI, Internet, e-mail, mobile, etc.			Permet d'avoir accès aux services de communication afin de communiquer avec l'ensemble des parties prenantes internes ou externes de l'organisation
		Gestion des tâches quotidiennes intégrées	ERP		Niveau 5 ERP	Optimise l'exécution des tâches quotidiennes de l'organisation mais nécessite d'être connecté à l'ensemble des systèmes TIC (système nerveux central d'une organisation)
		Facteur humain	Tous les systèmes TIC			Impacte l'ensemble des installations et des systèmes et peut par négligence ou malveillance causer des défaillances
Opérationnel (*industriel*)	Gestion globale	Gestion de l'ensemble du processus opérationnel des réseaux thermiques	Système de commande - ICS	*Safety*	Niveau 3 SCADA/HMI	Surveille, acquière, contrôle, et analyse l'ensemble du processus industriels (cœur de la partie opérationnelle d'une organisation)
		Protection physique des ICS				Dispersé sur plusieurs kilomètres, les ICS peuvent se retrouver dans des bâtiments non-protégés permettant ainsi d'accéder physiquement à certains systèmes ou installations
		Transmission des données provenant des capteurs			Niveau 1 Capteurs-actionneurs	Transmet les données des installations industriels au système de commande afin qu'il puisse les interpréter
		Gestion du système d'alarme			Niveau 3 SCADA/HMI	Alerte les responsables en cas de dysfonctionnement afin qu'ils puissent réagir, contrôler et corriger
	Production	Gestion de l'alimentation des pompes à chaleur			Niveau 3 SCADA/HMI	Alimente les pompes à chaleur en chaleur grâce à un compresseur à air, une pompe à eau ou une sonde géothermique
		Gestion de la production de chaleur (chaudières et pompes à chaleur)			Niveau 3 SCADA/HMI	Commande les unités de production de chaleur selon les processus industriels des chaudières et des pompes à chaleur
		Gestion de la récupération de chaleur			Niveau 3 SCADA/HMI	Récupère la chaleur produite par une autre activité industrielle afin d'alimenter le réseau thermique
		Gestion de la dépendance des rejets de chaleur			Niveau 4 MES	Dépendances organisationnelles et opérationnelles vis-à-vis d'une autre entreprise productrice de chaleur
	Transport	Gestion des systèmes de maintien de la pression			Niveau 3 SACADA/HMI	Maintien d'un niveau de pression optimal dans l'ensemble du réseau thermique afin de faire circuler la chaleur jusqu'à son point de consommation

Figure 21 : Activités critiques

7.4 Références, documents et normes

7.4.1 Documents normatifs

Le présent document tient compte des concepts, recommandations et mesures de diverses normes et autres documents normatifs (Tableau 49).

Titre	Année	Éditeur(s) et description
Stratégie nationale pour la protection des infrastructures critiques (PIC)	2012	Éd. : **Office fédéral de la protection de la population (OFPP)** La stratégie nationale PIC définit le champ d'application, désigne les infrastructures critiques et fixe les principes directeurs de la PIC. Elle s'adresse à tous les services assumant des responsabilités dans ce domaine, en particulier aux différentes autorités compétentes, aux responsables politiques et aux exploitants d'infrastructures critiques.
Mesures de protection des systèmes de contrôle industriels (SCADA/ICS)	2013–2020	Éd. : **Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI (2013) – Centre national pour la cybersécurité NCSC (2020)** Basées sur des documents américains de l'Industrial Control Systems Cyber Emergency Response Team (SCADA-CERT) 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 SCADA.
Guide pour la protection des infrastructures critiques (Guide PIC)	2015–2018	Éd. : **Office fédéral de la protection de la population (OFPP)** Le guide PIC constitue un instrument d'analyse et, le cas échéant, d'amélioration de la résilience des infrastructures critiques. Il est notamment conçu pour être utilisé dans des sous-secteurs critiques par les exploitants, les associations sectorielles et les autorités compétentes. Ce guide propose pour l'essentiel une procédure en matière de gestion des risques : analyse (identification des ressources, vulnérabilités, risques), évaluation, mesures (définition, mise en œuvre, contrôle et amélioration). Cette procédure peut tout à fait, voire devrait être intégrée aux processus de gestion existants ou être exécutée sur la base de ces derniers.
Loi fédérale sur l'approvisionnement économique du pays **(loi sur l'approvisionnement du pays, LAP ; RS 531)**	2016	Éd. : **Assemblée fédérale de la Confédération helvétique** Cette loi régit les mesures visant à garantir l'approvisionnement du pays en biens et services vitaux lors d'une pénurie grave à laquelle les milieux économiques ne peuvent pas faire face par leurs propres moyens. La Confédération peut encourager, dans les limites des crédits autorisés, des mesures prises par des entreprises de droit privé ou public pour garantir l'approvisionnement économique du pays, si ces mesures contribuent à renforcer substantiellement les préparatifs nécessaires pour garantir les systèmes d'approvisionnement et infrastructures vitaux en cas de pénurie grave. La présente norme minimale TIC de sécurité numérique constitue l'une de ces mesures.

Tableau 49 : Publications de la Confédération helvétique, des services administratifs et des associations constituant des références importantes pour ce document

Titre	Année	Éditeur(s) et description
Stratégie nationale de protection de la Suisse contre les cyber-risques (SNPC)	2018	Éd. : **Unité de pilotage informatique de la Confédération (UPIC)** Vu l'intérêt majeur que revêt la protection des infrastructures informatiques contre les cyberrisques pour la Suisse, le Conseil fédéral a chargé l'UPIC d'élaborer une stratégie nationale visant à protéger notre pays contre de tels risques. La SNPC a pour but de dresser un panorama actuel des cyberrisques et de recenser les moyens dont dispose la Suisse pour y faire face, où se situent les lacunes et comment y remédier le plus efficacement possible. La SNPC identifie les structures existantes et définit des objectifs assortis de mesures ad hoc (analyses des risques et des vulnérabilités d'un sous-secteur, p. ex.).

Tableau 49 : Publications de la Confédération helvétique, des services administratifs et des associations constituant des références importantes pour ce document

7.4.2 Normes internationales

Le tableau 50 répertorie les normes internationales qui ont été partiellement prises en compte dans la présente norme.

Titre	Année	Éditeur(s) et description
BSI-Standard 100-4 Notfallmanagement	2009	Éd. : ***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 200-2 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/IEC 62443 ss. Réseaux industriels de communication – Sécurité dans les réseaux et les systèmes	2009–2013	Éd. : ***International Society of Automation (ISA)/International Electrotechnical Commission (IEC)*** Cette série compte treize normes de sécurité et spécifications techniques applicables aux systèmes d'automatisation de commande industriels (industrial automation and control systems, IACS). Les normes CEI 61508 ss. (principes fondamentaux régissant la sécurité des IACS), qui englobent le thème de la sécurité de l'information, couvrent de manière complète et indépendante la thématique des IACS. Quatre aspects ou niveaux de sécurité de l'information différents sont retenus : • les aspects généraux (concepts, terminologie, unités de mesure, etc.) : CEI 62443-1-x ; • la gestion de la sécurité informatique : CEI 62443-2-x ; • le niveau « système » : CEI 62443-3-x ; • le niveau « composants » : CEI 62443-4-x. À relever que cette série de normes couvre également l'architecture de réseau et l'architecture zonale, alors que d'autres normes ne le font pas, ou alors de manière moins détaillée. Cette série de normes est en train de devenir une prescription normative fondamentale dans le contexte des normes du CENELEC (EN 50126, entre autres) en matière de fiabilité, de disponibilité, de maintenabilité et de sécurité (FDMS).

Tableau 50 : Normes nationales et internationales relatives à la sécurité numérique

Titre	Année	Éditeur(s) et description
BSI ICS Security-Kompendium	2013	Éd. : ***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 SCADA. Les bases nécessaires à la compréhension des SCADA, 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 SCADA étant mises en lumière.
ISA/IEC 62264 ss. *Enterprise Control System Integration*	2013–2016	Éd. : ***International Society of Automation (ISA)/International Electrotechnical Commission (IEC)*** Série de 5 normes relatives à l'intégration des systèmes informatiques d'entreprise et de contrôle-commande.
ISO 27001:2013 *Information technology – Security techniques – Information security management systems – Requirements* + ISO 27002:2022 *Information security, cybersecurity and privacy protection – Information security controls*	2013–2022	Éd. : ***Organisation internationale de normalisation (ISO)*** Cette norme détaille les exigences relatives à un système de management de la sécurité de l'information (*Information Security Management System,* ISMS). La suite ISO 2700ss comprend une série de normes concernant la sécurité de l'information, Celles qui représentent un intérêt particulier pour notre domaine sont les suivantes : • 27000:2018 Vue d'ensemble et vocabulaire • 27001:2013 Exigences : principes de base avec contrôles et objectifs de contrôle en annexe • 27002:2022 Mesures de sécurité de l'information • 27003:2017 Lignes directrices pour la mise en œuvre • 27005:2018 Gestion des risques liés à la sécurité de l'information • 27019:2017 Mesures de sécurité de l'information pour l'industrie des opérateurs de l'énergie Largement appliquées à l'heure actuelle, les normes ISO 27000 ss. devraient s'imposer comme le principal cadre de référence dans les années à venir. Les observer aujourd'hui déjà constitue donc la bonne approche. Contrairement à d'autres normes ou cadres, elles ne sont pas trop détaillées, sont modulables et peuvent être continuellement améliorées et développées sur une longue période. Le ISMS et le contenu des mesures doivent être adaptés et mis en œuvre en tenant compte des spécificités du secteur.
Framework for Improving Critical Infrastructure Cybersecurity	2014	Éd. : ***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.
Guide to Industrial Control Systems (ICS) Security SP 800-82 Rev. 2	2015	Éd. : ***National Institute of Standards and Technology (NIST)*** Ce guide fournit une introduction complète aux SCADA, 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 SCADA, basés sur le cadre 800-53 du NIST, sont également présentés.

Tableau 50 : Normes nationales et internationales relatives à la sécurité numérique

Titre	Année	Éditeur(s) et description
Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies	2016	Éd. : ***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 *defense in depth* dans le cadre de la sécurité des systèmes de contrôle industriels.
Communication network dependencies for ICS/SCADA Systems	2017	Éd. : ***European Union Agency for Network and Information Security (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.
BSI-Standard 200-1 Managementsysteme für Informationssicherheit (ISMS)	2017	Éd. : ***Bundesamt für Sicherheit in der Informationstechnik (BSI)*** Cette norme décrit les méthodes, les tâches et les activités pertinentes qui font le succès d'un ISMS et précise les tâches qui incombent à la direction. La méthodologie de l'IT-Grundschutz, qui explique, pas à pas, comment développer un ISMS 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.
BSI-Standard 200-2 IT-Grundschutz-Methodik	2017	Éd. : ***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 Risikomanagement	2017	Hrsg.: **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.
ISO 22301:2019 Sécurité et résilience – Systèmes de management de la continuité d'activité – Exigences	2019	Éd. : **Organisation internationale de normalisation (ISO)** Cette norme détaille les exigences relatives aux systèmes de gestion de la continuité d'activité.

Tableau 50 : Normes nationales et internationales relatives à la sécurité numérique

Titre	Année	Éditeur(s) et description
BSI IT-Grundschutz-Kataloge *BSI-Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz* *BSI Zuordnungstabelle ISO 27001 sowie ISO 27002 und IT-Grundschutz*	2019	Éd. : ***Bundesamt für Sicherheit in der Informationstechnik (BSI)*** À l'aide des normes 200-1 à 200-3 et la 100-4 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 (ISMS). 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* développées 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. Les normes ISO laissent donc plus de place à l'interprétation et sont plus flexibles, mais elles fournissent aussi moins d'instructions et de soutien détaillés. C'est donc l'inverse qui s'applique à l'approche de la protection informatique de base. Comme son nom l'indique, elle offre une «protection de base». L'effort nécessaire pour obtenir une certification basée sur les normes ISO est moins important.
Mapping of Dependencies to International Standards (tableau de correspondance)	2020	Éd. : **Agence de l'Union européenne pour la cybersécurité (ENISA)** Ce rapport analyse les dépendances et les interactions entre les opérateurs de services essentiels (operators of essential services, OES) et les fournisseurs de services numériques (digital service providers, DSP), et propose une série d'indicateurs en vue de leur évaluation. Ces indicateurs sont mis en regard de normes et conditions-cadre internationales (ISO/CEI 27002, COBIT 5, mesures de sécurité du groupe de coopération SRI et *NIST Cybersecurity Framework*).
ISA/IEC 62351:2022 Gestion des systèmes de puissance et échanges d'informations associés – Sécurité des communications et des données	2022	Éd. : ***International Society of Automation (ISA)/International Electrotechnical Commission (IEC)*** Les normes IEC 62351 ss. décrivent le standard de sécurité pour les systèmes de gestion énergétique et l'échange de données énergétiques. Elles définissent les mesures visant à satisfaire aux quatre exigences de base en matière de communication et de traitement sécurisés des données.

Tableau 50 : Normes nationales et internationales relatives à la sécurité numérique

7.5 Glossaire

Abréviation	Description
AEP	Approvisionnement économique du pays
ASCAD	Association suisse du chauffage à distance (à partir de 2023 Réseaux Thermiques Suisse, RETS)
BSI	*Bundesamt für Sicherheit in der Informationstechnik* (Allemagne)
CCF	Couplage chaleur-force (installation de cogénération)
CEO-Fraud	Un ordre de paiement urgent mais factice est transmis par un pirate informatique se faisant passer pour membre de la direction qui souvent est injoignable à ce moment
DCS	*Distributed Control System*
DDC	*Direct Digital Control*
DMZ	*Demilitarized Zone* (zone démilitarisée), réseau informatique avec accès sécurisé (est souvent utilisé pour garantir une séparation logique entre deux zones de réseaux)
EDI	*Electronic Data Interchange*
ENISA	*European Union Agency for Network and Information Security*
ERP	*Enterprise Ressource Planning-System*
EWS	*Engineering Workstations*
Fake-sextortion	Un maître chanteur menace de divulguer des photos ou d'autres informations compromettantes
FINMA	Autorité fédérale de surveillance des marchés financiers
HMI	*Human Machine Interface*, organe ou action permettant la mise en contact d'un être humain avec une machine
ICS	*Industrial Control System*
IDS	*Intrusion Detection System*
IP	*Internet Protocol*
ISA	*International Society of Automation*
ISMS	*Information Security Management System* (système de management de la sécurité de l'information)
ISO	Organisation internationale de normalisation
IT	Technologie de l'information (Information Technology), ici en particulier Office-IT/bureautique/ adminstatif. Tout ce qui n'est pas OT.
MELANI	Centrale d'enregistrement et d'analyse pour la sûreté de l'information (Unité de pilotage informatique de la Confédération)
MES	*Manufacturing Execution System*

Tableau 51 : Glossaire

Abréviation	Description
NCSC	Centre national pour la cybersécurité
NIST	*National Institute of Standards and Technology*
OFAE	Office fédéral pour l'approvisionnement économique du pays
OFEN	Office fédéral de l'énergie
OFPP	Office fédéral de la protection de la population
OT	*Operational Technology* (en particulier systèmes SCADA)
PAC	Pompe à chaleur
Phishing	Les victimes sont amenées à divulguer leurs mots de passe et d'autres informations personnelles
PLC	*Programmable Logic Controller*
Ransomware	Les données sont cryptés et inaccessibles pour son propriétaire
Réseau thermique	Dénomination englobant à la fois le chauffage et le froid à distance
RETS	Réseaux Thermiques Suisse (auparavant Association suisse du chauffage à distance, ASCAD)
RTU	*Remote Terminal Unit*
SCADA	Supervisory Control and Data Acquisition, surveillance et pilotage des processus techniques. Le système SCADA intègre, outre la surveillance et le pilotage, les capteurs, les lignes, les ordinateurs et la centrale de télégestion du système (de production). Il s'agit en particulier des systèmes de préparation des livraisons, des systèmes de gestion de la production des transformateurs ainsi que des systèmes d'encaissement des détaillants.
SNPC	Stratégie nationale de protection de la Suisse contre les cyber-risques
SSIGE	Société Suisse de l'Industrie du Gaz et des Eaux
STEP	Station d'épuration des eaux usées
TIC	Technologies de l'information et de la communication (traitement électronique des données TED)
TWh	Térawattheure
UPIC	Unité de pilotage informatique de la Confédération
UVTED	Usine de valorisation thermique et électrique des déchets
VoIP	*Voice-over-IP*
WAN	*Wide Area Network*

Tableau 51 : Glossaire

7.6 Liste des tableaux

7.7 Liste des figures

Auteurs et auteure de la première édition

Nom	Organisation	Fonction
Sven Peter	OFAE	Auteur principal/ responsable du projet
Stefan Güpfert	SSIGE	Co-auteur/expert/ assurance qualité
Andreas Hurni	RETS	Co-auteur/expert/ assurance qualité
Hans-Peter Käser	OFAE	Expert/assurance qualité
Karsten Reichart	SSIGE	Expert/assurance qualité
Stéphane Henry	OFEN	Expert/assurance qualité
Giorgio Ravioli	OFPP	Expert/assurance qualité
Alicia Kayser	ESB	Experte/assurance qualité
Andreas Willen	EBL	Expert/assurance qualité
Boris Wächter	Primeo Energie	Expert/assurance qualité
Marcel Kränzlin	AEW	Expert/assurance qualité
Michael Gauer	IWB	Expert/assurance qualité
Patrick Steiger	SWL	Expert/assurance qualité
Philippe Roten	ERZ	Expert/assurance qualité
Reto Schär	Localnet AG	Expert/assurance qualité
Dominik Noger	EASZ	Expert/assurance qualité

Impressum et contact

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

Associations consultées :
Réseaux Thermiques Suisse (RETS) – auparavant Association suisse du chauffage à distance (ASCAD)
Société Suisse de l'Industrie du Gaz et des Eaux (SSIGE)

Images de couverture :
Brugg Rohrsystem AG, SIG – Services Industriels de Genève, EBL (Genossenschaft Elektra Baselland)

Chronologie

Date	Intitulé raccourci
Février 2021	Prise de contact avec la SSIGE pour l'établissement de la norme minimale TIC pour le chauffage à distance
Mars 2022	Prise de contact avec RETS pour l'établissement de la norme minimale TIC pour le chauffage à distance
Juin 2021	Première réunion du groupe de travail
Décembre 2021	Indentification des activités critiques du secteur
Avril–Mai 2022	Élaboration de la version beta du document français et traduction en allemand
Juillet 2022	Validation de la version Beta et ajout des commentaires des experts
Septembre 2022	Relecture finale du document
Décembre 2022	Création du Design final du document
Février 2023	Publication de la norme minimale TIC pour le secteur du chauffage et du froid à distance

Ce document a été élaboré avec l'implication et le soutien de l'Office fédéral pour l'approvisionnement économique du pays (OFAE), de la Société Suisse de l'Industrie du Gaz et des Eaux (SSIGE), de Réseaux Thermiques Suisse (RETS) et d'experts de l'approvisionnement des réseaux thermiques.

Exclusion de responsabilité