Norme minimale pour la sécurité des technologies de l'information et de la communication (TIC) dans l'approvisionnement en gaz

G1008 Publication mai 2024

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Office fédéral de l'énergie OFEN

Office fédéral pour l'approvisionnement économique du pays OFAE

gaz energie

SVGW

Table des matières

Introduction

En 2014, une analyse des risques et de la vulnérabilité de l'approvisionnement en gaz naturel[1] a été menée conjointement par la Confédération et les exploitants gaziers et s'est concentrée sur les processus assurant l'approvisionnement en gaz des industries et de la population suisse. Cette analyse a, notamment, révélé une dépendance grandissante des systèmes TIC dans le processus d'approvisionnement en gaz. La numérisation croissante, notamment l'interconnections et l'automatisation des systèmes, a permis de gagner en efficacité mais a complexifié et rendu plus vulnérable le processus d'approvisionnement. En effet, la défaillance des systèmes TIC peut désormais avoir des répercussions conséquentes sur l'approvisionnement en gaz.

Afin de protéger convenablement le secteur du gaz suisse contre ces défaillances TIC, l'Office fédéral pour l'approvisionnement économique du pays (OFAE) ainsi que l'association professionnelle pour l'eau, le gaz et la chaleur (SVGW) ont conjointement élaboré la norme minimale TIC pour l'approvisionnement en gaz (recommandation G1008). Cette première version a été publiée en 2020 et se voulait être un cadre permettant aux exploitants gaziers d'évaluer eux-mêmes les cyberrisques encourus et de mettre en œuvre les mesures appropriées. Depuis, la situation s'est considérablement complexifiée. Le COVID, la guerre en Ukraine, les difficultés d'approvisionnement énergétique ou encore l'augmentation considérable des cyberattaques ont profondément modifié le visage de notre société. Afin de répondre à ce changement de contexte et à cette augmentation des cyberrisques, il a été décidé de remplacer la norme minimale TIC pour l'approvisionnement en gaz (recommandation G1008) par une nouvelle version plus contraignante.

Cette nouvelle version « norme minimale TIC pour l'approvisionnement en gaz 2.0 » a été élaborée en collaboration par l'Office fédéral pour l'approvisionnement économique du pays (OFAE), l'Office fédéral de l'énergie (OFEN), l'association suisse de l'industrie gazière (ASIG) et l'association pour l'eau, le gaz et la chaleur (SVGW). Contrairement à la version précédente qui se voulait être une recommandation, la présente norme a pour objectif d'être rendue obligatoire pour tous les exploitants gaziers d'installation de transport par conduite[2]. Afin de dresser un cadre efficace et adapté, trois niveaux de protection (A, B et C) ont été créés en se basant sur deux critères principaux : la pression du réseau ou des installations (bar) combinée à la longueur du réseau (km) ainsi que le volume de gaz transporté (GWh/an). Pour chaque niveau de protection, les cent huit mesures du *NIST Framework* (programme de cybersécurité) ont été minutieusement examinées et un niveau de maturité a été attribué à chacun d'elles. Chaque exploitant gazier doit, dès lors, atteindre les exigences qui lui ont été fixées selon le niveau de protection auquel il appartient. L'autorité de surveillance compétente s'assurera que les exigences définies soient respectées.

Le présent document est divisé en six chapitres. Le premier défini le champ d'application et les limites de ce document. Le deuxième introduit différents concepts permettant une meilleure compréhension des enjeux ainsi que des termes utilisés dans le cadre de cette norme minimale TIC. Le chapitre trois se concentre sur le secteur gazier en développant sa structure, ses processus TIC ainsi que l'évaluation de ses activités critiques. Le quatrième chapitre détaille les différentes parties du programme de cybersécurité de la norme minimale TIC qui est basée sur le *NIST Framework*. Le chapitre cinq se concentre sur les niveaux de protection et les exigences que chaque exploitant gazier d'installation de transport par conduite doit atteindre. Finalement, le chapitre six clôture ce rapport avec les annexes.

Il est également recommandé d'associer cette norme minimale TIC à l'outil d'évaluation Excel[3] de l'OFAE ainsi qu'au document d'accompagnement[4] ceci afin de simplifier respectivement, l'évaluation des différentes mesures du programme de cybersécurité et la compréhension de l'ensemble du programme de cybersécurité.

---

[1] Analyse des risques et de la vulnérabilité relative à l'approvisionnement en gaz naturel. Office fédéral pour l'approvisionnement économique du pays (OFAE), Berne 2014 (*n'existe qu'en allemand*).

[2] Rendu obligatoire par la révision de l'ordonnance concernant les prescriptions de sécurité pour les installations de transport par conduites (OSITC ; RS 746.12).

[3] Il s'agit du document Excel "IKT-Minimalstandard-Assessment.Tool" disponible sur le site de l'OFAE.

[4] Guide pour les exploitants de réseaux de gaz (en cours d'élaboration).

1 Champ d'application et délimitations

La présente norme minimale TIC se concentre sur les activités critiques et les processus TIC associés qui sont nécessaires pour l'approvisionnement de la Suisse en gaz. Elle associe, également, à chaque exploitant gazier d'installation de transport par conduite un niveau de protection (A, B ou C) selon des critères définis. Chaque niveau de protection définit des exigences spécifiques auxquelles le gestionnaire de réseau de gaz doit se conformer en fonction du niveau de maturité correspondant. Le champ d'application de ce document est défini comme suit :

Champ d'application

- Cette norme minimale TIC s'adresse à tous les exploitants d'installations de transport par conduites soumis à l'ordonnance sur la sécurité des installations de transport par conduites (OSITC ; RS 746.12).
- Les menaces liées aux TIC sont comprises de manière globale : elles vont des dégâts concrets aux cyberattaques à visée destructrice, en passant par la perte ou la manipulation de données. Les risques identifiés lors de l'analyse de vulnérabilité menée dans le cadre de la Stratégie nationale de protection de la Suisse contre les cyberrisques[5] sont particulièrement pris en compte. Outre les mesures techniques, la norme minimale TIC englobe aussi la formation des collaborateurs et la gouvernance afin d'améliorer la résilience des systèmes informatiques importants.
- La résilience des systèmes doit être améliorée et standardisée dans toute la branche. L'objectif du niveau minimal de protection doit permettre de limiter les effets d'un cyberincident (violation de la politique de sécurité d'un système qui affecte son intégrité, sa disponibilité ou sa confidentialité) sur l'approvisionnement en gaz.
- La norme se concentre principalement sur les systèmes ICS (en particulier SCADA), ERP[6] et les systèmes de communication des TIC qui permettent la surveillance des réseaux respectivement des installations de réseau. Cela comprend notamment les ordinateurs portables et fixes, les téléphones, les logiciels de maintenance, les interfaces SCADA, les imprimantes, le *Smart Metering*, les appareils interconnectés (*Internet of Things*) ou encore les réseaux et systèmes installés dans les bâtiments d'exploitation, dans la mesure où ceux-ci ne peuvent pas être opérés séparément du réseau gazier.
- Cette norme s'adresse à tous les exploitants gaziers d'installation de transport par conduite qui sont soumis à l'ordonnance sur la sécurité des installations de transport par conduites (OSITC ; RS 746.12).
- Chaque exploitant gazier doit, selon le niveau de protection auquel il est associé, atteindre les exigences définies au chapitre 5.2 de ce présent document.
- Ce document doit être implémenté par les exploitants gaziers soit en interne par des collaborateurs compétents soit à l'externe via une entreprise spécialisée.
- Les niveaux de protection (A, B et C) et les exigences correspondantes (niveau de maturité à atteindre pour chacune des mesures du *NIST Framework Core*) ont été définis par l'ASIG et la SVGW et ont été rendus obligatoire par la révision de l'ordonnance sur la sécurité des installations de transport par conduites (OSITC ; RS 746.12).
- Il incombe à l'autorité de surveillance compétente de vérifier la mise en application de cette norme minimale TIC par les exploitants gaziers d'installation de transport par conduite.

[5] Analyse des risques et de la vulnérabilité relative à l'approvisionnement en gaz naturel. Office fédéral pour l'approvisionnement économique du pays (OFAE), Berne 2014 (*n'existe qu'en allemand*).

[6] Système *Enterprise Ressource Planning* : 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.

Délimitation

- Le cas où une entreprise peut aussi faire fonctionner son système d'approvisionnement en gaz 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. Le fonctionnement manuel est essentiel pour les infrastructures critiques – l'arrêt contrôlé de l'infrastructure devrait au moins être possible à tout moment.
- Cette norme minimale pour les TIC se concentre sur les composantes TIC et leur forte dépendance à l'approvisionnement électrique. Sans électricité, les systèmes SCADA, la station de compression, le processus d'odorisation, la planification des besoins ainsi que les postes de comptage douaniers fonctionneraient uniquement manuellement, ce qui nécessiterait une capacité humaine importante. Il est recommandé de prévoir, pour chaque système d'approvisionnement, un plan d'urgence qui permette d'affronter une pénurie ou une panne électrique généralisée.
- Les mesures de la norme minimale TIC doivent être accompagnées des mesures techniques appropriées afin de garantir la sécurité des installations.
- Le présent document a été rédigés de bonne foi et avec le plus grand soin. L'OFAE, l'OFEN, la SVGW, l'ASIG, les experts et les entreprises ayant participé à son élaboration n'assument aucune garantie explicite ou implicite. Il incombe aux utilisateurs – et à eux seuls – d'assumer la responsabilité d'éventuels dommages et d'un bon fonctionnement. L'implémentation des mesures préconisées dans ce document ne garantit aucunement une cybersécurité infaillible. Il est, dès lors, recommandé d'aller au-delà de cette norme afin de se protéger de manière optimale.
- Les clients finaux qui ne distribuent ou ne transportent pas de gaz pour des tiers ne sont pas concernés par cette présente norme minimale TIC.

2 Analyse de la situation et du contexte

L'évolution du monde numérique a permis l'essor des technologies de l'information et de la communication (TIC). Les entreprises industrielles sont de plus en plus nombreuses à automatiser et interconnecter leurs systèmes de contrôle industriel (ICS[7]). La digitalisation optimise la productivité et simplifie l'exécution des tâches quotidiennes, mais fragilise aussi la fiabilité et la sécurité des systèmes industriels. L'objectif de la norme minimale TIC pour l'approvisionnement en gaz 2.0 est d'améliorer la cybersécurité des infrastructures gazières afin de garantir l'approvisionnement de la Suisse en gaz.

2.1 L'évolution des systèmes de contrôle industriel (ICS)

Pour les entreprises industrielles, un système de contrôle industriel (ICS) est primordial car il contrôle le cœur de leurs activités. Un ICS est composé de plusieurs éléments de contrôle pouvant être électriques, mécaniques, hydrauliques ou encore pneumatiques qui interagissent ensemble afin d'atteindre un objectif commun, comme par exemple, la gestion du transport du gaz. La tâche d'un ICS consiste à collecter des données provenant de processus variables ou des statuts de machines industrielles et à contrôler des machines sur place ou à distance[8]. Le terme ICS est générique et englobe plusieurs types de systèmes de contrôle dont les systèmes de contrôle et d'acquisition de données (SCADA)[9] particulièrement utilisés dans la distribution industrielle (y compris pour le transport du gaz). La spécificité d'un système SCADA est sa capacité à effectuer des contrôles opérationnels sur de longues distances en utilisant les ondes radio, la transmission satellite, le réseau téléphonique ou encore le réseau WAN[10]. Un système SCADA permet le contrôle à distance de 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[11].

2.2 La convergence entre les technologies de l'information (IT) et les technologies opérationnelles (OT)

Au sein des technologies de l'information et de la communication (TIC), il existe deux sous-catégories qui ont longtemps été distinctement séparées, mais qui depuis plusieurs années convergent l'une vers l'autre. Il s'agit des technologies de l'information (*Information Technology,* IT) et des technologies opérationnelles (*Operational Technology*, OT). La première regroupe l'ensemble des systèmes informatiques qui soutient le travail quotidien d'une entreprise (e-mail, imprimantes, téléphonie, etc.). Quant à la deuxième, elle est utilisée pour le travail opérationnel lié aux processus industriels d'une organisation et nécessaire au bon fonctionnement des ICS (capteurs, thermomètres, machines industrielles, etc.). Afin de réduire les coûts et d'améliorer le fonctionnement des ICS, les technologies opérationnelles ont commencé à fusionner avec les technologies de l'information. Cette convergence entre IT et OT a permis de connecter et d'automatiser les systèmes industriels. De ce fait, il est désormais possible de contrôler à distance les équipements OT, sur lesquels sont implémentés les ICS, grâce aux protocoles de communication IT standard. Les ICS gagnent donc en productivité au détriment de la sécurité en s'exposant aux menaces extérieures provenant des équipements IT[12]. L'objectif de la norme minimale TIC est donc de sécuriser convenablement l'ensemble des équipements TIC et de s'assurer que les ICS sont correctement protégés face à ces « nouveaux » risques.

---

[7] ICS : *Industrial Control System* (système de control industriel).

[8] National Institute of Standards and Technology. "*Glossary: industrial control system ICS*".

[9] 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*.

[10] 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.

[11] National Institute of Standards and Technology. "*Glossary: Supervisory Control and Data Acquisition SCADA*".

[12] Balmelli, Laurent. « Build a Cyber Security Program for Industrial Control Systems ». *Medium*, 14 février 2020.

2.3 La dépendance du secteur gazier aux TIC

En Suisse, le gaz est principalement utilisé comme énergie thermique permettant le fonctionnement de certaines industries mais servant également de chauffage pour les particuliers. Le processus d'approvisionnement de la Suisse en gaz implique quatre étapes principales : l'acquisition, le transport, la distribution et la consommation. Comme le Suisse ne dispose pas d'extraction gazière, le pays est tributaire des importations de l'étranger. Le gaz est acheminé en Suisse par un vaste réseau de gazoducs (environ 190'000km de réseau de transport longue distance). La position géographique centrale de la Suisse au sein de l'Europe lui permet d'être approvisionnée par plusieurs axes (Genève, Bâle, Thurgovie ou encore St-Gall). De plus, la Suisse joue un rôle-clé dans le réseau européen par le biais de la station de compression de Ruswil qui permet au gaz de franchir les Alpes et d'approvisionner l'Italie ou l'Allemagne selon les besoins.

Le réseau suisse de pipelines est principalement géré par des systèmes de contrôle et d'acquisition de données (SCADA) utilisant un grand nombre de capteurs et offrant la possibilité de surveiller, collecter, analyser et administrer le réseau. Les systèmes SCADA permettent, par exemple, de contrôler à distance l'ensemble des postes de détente et de comptage (PDC) dont le but est de réduire la pression afin d'acheminer le gaz mesuré jusqu'à son point de consommation. En cas de panne des systèmes SCADA, la gestion du réseau de transport ne serait plus assurée car les entreprises responsables n'auraient plus de visibilité sur le réseau et ne pourraient plus intervenir à distance. Outre les systèmes SCADA, les outils de communication comme la messagerie électronique, les terminaux mobiles, la VoIP, voire la radio, sont essentiels pour les exploitants gaziers. Sans ces instruments, ils ne sont plus en mesure de communiquer efficacement avec des installations décentralisées et de remédier à leurs dysfonctionnements.

2.4 L'intensification des cyberattaques

Le monde numérique a révolutionné l'univers industriel en rendant les systèmes de contrôle plus intelligents, interconnectés et donc plus productifs mais en contrepartie, il l'a exposé à de nouvelles menaces. Tous les secteurs sont touchés par des cyberattaques, y compris celui du gaz. 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 exploitants gaziers sont de plus en plus nombreux à connecter leurs systèmes de commande à l'Internet pour des raisons économiques ou pour gagner en flexibilité grâce à la télésurveillance. Cela entraîne de nouveaux types de vulnérabilité, ces failles pouvant, par exemple, être exploitées par des pirates pour voler des données, utiliser des ressources TIC externes voire prendre le contrôle d'infrastructures critiques. En cas d'attaque de *ransomware*, par exemple, les réseaux informatiques ou les systèmes de contrôle sont bloqués et ne sont libérés que contre le paiement d'une rançon. Ces attaques produisent des dommages colossaux et des pertes financières importantes.

Les grandes entreprises pétrolières et gazières américaines ont fait face à ces menaces. En avril 2018, par exemple, le système EDI (échange de données informatisées) qui traite les transactions clients au sein du réseau de pipelines d'une importante entreprise américaine (*Energy Transfer Partners*), a été paralysé par une cyberattaque. Cependant, *Energy Transfer* a affirmé que cette panne n'a pas affecté son travail, l'entreprise ayant réussi à compenser la perte de ce logiciel avec des ressources internes[13]. Début 2018, un groupe de « hacker » a piraté un ICS (*industrial control systems*) principalement utilisé par les entreprises nucléaires, pétrolières et gazières, par les biais du logiciel malveillant « Triton ». L'entreprise ciblée par l'attaque ne s'est rendu compte de la situation que lorsque les pirates ont essayé de reprogrammer certains capteurs, déclenchant ainsi le mode sécurité du système et son arrêt automatique, ce qui a permis à l'entreprise d'éviter le piratage complet des installations[14]. Ces exemples démontrent que de telles menaces sont bel et bien réelles. Afin de limiter au maximum ces risques, les systèmes TIC requis pour l'approvisionnement en gaz doivent présenter un niveau de sécurité élevé. L'instauration d'une norme obligatoire en matière de cybersécurité permet aux exploitants gaziers d'optimiser la protection de leurs systèmes TIC et d'améliorer leur protection en continu.

[13] Digital Guardian. "*Gas Pipeline Company Recovers From Cyberattack*", 5 avril 2018.

[14] The Guardian. « *Triton: hackers take out safety systems in 'watershed'* attack on energy plant", 15 décembre 2017.

2.5 Identification des activités critiques

La norme minimale TIC pour l'approvisionnement en gaz 2.0 repose sur des bases concrètes et éprouvées comme le *NIST Framework Core*[15] et l'analyse des risques et de la vulnérabilité de l'approvisionnement en gaz naturel, menée par l'OFAE[16]. La norme minimale TIC permet de garantir une méthode uniforme débouchant sur des résultats comparables au sein de la branche et d'optimiser le niveau de sécurité des systèmes TIC requis pour l'approvisionnement en gaz.

Afin de protéger plus efficacement les différents secteurs jugés critiques pour l'approvisionnement du pays, toutes les normes minimales TIC « spécifiques à un secteur » se basent sur le même programme de cybersécurité et préconisent les mêmes mesures de sécurité. De ce fait, la norme minimale TIC pour l'approvisionnement en gaz 2.0 partage les mêmes prérequis que celles pour l'approvisionnement en électricité[17],en eau potable[18] ou encore pour le chauffage à distance[19].

Les particularités des normes minimales TIC « spécifiques à un secteur » résident donc dans l'identification des activités critiques du domaine concerné. En se basant sur l'analyse des risques et de la vulnérabilité du secteur du gaz[20] réalisée par l'OFAE ainsi que sur les experts en gaz, la structure du marché et le processus d'approvisionnement de ce secteur ont été analysées permettant ainsi de définir les activités critiques et les systèmes TIC associés. L'identification des activités critiques permet de prioriser certaines mesures du programme de cybersécurité afin que les exploitants gaziers puissent garantir la sécurité des éléments indispensables au bon fonctionnement de leurs installations. 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. Dans le cas du gaz, neuf activités critiques ont été identifiées : le négoce, la nomination, les postes de comptage douaniers, l'odorisation, la gestion du réseau, la compression, le stock journalier, les données clients et les outils de communication. Ces activités critiques sont expliquées en détail dans le chapitre 3.3.

Dans le cas de la norme minimale TIC pour l'approvisionnement en gaz 2.0, il est important de préciser que l'identification de activités critiques n'est pas la seule spécificité de cette norme. En effet, comme il s'agit d'un document qui a pour vocation d'être rendu obligatoire lors de la révision de l'ordonnance sur la sécurité des installations de transport par conduites (OSITC), les niveaux de protection et les exigences qui en découlent sont obligatoires uniquement pour la norme minimale TIC pour l'approvisionnement en gaz 2.0.

[15] 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.

[16] Risiko- und Verwundbarkeitsanalyse des Teilsektors Erdgasversorgung. Office fédéral pour l'approvisionnement économique du pays (OFAE), Berne 2014 (*n'existe qu'en allemand*).

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

[18] Norme minimale pour garantir les technologies de l'information et de la communication (TIC) requises pour l'approvisionnement en eau. Office fédéral pour l'approvisionnement économique du pays, Bern 2023.

[19] Norme minimale pour garantir les technologies de l'information et de la communication (TIC) requises pour l'approvisionnement du chauffage et du froid à distance. Société Suisse de l'Industrie du Gaz et des Eaux (SVGW), Zurich 2019.

[20] Risiko- und Verwundbarkeitsanalyse des Teilsektors Erdgasversorgung. Office fédéral pour l'approvisionnement économique du pays (OFAE), Berne 2014 (*n'existe qu'en allemand*).

3 Processus et activités critiques du secteur du gaz

Ce chapitre consacré au secteur du gaz permet d'identifier la structure du marché, les processus d'approvisionnement ainsi que les activités critiques. Le but étant d'adapter de manière optimale la norme minimale TIC au secteur du gaz.

3.1 Composition du marché

Le marché suisse du gaz est, aujourd'hui encore, fortement segmenté. On compte une centaine de sociétés de distribution locales (SDL) qui approvisionnent les consommateurs finaux du secteur privé et industriel. Afin d'optimiser l'approvisionnement et le transport du gaz, les SDL se sont regroupées au sein de quatre sociétés de transport régionales (STR). Celles-ci sont chargées d'acheter et d'acheminer le gaz pour les SDL. L'entreprise Swissgas, plateforme de services commune aux quatre sociétés régionales, a été créée dans une optique d'optimisation et de d'économies d'échelle. Le principal objectif commercial de Swissgas est de garantir la sécurité d'approvisionnement du côté du transport et l'exploitation compétitive du réseau. Swissgas détient, par exemple, une participation de 51 % dans Transitgas AG et exploite un réseau de gazoducs à haute pression d'une longueur de 260 km. Les sociétés régionales d'approvisionnement et d'autres importateurs se procurent du gaz sur le marché de gros de l'UE et l'importent en Suisse afin de couvrir au mieux les besoins suisses. Outre l'exploitation technique des gazoducs, les STR sont actives dans le transport et le négoce de gaz. La dissociation entre le transport et le négoce se fait selon différentes approches (Figure 1).

La Suisse est au centre du réseau de pipelines européen. Afin de relier le nord et le sud de l'Europe, la société Transitgas, détenue par Swissgas, FluxSwiss et dans une faible mesure Uniper Global Commodities SE, est en charge de l'exploitation du tronçon helvétique reliant l'Allemagne à l'Italie. Il s'agit de l'épine dorsale du réseau de pipelines suisse car jusqu'à trois quarts de la quantité importée par le pays y transite [21]. De plus, il incombe aussi à Transitgas de gérer la station de compression de Ruswil qui assure la pression nécessaire au transport.

Le secteur du gaz se compose de plusieurs organisations qui effectuent des tâches spécifiques. Voici un aperçu des acteurs les plus importants :

- Le réseau haute-pression (> 5 bar et diamètre > 6cm) se compose de Transitgas, Swissgas, les sociétés de transport régionales (STR) et AIL (Aziende Industriali di Lugano). L'Office fédéral de l'énergie (OFEN) est responsable de la surveillance du réseau haute pression en collaboration avec l'Inspection fédérale des pipelines (IFP) qui exerce la surveillance technique.
- Le réseau basse-pression (≤ 5 bar) est géré par des sociétés de distribution locales (SDL). Les cantons sont responsables de la surveillance, en collaboration avec l'Inspection technique de l'industrie gazière suisse (ITIGS) qui exerce la surveillance technique.
- En ce qui concerne la défense des intérêts du secteur gazier, l'Association Suisse de l'Industrie Gazière (ASIG) apporte son soutien à ses membres dans les domaines de la politique, du marketing, des relations publiques et de la formation. Quant à l'association pour l'eau, le gaz et la chaleur (SVGW), elle représente l'ensemble des SDL.

[21] *Risikobewertung Erdgasversorgung Schweiz. Office fédéral de l'énergie (OFEN), 2014, Bern (n'existe qu'en allemand).*

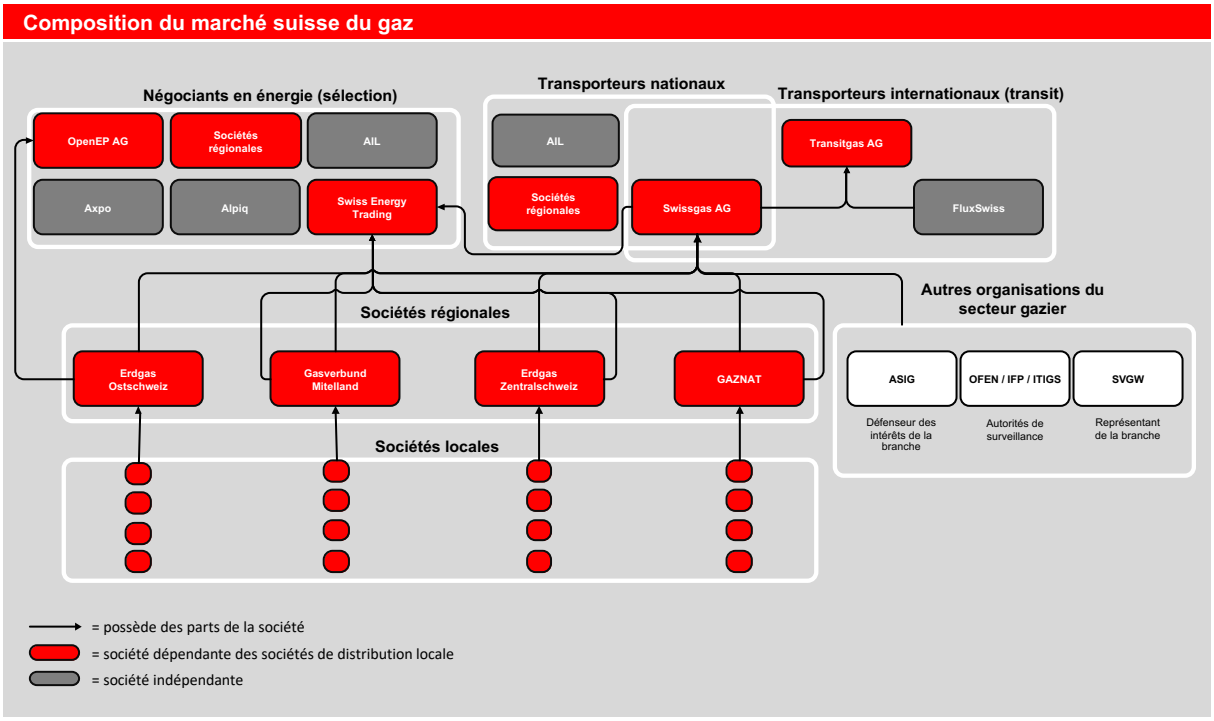

Figure 1 : Structure du marché suisse du gaz (vue simplifiée)

3.2 Processus d'approvisionnement du gaz

Le processus d'approvisionnement de la Suisse en gaz a été divisé en cinq sous-processus (acquisition, production, transport, distribution et consommation) comprenant chacun un certain nombre d'activités. L'ensemble du processus d'approvisionnement est détaillé à l'aide de la Figure 2.

Afin d'approvisionner la Suisse en gaz, il est tout d'abord nécessaire de l'acquérir. Le commerce du gaz est effectué par les négociants en énergie sur le marché européen de l'énergie. Il existe deux modalités d'achat : des achats à long terme (de 5 à 10 ans) ou à court terme (de 1 jour à 3 ans). La première possibilité permet d'acheter des quantités prédéfinies selon les estimations de la consommation et la deuxième d'adapter l'approvisionnement suivant les besoins spécifiques du moment. Le commerce du gaz permet donc de définir une quantité de gaz à livrer, mais il est aussi nécessaire de procéder à la nomination du gaz. Ceci consiste à définir les capacités et les disponibilités du réseau pour la quantité achetée afin de déterminer « l'itinéraire » que le gaz doit emprunter jusqu'à son point de consommation.

Le gaz qui est une énergie majoritairement fossile (la quantité de biogaz actuellement produite et injectée dans les pipelines suisses est encore négligeable), est extrait des gisements gaziers puis traité avant d'être injecté directement ou sous forme de GNL (gaz naturel liquéfié) regazéifié dans le réseau de pipelines européen. La Suisse ne disposant pas de ressources naturelles suffisantes dans son territoire, elle doit importer la totalité du gaz. De ce fait, la Suisse est dépendante des pays producteurs en ce qui concerne le sous-processus « production ».

Le réseau de pipelines européen s'étend de la Norvège à la l'Italie et du Portugal à la Russie. Le gaz y circule généralement à une pression allant de 40 à 80 bar. Il est acheminé en Suisse par l'un des points d'injection. Le réseau suisse est traversé par le gazoduc de Transitgas qui relie le nord et le sud de l'Europe. La station de compression de Ruswil permettant de compresser le gaz afin de le faire transiter à travers les Alpes est particulièrement importante. Normalement, le transport se fait du nord au sud. Une plus grande flexibilité est obtenue grâce au « Reverse Flow » ou flux inversé (du sud au nord).

Le réseau suisse de gazoducs s'étend sur environ 19'000 km avec différents niveaux de pression allant de 5 à 80 bar pour le réseau de transport (Swissgas, les sociétés de transport régionales et Transitgas) et de 20 mbar à 5 bar pour le réseau de distribution (les sociétés de distribution locales). Afin de gérer ces différents niveaux de pression, le réseau suisse dispose d'un certain nombre de postes de détente

et de comptage (PDC) permettant de diminuer la pression afin que le gaz transite correctement jusqu'à son point de consommaiton. Afin de gérer le réseau de manière optimale, le fonctionnement et la coordination des activités liées aux sous-processus « transport » et « distribution » sont commandés et surveillés par un système SCADA. Il évalue et collecte un grand nombre de données permettant aux employés (*dispatcher*) de réguler au mieux le flux de gaz à travers le réseau.

La consommation du gaz diffère selon les utilisateurs. Le gaz est généralement employé pour le chauffage des bâtiments mais peut aussi être utilisé comme carburant pour les véhicules. De plus, le secteur industriel (buanderies, briquèteries, thermolaquage) ainsi que les artisans (boulangerie, brasserie, restauration) dont les activités nécessitent un niveau de chaleur très élevé, en consomment également. Dans le processus d'approvisionnement du gaz, une distinction est effectuée suivant le type d'installation utilisée. Certaines disposent d'un brûleur bicombustible gaz-mazout (interruptible) leur permettant de passer d'un combustible à l'autre selon les besoins. Les autres installations dites « non-interruptibles » fonctionnent exclusivement au gaz et sont donc dépendantes de cette énergie. Rappelons que la Suisse ne dispose pas de réservoir à gaz et que le stockage n'est donc pas possible, excepté le stockage journalier (gaz présent dans les pipelines) représentant un stock limité dont la durée diffère selon les périodes d'utilisation (en hiver, la réserve est d'environ une heure alors qu'en été, celle-ci peut durer plusieurs heures).

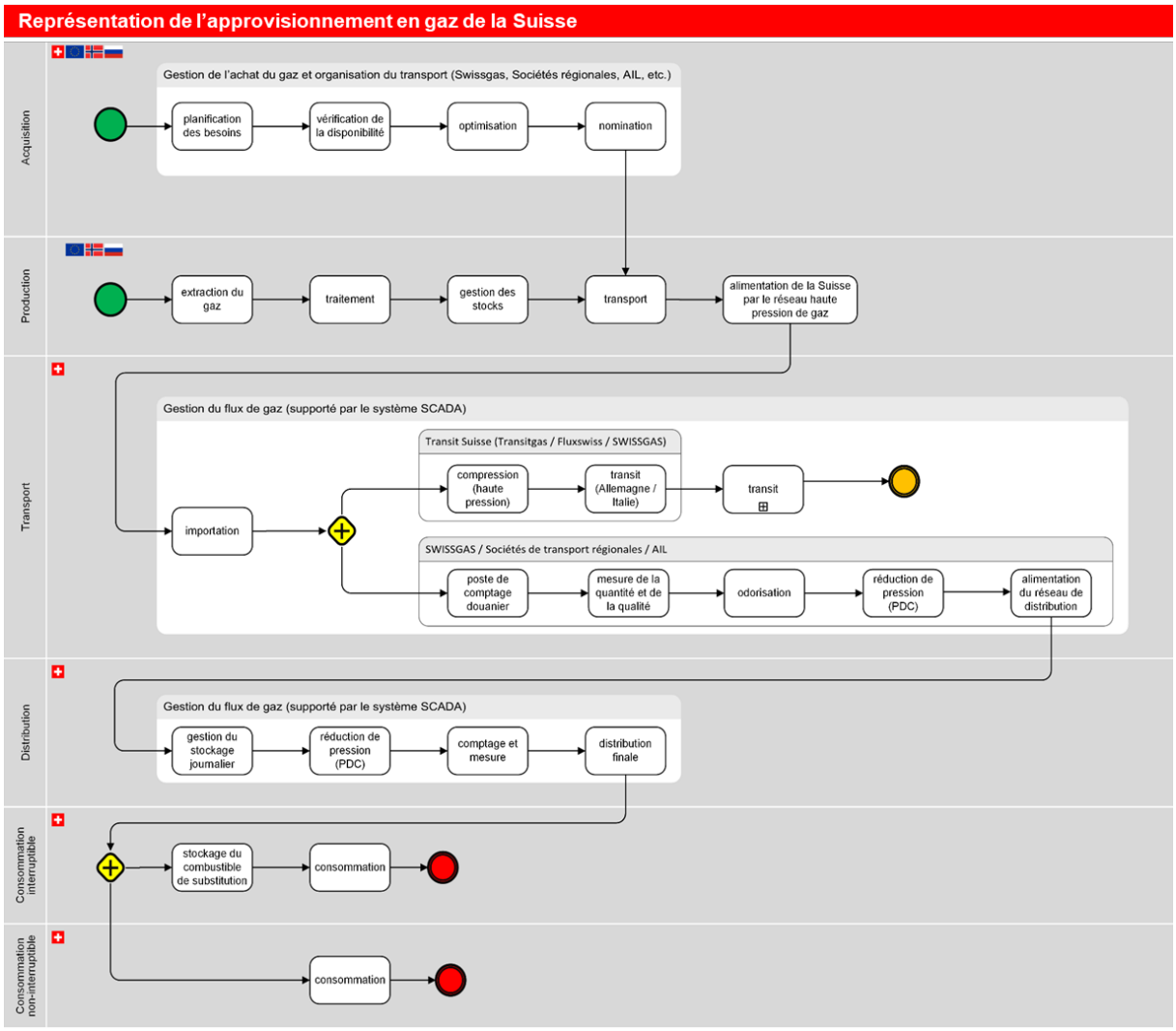

Figure 2 : Processus d'approvisionnement en gaz

3.3 Activités critiques

Afin d'adapter la norme minimale à un secteur, il est indispensable de déterminer les éléments qui nécessitent une attention particulière (lors de l'implémentation de la norme mais aussi au quotidien). Une activité est considérée comme critique si elle remplit deux conditions : être dépendante des systèmes TIC et être indispensable au processus d'approvisionnement (sans cette dernière, l'approvisionnement du pays n'est plus assuré). Les experts du domaine gazier, présents lors de l'élaboration de ce document, ont identifié les activités critiques du secteur du gaz en se basant sur l'analyse des risques et de la vulnérabilité de l'approvisionnement en gaz naturel de l'OFAE[22]. L'ensemble des activités critiques ainsi que les acteurs gaziers et les systèmes TIC associés sont illustrés par la Figure 3.

Remarque : Bien que les activités critiques de l'approvisionnement à l'échelle nationale soient présentées ci-dessous, l'identification des activités critiques au sein même des entreprises est indispensable. Il est donc du devoir de chaque exploitant de définir quelles activités sont essentielles pour son fonctionnement.

Négoce

Pour se procurer du gaz, la première étape consiste à en acheter. Le négoce du gaz naturel s'effectue sur le marché européen de l'énergie et met en contact plusieurs acteurs. Les fournisseurs de gaz, les négociants en énergie ainsi que les exploitants gaziers commercent ensemble afin d'obtenir, au meilleur prix, les quantités de gaz voulues suivant les conditions d'achat à court ou long terme. La gestion des achats se fait de manière numérique à l'aide de systèmes TIC spécifiques (système de négoce et de traitement). Une panne prolongée du système de négoce et de traitement ou des canaux de communication rendrait l'approvisionnement en gaz et le transport plus difficiles, voire impossibles. La sécurité du pays peut être renforcée par des mesures préventives telles que l'attribution contraignante des responsabilités en matière de sécurité d'approvisionnement, la diversification de l'approvisionnement et du transport, des systèmes informatiques et de communication de secours et/ou des contrats de réserve d'urgence nationaux.

Nomination

Une fois l'achat du gaz effectué, il est nécessaire de le transporter jusqu'en Suisse. Le flux physique est soutenu par des systèmes SCADA tandis que le flux commercial est soutenu par des outils d'approvisionnement et de traitement ainsi que par des plateformes de bilan/nomination de responsables de zones de marché et de GRT en Suisse et à l'étranger. À cette fin, les fournisseurs de gaz procèdent à des nominations. Il s'agit de déterminer l'itinéraire à emprunter par le gaz jusqu'à son lieu de consommation ainsi que la capacité et la disponibilité des réseaux traversés. Il est aussi nécessaire de nommer les entrées et les sorties de chaque réseau que le gaz parcourt. En d'autres termes, il s'agit d'organiser l'importation du gaz. La nomination s'effectue de manière numérique par le biais des systèmes de gestion du transport. En cas de dysfonctionnement des systèmes TIC, les sociétés de transport gazières ne seraient plus capables de gérer le transport du gaz et ne pourraient plus assurer son importation.

Poste de comptage douanier (contrôlé par un système SCADA)

Les postes de comptages douaniers permettent de procéder à des mesures aux entrées et sorties d'un réseau. Lorsque le gaz arrive en Suisse, il passe obligatoirement par un poste de comptage douanier afin de déterminer précisément la quantité de gaz réellement importée dans le pays et d'adapter correctement la facturation. De plus, ils mesurent aussi la qualité du gaz ainsi que sa composition. Ce sont les systèmes SCADA qui collectent les données mesurées par les postes de comptage douaniers. En cas de dysfonctionnement, la connexion avec les postes de comptage douaniers serait interrompue. Ce dommage entraînerait d'importantes pertes financières pour les exploitants gaziers, ce qui les mettrait en difficulté. Comme l'approvisionnement de la Suisse en gaz dépend des exploitants gaziers, les postes de comptage douaniers sont considérés comme critiques. Les interventions manuelles sont en principe possibles, mais elles nécessitent des ressources en personnel significativement plus élevées.

[22] Risiko- und Verwundbarkeitsanalyse des Teilsektors Erdgasversorgung. Office fédéral pour l'approvisionnement économique du pays (OFAE), Berne 2014 (*n'existe qu'en allemand*).

Odorisation (contrôlée par un système SCADA)

Le gaz est naturellement incolore et inodore ce qui le rend indétectable pour l'être humain et donc particulièrement dangereux. Afin de remédier à ce problème, le gaz est odorisé artificiellement à l'aide d'un composé chimique : le tétrahydrothiophène (THT). L'odorisation est une tâche spécifique qui est effectuée au sein des postes de comptage douaniers. Les systèmes SCADA mesurent le taux de THT dans le gaz et en injectent automatiquement si le niveau est insuffisant. En cas de dysfonctionnement de ce système, l'approvisionnement en gaz est toujours assuré. Cependant, il est obligatoire pour des raisons légales et de sureté (*safety*) de garantir l'odorisation du gaz. Cette activité a donc été jugée critique afin de préserver un niveau de sécurité acceptable.

Gestion du réseau de pipelines suisse (contrôlé par un système SCADA)

La gestion du réseau suisse de pipelines est l'élément principal des sous-processus « transport » et « distribution » illustrés par la Figure 2. Les systèmes SCADA collectent toutes les données du réseau permettant ainsi de surveiller, à distance, l'ensemble du réseau au travers d'une interface propre à chaque entreprise de transport. Le système de gestion du réseau regroupe la totalité des différents éléments fonctionnant avec un système SCADA (poste de comptage douanier, odorisation, poste de détente et de comptage, etc.) ce qui permet à chaque transporteur gazier d'avoir une vision générale de son réseau, de l'importation à la distribution. En cas de dysfonctionnement de ce système et selon leur durée, les transporteurs gaziers seraient dans l'incapacité de gérer correctement leurs activités. La sécurité de l'approvisionnement en gaz du pays ne serait plus garantie. Les interventions manuelles sont en principe possibles, mais elles nécessitent des ressources en personnel significativement plus élevées.

Compression (contrôlé par un système SCADA)

La compression du réseau gazier est principalement sous la responsabilité de Transitgas et plus spécifiquement de la station de compression de Ruswil. Au niveau national, le processus de compression permet de garantir une pression suffisante dans le réseau haute pression afin de faire circuler le gaz jusqu'à son lieu de consommation. Au niveau international, le processus de compression permet d'assurer une pression suffisamment élevée pour que le gaz puisse traverser les Alpes. La compression est gérée exclusivement à l'aide des systèmes SCADA ce qui rend cette activité complétement dépendante des systèmes TIC. Un dysfonctionnement « national » du processus de compression, lors des mois d'hiver, ne permettrait en effet plus d'assurer un niveau de pression suffisant dans certaines parties du réseau suisse, pouvant priver certaines régions de gaz. Un dysfonctionnement de compression « international » n'affecterait quant à lui pas directement l'approvisionnement de la Suisse mais pénaliserait le réseau européen. Afin d'assurer le bon fonctionnement du réseau et de préserver la réputation ainsi que les engagements contractuels de la Suisse, la compression a été définie comme critique.

Stockage journalier et données clients

La gestion du stockage journalier et les données clients permettent aux sociétés de distribution locales (SDL) de s'adapter aux variations de la consommation de gaz. Lorsque la quantité disponible de gaz passe en dessous d'un certain seuil, les SDL peuvent utiliser le stockage journalier pour réguler la demande de gaz, ce qui leur permet de s'adapter temporairement aux besoins. Dans le même cas de figure, la gestion des données clients permet aux SDL d'avoir une vision globale sur la consommation. Lorsque les prévisions prévoient une consommation élevée, les SDL se servent des données clients pour adapter au mieux possible la distribution et par exemple, avertir certaines entreprises disposant d'installations interruptibles qu'elles doivent se tenir prêtes à passer au mazout. En cas de dysfonctionnement de ces systèmes TIC, les exploitants gaziers seraient en difficulté pour garantir la distribution du gaz, ce qui compromettrait la sûreté de l'approvisionnement en gaz.

Outils de communication

Il s'agit de l'ensemble des systèmes TIC utilisés pour la communication. En font notamment partie : la téléphonie vocale en mode *Voice over IP* (VoIP), l'échange électronique de données (*Electronic Data Interchange* EDI selon les standards GS1), les messageries électroniques (e-mail) et la communication mobile. Les infrastructures de télécommunication qui rendent possible la communication et les échanges des données sont aussi un élément important à prendre en compte. Il s'agit notamment, de bien régir la relation de dépendance qu'il peut y avoir entre les fournisseurs de télécommunication et

les exploitants gaziers afin de s'assurer de la bonne protection des infrastructures de télécommunication. Les systèmes de communication jouent donc un rôle essentiel dans les relations internes et externes des exploitants gaziers. Sans ces outils et leur infrastructure, il serait impossible de garantir un approvisionnement en gaz sûr. Les interventions manuelles sont en principe possibles, mais elles nécessitent des ressources en personnel significativement plus élevées.

Postes de détente et de comptage

Les postes de détente et de comptage (PDC) sont une activité essentielle du processus d'approvisionnement en gaz. Leur rôle consiste à décompresser le gaz afin de lui permettre de passer du réseau de transport jusqu'au réseau de consommation. Bien que les PDC soient primordiaux pour l'acheminement du gaz, ils disposent de plusieurs éléments qui limitent leur criticité. Le système de réduction de pression électronique des PDC est secondé par un système pneumatique (indépendant des TIC). Les PDC disposent aussi d'une sécurité leur permettant de garder en mémoire la dernière valeur enregistrée, permettant ainsi d'éviter toute interruption. De plus, les PDC peuvent aussi être contrôlés manuellement sur place (mais cela nécessite une main-d'œuvre importante). En vue de ces éléments, les PDC sont indépendants des systèmes TIC et ne sont pas, dans ce cas-ci, envisagés comme une activité critique. Cependant, il ne s'agit pas d'une vérité absolue et certains PDC peuvent être considérés comme une activité critique en fonction de leur conception. Chaque organisation est responsable de définir le niveau de criticité de ses PDC et de les considérer ou non comme une activité critique.

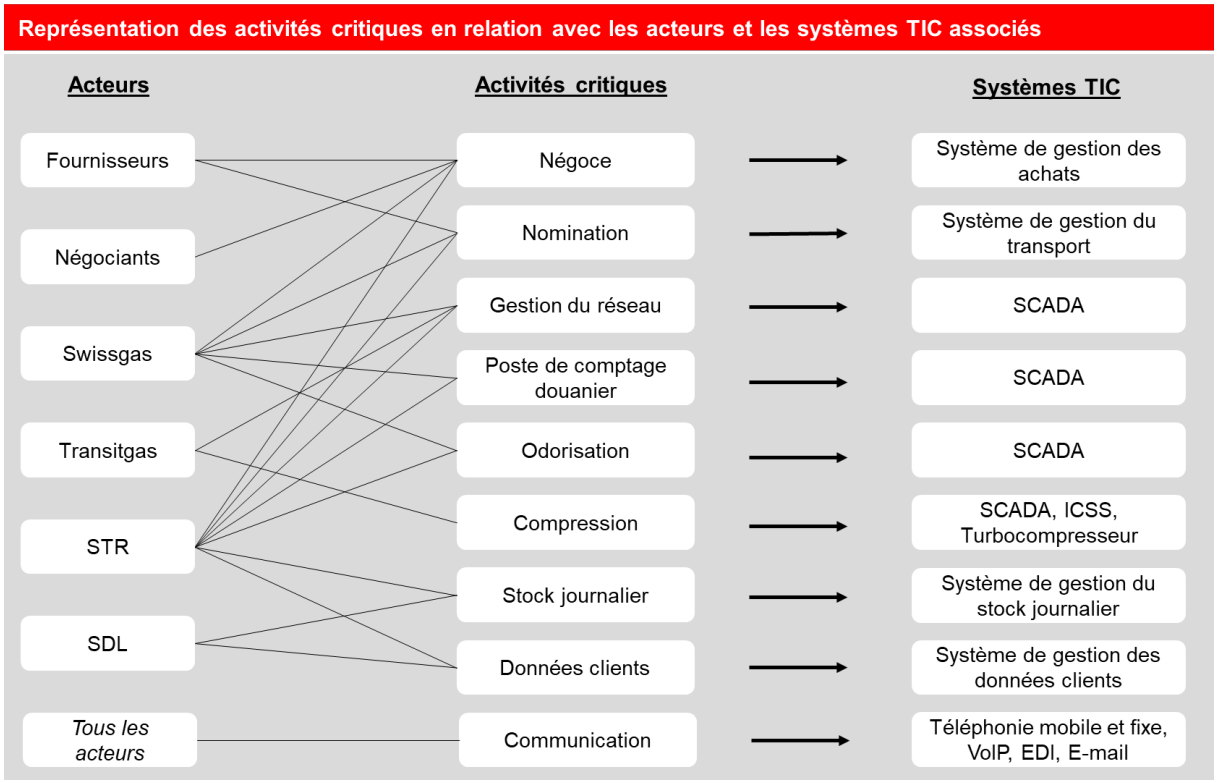

Figure 3 : Relations entre les acteurs gaziers, les activités critiques et les systèmes TIC associés

4 Programme de cybersécurité de la norme minimale TIC

Ce chapitre permet de traiter des éléments concrets de la norme minimale TIC pour l'approvisionnement en gaz 2.0. Il commence par aborder les notions de base de tout programme de cybersécurité : la triade CIA[23]. Il continue en se concentrant sur le programme de cybersécurité de la norme minimale TIC à savoir le *NIST Framework*. Les fondements, les fonctions ainsi que les mesures du *NIST Framework* sont expliqués succinctement. Pour obtenir des informations plus détaillées sur le cadre de cybersécurité de la norme minimale TIC, il est recommandé de consulter le document d'accompagnement[4].

4.1 Les concepts de base de la cybersécurité

Dans le domaine de la cybersécurité et plus particulièrement de la sécurité des données, il existe trois principes fondamentaux qui régissent la mise en place d'une politique de sécurité. Il s'agit de la confidentialité, de l'intégrité et de la disponibilité des données (Figure 4). La norme minimale TIC ne déroge pas à la règle et chaque mesure contenue dans son programme de cybersécurité a pour but d'améliorer le niveau de sécurité d'au moins l'une de ces trois notions. La confidentialité qui a longtemps été un symbole de la sécurité, signifie que seuls les systèmes et les personnes autorisées peuvent accéder aux données. Cependant, travailler uniquement sur la confidentialité des données n'est pas suffisant pour permettre aux organisations de se protéger contre des cyberrisques. En effet, il est aussi important de garantir l'intégrité des données, ce qui signifie s'assurer que les données soient en tout temps complètes et exactes afin d'éviter de prendre de mauvaises décisions en se basant sur des informations erronées. Le dernier élément est la disponibilité des données qui signifie qu'une organisation doit avoir accès à ses données à chaque fois que cela est nécessaire. Il s'agit d'une notion primordiale car même si les données sont confidentielles et intègres mais qu'elles ne sont pas accessibles, elles ne sont d'aucune utilité. Ces trois principes constituent donc le socle d'une infrastructure protégée efficacement contre les cyberrisques. L'application de ce modèle est essentielle à tous programmes de cybersécurité car il se concentre sur la sécurité et la protection des données.

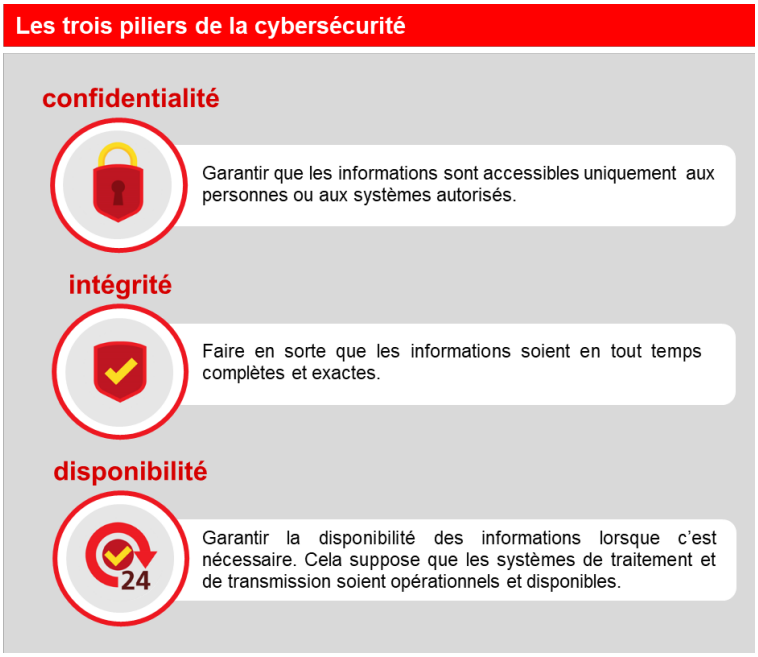

Figure 4 : Triade CIA

[23] Il s'agit de trois concepts de base comprenant la confidentialité (*Confidentiality*), l'intégrité (*Integrity*) et la disponibilité (*Availability*) des données.

4.2 Le NIST Framework comme programme de cybersécurité

La norme minimale TIC se base sur le *NIST Framework*[24] qui a été développé afin de réduire les cyberrisques pour les infrastructures critiques. Cette méthodologie 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* est de fournir aux opérateurs d'infrastructures critiques et à toutes les 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.

L'objectif du *NIST Cybersecurity Framework* est de fournir un cadre qui permet d'accroître efficacement le niveau de protection face aux cyberrisques. Pour ce faire, ce programme de cybersécurité se base sur une approche fondée sur le risque acceptable et sur la stratégie de défense en profondeur (*defense-in-depth*). Il offre également 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 autres normes internationales comme les normes ISO 2700x.

Plus concrètement, le *NIST Framework* repose sur 108 mesures réparties dans 23 catégories et regroupées sous cinq fonctions : identifier, protéger, détecter, réagir et récupérer. Ces cinq fonctions reflètent la philosophie du *NIST Framework* qui aborde la cybersécurité comme un processus dynamique qui nécessite des contrôles réguliers et une procédure d'amélioration continue (Figure 5). L'implémentation de la norme minimale TIC consiste à évaluer de 0 à 4 (niveaux de maturité) l'ensemble des mesures du *NIST Framework.* Ce diagnostic permet à chaque organisation de déterminer ses forces ainsi que ses faiblesses et d'appliquer les solutions de sécurité correspondantes en améliorant les mesures qui sont en-dessous des valeurs définies. L'évaluation de ces mesures offre un cadre de sécurité complet permettant aux exploitants gaziers d'adapter en continu leur programme de sécurité à leurs besoins.

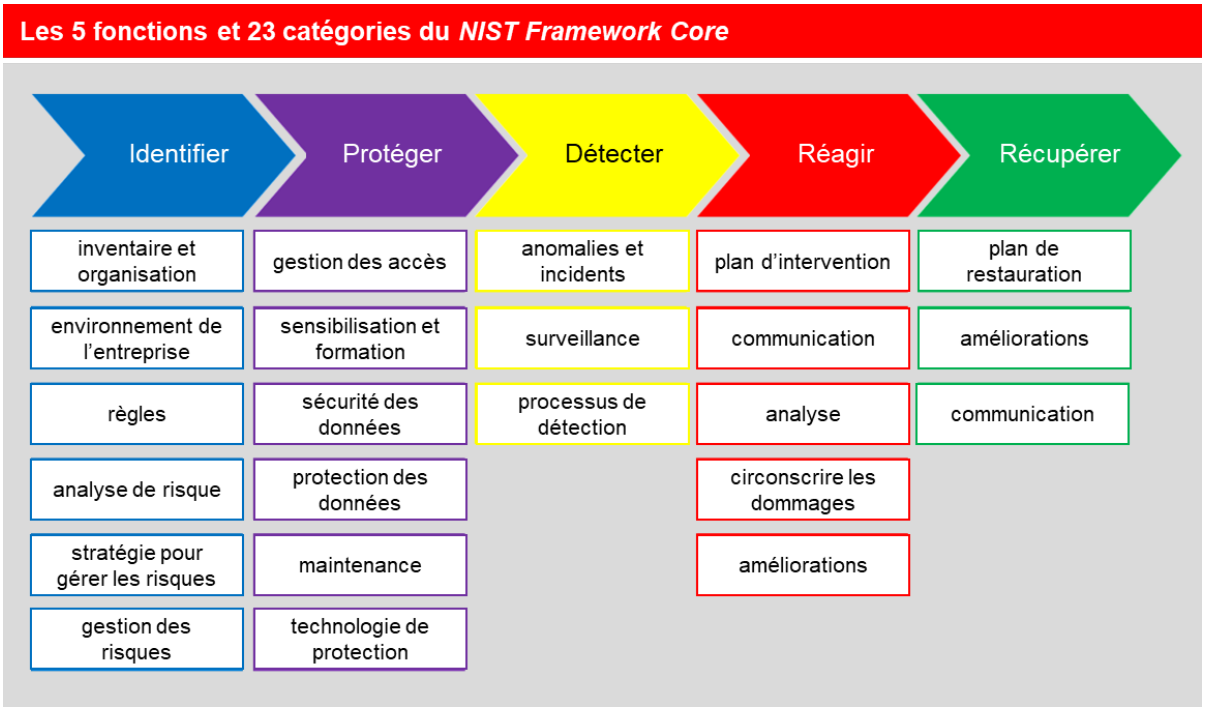

Figure 5 : Structure du NIST Framework Core

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

4.3 Les fonctions du NIST Framework Core

Les fonctions du *NIST Framework Core* constituent le niveau le plus général de ce cadre de cybersécurité. Elles forment l'épine dorsale sur laquelle s'articule tous les autres éléments (Figure 6). Ces cinq fonctions ont été choisies car elles représentent les principales thématiques d'un programme de cybersécurité efficace. Elles permettent de déterminer efficacement les cyberrisques et de prendre des décisions adaptées en matière de gestion des risques. Elles sont en outre réparties en 23 catégories afin de classifier toutes les mesures du *NIST Framework Core.*

Identifier

Dans le cadre de l'identification du framework NIST, les actifs, les menaces et les vulnérabilités sont répertoriés. Cela permet d'évaluer les risques et leur impact sur les objectifs commerciaux. L'identification est un processus continu qui nécessite un suivi régulier. Les entreprises concentrent leurs ressources sur les domaines présentant les risques les plus élevés. L'objectif est de créer une base efficace pour la stratégie de cybersécurité.

Protéger

Cette fonction comprend des mesures visant à garantir une protection adéquate, y compris des contrôles de sécurité pour l'ensemble des actifs TIC de l'organisation. Il s'agit en particulier de procédés techniques (anti-virus, DMZ, architecture réseau, etc.) mais aussi d'aspects organisationnels tels que la sensibilisation des collaborateurs aux cyberrisques. Le but est d'éviter ou de limiter les dégâts engendrés par une potentielle menace.

Détecter

Après avoir identifié les éléments TIC et appliqué les mesures de protection adéquates, il est nécessaire de procéder à une surveillance en continu de la sécurité des infrastructures. Les mesures de cette fonction ont pour objectifs de mettre en place un système de surveillance efficace et ciblé des éléments TIC afin de déceler suffisamment tôt des menaces et ainsi d'éviter ou d'atténuer les conséquences d'un cyberincident.

Réagir

Au sein de cette fonction, les mesures permettent d'adapter les procédures de sécurité lors de la détection de cybermenaces. L'objectif est de répondre correctement à un cyberincident en limitant un maximum l'impact de ce dernier sur l'organisation. L'idéal est de disposer de procédures détaillées et approuvées afin de résoudre l'incident le plus efficacement possible.

Récupérer

Cette fonction contient les mesures permettant de restaurer toutes les capacités qui ont été altérées par un incident de cybersécurité. Il s'agit d'appliquer les plans de résilience afin de rétablir les infrastructures de l'organisation pour lui permettre de reprendre rapidement un rythme de travail normal. Cette fonction est primordiale pour permettre de relancer, sur une base solide, les éléments TIC d'une entreprise et donc réduire l'impact d'un incident de cybersécurité.

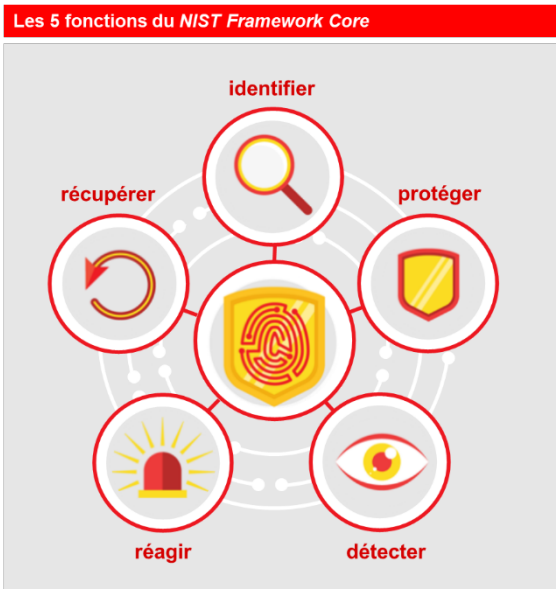

Figure 6 : Fonctions du NIST Framework Core

4.4 Les mesures du NIST Framework Core

Ce chapitre contient l'ensemble des mesures du *NIST Framework Core* qui doivent être évaluées dans le cadre de la norme minimale TIC. Chacune des mesures est décrite brièvement. Pour une meilleure compréhension, il est recommandé d'utiliser, en complément à cette norme minimale TIC, le document d'accompagnement[4] ainsi que l'outil d'évaluation Excel[25]. Le premier offre une meilleure description des mesures via des définitions plus concrètes, une mise en contexte et des exemples explicites. Quant au deuxième, il est spécialement conçu pour faciliter l'évaluation des mesures.

4.4.1 Identifier – *Identify*

4.4.1.1 *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	Les ressources (par exemple, le hardware, les équipements, les données, le temps, le personnel et les softwares) sont classées par ordre de priorité en fonction de leur classification, de leur criticité et de leur valeur pour l'entreprise
ID.AM-6	Les rôles et responsabilités de l'ensemble du personnel et des parties prenantes externes (p.ex. fournisseurs, clients, partenaires) sont établies.

Tableau 1 : Tâches ID.AM

4.4.1.2 *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.

[25] Il s'agit du document Excel "IKT-Minimalstandard-Assessment.Tool" disponible sur le site de l'OFAE : https://www.bwl.admin.ch/bwl/fr/home/themen/ikt/ikt_minimalstandard.html

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 critique 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	Pour toutes les circonstances (p.ex. en cas d'attaque/contrainte, pendant la récupération, en fonctionnement normal) sont établies des exigences de résilience pour la fourniture de services critiques.

Tableau 2 : Tâches ID.BE

4.4.1.3 *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	Des directives sur la sécurité de l'information sont établies et communiquées dans l'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 3 : Tâches ID.GV

4.4.1.4 *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 4 : Tâches ID.RA

4.4.1.5 *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 5 : Tâches ID.RM

4.4.1.6 *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	Les fournisseurs et prestataires pour les systèmes d'information, composants et services sont identifiés, classés par priorité et évalués par un processus d'évaluation des risques pour la chaîne d'approvisionnement cyber.
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 un incident.

Tableau 6 : Tâches ID.SC

4.4.2 Protéger – Protect

4.4.2.1 *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	Vérifiez que l'intégrité de votre réseau est protégée. Séparez votre réseau au niveau logique comme physique, si c'est nécessaire et judicieux.
PR.AC-6	N'attribuez des identités numériques qu'à des personnes ou à des processus que vous avez clairement identifiés.
PR.AC-7	L'authentification d'utilisateurs, appareils et autres assets (p.ex. Authentification à un ou plusieurs facteurs) est effectuée en fonction du risque de la transaction (p.ex. Risques de sécurité ou protection des données pour des personnes et autres risques d'entreprise).

Tableau 7 : Tâches PR.AC

4.4.2.2 *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 8 : Tâches PR.AT

4.4.2.3 *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.
PR.DS-6	Définissez un processus pour vérifier l'intégrité des firmwares, des systèmes d'exploitation, des softwares d'application et des données.
PR.DS-7	Ayez un environnement informatique (IT) pour le développement et les tests qui soit totalement indépendant des systèmes de production.
PR.DS-8	Définissez un processus pour vérifier l'intégrité des hardwares utilisés.

Tableau 9 : Tâches PR.DS

4.4.2.4 *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 l'utilisation des équipements TIC.
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	Veillez à ce que toutes les exigences (réglementaires) et les directives concernant les équipements « physiques » soient respectées.
PR.IP-6	Veillez à ce que les données soient toujours détruites selon les prescriptions.
PR.IP-7	Développez et améliorez régulièrement vos processus de sécurité informatique.
PR.IP-8	Discutez de l'efficacité des différentes technologies de protection avec vos partenaires.

Désignation	Tâche
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 10 : Tâches PR.IP

4.4.2.5 *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 11 : Tâches PR.MA

4.4.2.6 *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 assurer en tout temps une fonctionnalité minimale (Hardening de système).
PR.PT-4	Assurez la protection de vos réseaux de communication et de contrôle.
PR.PT-5	Assurez-vous que des mécanismes (par ex. sécurité en cas de panne, équilibrage de charge, remplacement à chaud) sont mis en œuvre pour répondre aux exigences en matière de sécurité en cas de panne dans des situations normales et défavorables.

Tableau 12 : Tâches PR.PT

4.4.3 Détecter – *Detect*

4.4.3.1 *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. Gérez 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 13 : Tâches DE.AE

4.4.3.2 *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 (surveillance) de tous les équipements et des bâtiments pour détecter les incidents de cybersécurité.
DE.CM-3	Mettez en place une surveillance de l'utilisation des TIC par les 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 14 : Tâches DE.CM

4.4.3.3 *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 15 : Tâches DE.DP

4.4.4 Réagir – Respond

4.4.4.1 *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 16 : Tâches RS.RP

4.4.4.2 *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 le signalement des incidents de cybersécurité et assurez-vous qu'ils soient 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	La coordination avec toutes les parties prenantes et les groupes d'intérêt se fait en accord avec les plans de réaction selon les critères prédéfinis.

Désignation	Tâche
RS.CO-5	Des informations sont régulièrement et volontairement échangées avec des acteurs externes afin d'accroître la sensibilisation à la situation actuelle en matière de cybersécurité.

Tableau 17 : Tâches RS.CO

4.4.4.3 *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 ce que les impacts d'un incident de sécurité cyber soient connus et compris.
RS.AN-3	Effectuez une analyse forensique après chaque incident.
RS.AN-4	Classez les incidents selon les exigences du plan de réaction.
RS.AN-5	Mettre en place des processus pour recevoir, analyser et réagir aux vulnérabilités portées à la connaissance de l'organisation par des sources internes et externes (par exemple, audits internes, bulletins de sécurité ou chercheurs en sécurité).

Tableau 18 : Tâches RS.AN

4.4.4.4 *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 propagation.
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 19 : Tâches RS.MI

4.4.4.5 *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 20 : Tâches RS.IM

4.4.5 Récupérer – Recover

4.4.5.1 *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 21 : Tâches RC.RP

4.4.5.2 *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.

Désignation	Tâche
RC.IM-2	Actualisez vos stratégies de récupération.

Tableau 22 : Tâches RC.IM

4.4.5.3 *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	Veillez à ce que votre perception publique soit activement prise en compte.
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 23 : Tâches RC.CO

4.5 L'évaluation des mesures et définition des niveaux de maturité (*Tiers)*

Le *NIST Framework* comprend plusieurs niveaux de maturité, appelés *Implementation Tiers*. Ils permettent d'évaluer le niveau de mise en œuvre des mesures de cybersécurité. Ces niveaux vont de « non mis en œuvre » (*Tier 0*) à « dynamique » (*Tier 4*). Pour déterminer son niveau de maturité, une organisation 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 ainsi que ses besoins organisationnels.

Les descriptions des quatre niveaux de maturité (*Tiers*) sont détaillées dans les paragraphes suivants et sont complétées par la Figure 7 qui illustre de manière simplifiée les caractéristiques principales de chaque niveau.

Remarque importante concernant n/a : non applicable

- Cette mesure ne peut pas être évaluée, car elle ne concerne pas l'organisation en question et ne peut donc pas être appliquée. Il est toutefois nécessaire de justifier pourquoi cette mesure ne peut pas être appliquée.
- Exemple : Une entreprise peut renoncer à utiliser certains services. Dans ce cas, les sous-catégories liées exclusivement à ces services ne s'appliqueront pas. Par exemple, si l'entreprise renonce à la maintenance à distance, la mesure PR.MA-2 sera N/A et une justification sera nécessaire.

***Tier 0* : non mis en œuvre**

- Il s'agit du niveau le plus bas qui correspond à une protection inexistante. Les mesures ne sont pas mises en œuvre, aucun processus n'existe et rien n'a été entrepris.

***Tier 1* : partiellement mis en œuvre, pas entièrement défini ni validé**

- 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. De ce fait, les risques de cybersécurité sont généralement gérés de manière ad hoc ou réactive.
- Il existe un programme intégré de gestion des risques au niveau de l'organisation, mais pas de sensibilisation institutionnalisée aux risques de cybersécurité ni d'approche à l'échelle de l'organisation pour les gérer.
- En règle générale, l'organisation ne dispose pas de mécanismes permettant d'utiliser de manière coordonnée les informations relatives à la cybersécurité. Lorsque des incidents de cybersécurité surviennent, l'organisation ne dispose pas de procédures standardisées pour partager les informations ou coordonner la collaboration avec des partenaires externes.

***Tier 2* : partiellement mis en œuvre, entièrement défini et approuvé**

- Les organisations qui se classent dans le niveau 2 disposent généralement de procédures de gestion des risques pour contrer les risques de cybersécurité. Cependant, elles ne sont pas mises en œuvre sous la forme d'instructions spécifiques que le personnel doit suivre.
- Au niveau de l'organisation, les risques de cybersécurité sont intégrés dans le système de gestion des risques à l'échelle de l'entreprise, et il existe une certaine prise de conscience à tous les niveaux de l'entreprise. Cela dit, ces organisations ne disposent généralement pas d'approches à l'échelle de l'entreprise pour gérer et améliorer la sensibilisation aux risques de cybersécurité actuels et futurs.
- Les procédures et processus approuvés sont définis et mis en œuvre. Le personnel dispose de ressources suffisantes pour remplir ses rôles en matière de cybersécurité. Les informations relatives à la cybersécurité sont partagées au sein de l'organisation de manière informelle.
- L'organisation comprend son rôle dans un environnement plus large et communique avec les partenaires externes (par exemple, les clients, les fournisseurs, les prestataires de services, etc.) sur les questions de cybersécurité. Il n'existe cependant pas de procédures standardisées pour coopérer ou partager des informations avec ces partenaires.

***Tier 3* : entièrement ou très largement mis en œuvre, statique**

- Les organisations de niveau 3 disposent de plans de gestion des risques officiellement approuvés, ainsi que des exigences relatives à leur mise en œuvre dans l'ensemble de l'entreprise.
- Les politiques applicables à l'ensemble de l'entreprise définissent la manière dont les risques de cybersécurité doivent être traités. Les risques de cybersécurité et les exigences relatives à leur traitement sont standardisés et régulièrement mis à jour. Ces mises à jour tiennent compte des changements dans les besoins de l'entreprise, des développements techniques et de l'évolution du paysage des menaces (en raison de l'apparition de nouveaux acteurs, par exemple) ou des changements politiques.
- Les procédures et les processus permettant de faire face à ces nouveaux risques sont définis par écrit. L'organisation utilise des méthodes standardisées pour répondre aux changements de risques. Les collaborateurs ont les connaissances et les compétences nécessaires pour accomplir leurs tâches.
- L'organisation a connaissance de ses dépendances vis-à-vis des partenaires externes et partage régulièrement avec eux des informations qui permettent à sa direction de prendre des décisions en réponse à des incidents.

***Tier 4 :* mis en œuvre de manière dynamique, contrôlé continuellement et amélioré**

- Le niveau 4 signifie qu'une organisation répond intégralement à toutes les exigences des niveaux 1 à 3, et qu'elle examine également ses propres procédures, méthodes et capacités en permanence, en les améliorant si nécessaire. Cette amélioration continue repose sur la documentation complète de tous les incidents de cybersécurité.
- L’organisation 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 liés à la cybersécurité fait partie intégrante de la culture de l'entreprise.
- Les conclusions tirées d'incidents antérieurs, les informations provenant de sources externes et de la surveillance continue par l'entreprise de ses propres systèmes et réseaux sont intégrées en permanence dans le processus de gestion des risques.
- L'organisation partage constamment des informations avec ses partenaires, pour lesquels elle a mis en place des procédures standardisées.

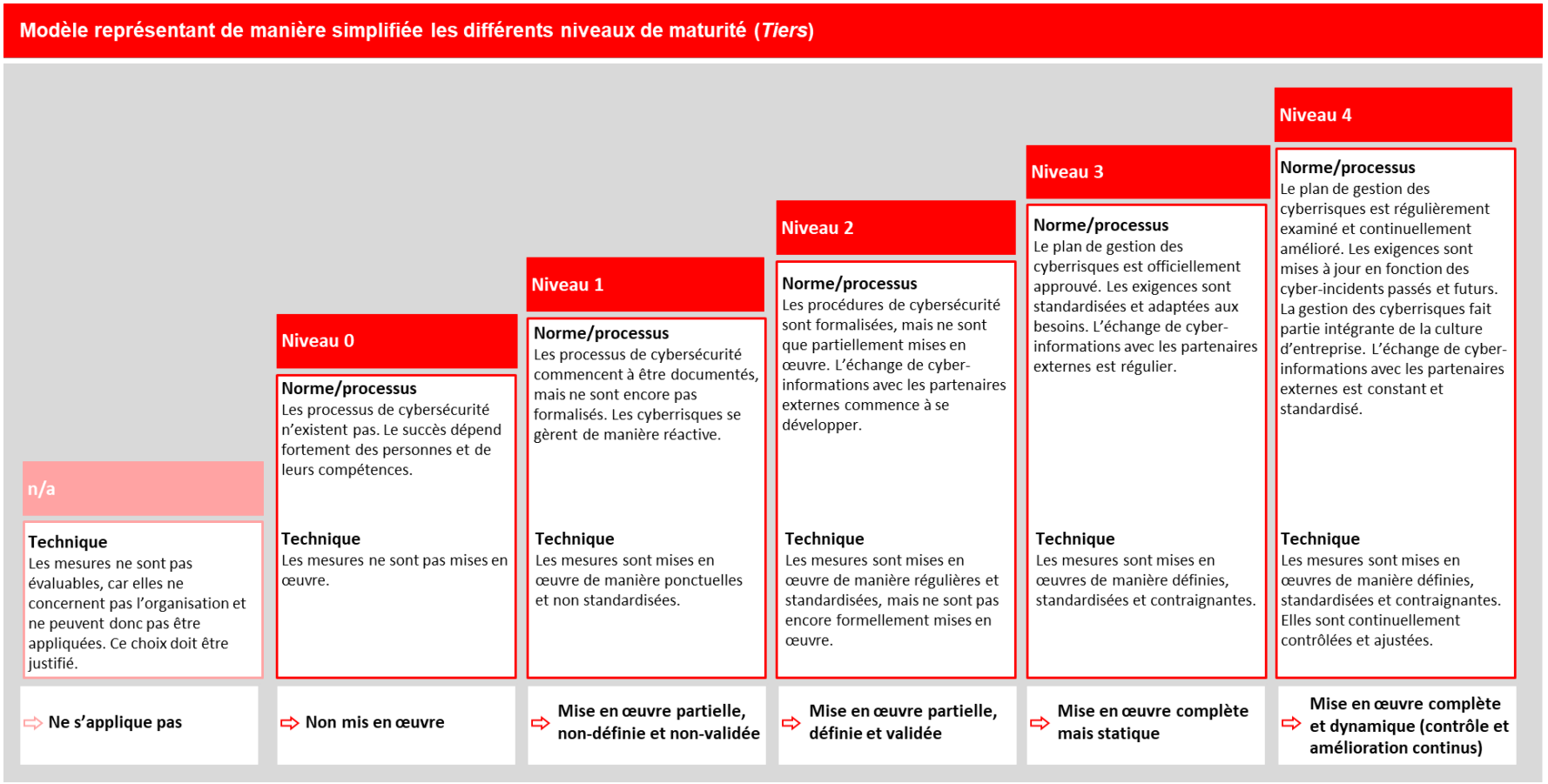

Figure 7 : Résumé des niveaux de maturité (tiers)

5 Niveaux de protection et exigences

La révision de l'ordonnance sur la sécurité des installations de transport par conduites (OSITC ; RS 746.12) vise à rendre la norme minimale TIC obligatoire pour les exploitants gaziers d'installation de transport par conduite. Elle contraint, les acteurs tenus d'appliquer cette norme, à atteindre un niveau de protection donné pour la mise en œuvre des mesures prévues. Afin de respecter le principe de proportionnalité et de répondre au mieux aux besoins de la branche gazière, trois niveaux de protection ont été définis (A, B et C). À chaque niveau de protection correspondent des niveaux de maturité spécifiques, ce qui permet d'échelonner les exigences.

5.1 Niveaux de protection

Des critères sont définis pour différencier les exploitants gaziers selon leurs besoins, leur criticité et leurs ressources. Les niveaux de protection s'appliquent uniquement aux exploitants gaziers d'installation de transport par conduite. Les clients finaux sont exclus de cette obligation.

Critères		Niveau de protection A	Niveau de protection B	Niveau de protection C
Pression du réseau/installation (bar) et longueur des conduites (km) :	> 5 bar et > 15 km	X		
Volume de gaz transporté :	> 2600 GWh/an	X		
	≤ 2600 GWh/an et >400 GWh/an		X	
	≤ 400 GWh/an			X

Energie GWh/an : basé sur la moyenne des cinq dernières années civiles

Figure 8 : Critères des niveaux de protection

La classification des entreprises selon les critères définis ci-dessus (Figure 8) permet de leur attribuer un niveau de protection : A, B ou C. Si un exploitant gazier remplit les critères d'un niveau de protection, il doit appliquer les exigences correspondantes (voir chapitre 5.2). Le volume de gaz transporté comprend la somme totale de gaz qui transite dans les installations de transport par conduite. Il s'agit du volume distribué aux clients finaux mais également de celui transmis à d'autres exploitants de réseaux gaziers (rôle de transporteur intermédiaire).

Les exploitants gaziers d'installations de transport par conduites d'une pression supérieure à 5 bar et dont la longueur du réseau est supérieure à 15 kilomètres sont automatiquement associés au niveau de protection A. Pour les autres exploitants gaziers, il faut se référer à la moyenne du volume de gaz transporté des 5 dernières années. Si cette valeur est supérieure à 2'600 GWh/an, il s'agit également du niveau de protection A. Pour une valeur comprise entre 400 GWh/an et 2'600 GWh/an, cela correspond au niveau de protection B. Pour une valeur inférieure ou égale à 400 GWh/an, c'est le niveau de protection C qui s'applique. Afin d'aider à l'identification du niveau de protection correspond, la Figure 9 offre une vision plus graphique de ce processus.

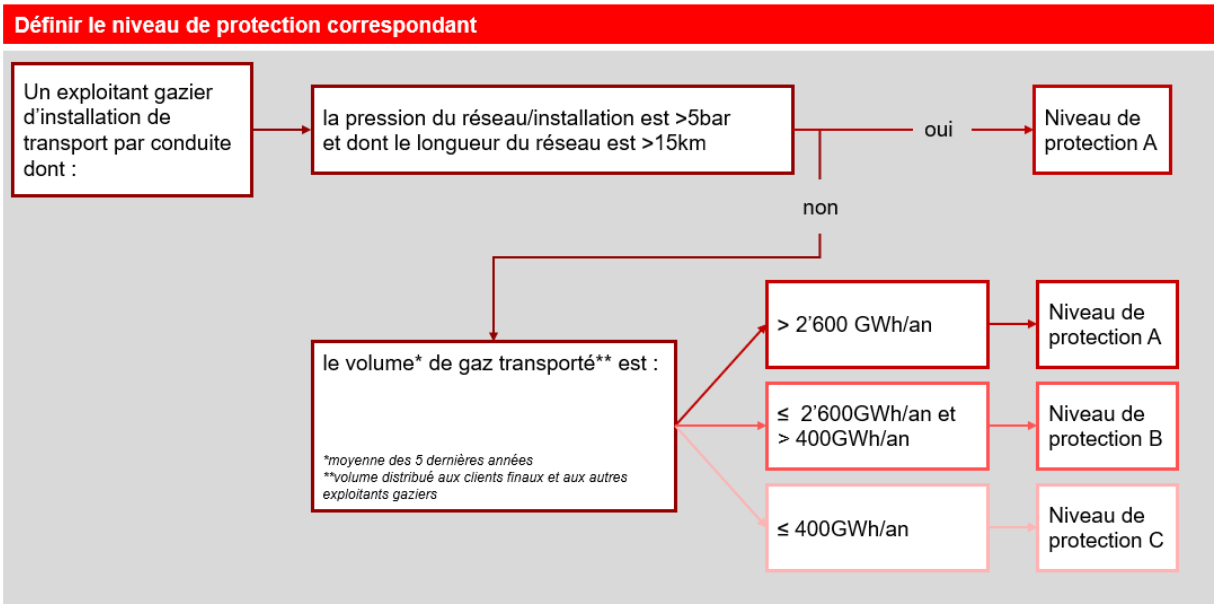

Figure 9 : Définir le niveau de protection correspondant

5.2 Exigences des niveaux de protection

Les niveaux de protection définissent les exigences à atteindre concernant le niveau de maturité des mesures du *NIST Framework Implementation Tiers* qui sont traitées dans la norme minimale TIC pour l'approvisionnement en gaz 2.0. Les exigences du niveau de protection A sont les plus strictes et s'adressent aux entreprises les plus importantes pour l'approvisionnement en gaz. Les niveaux B et C comportent des exigences moindres, respectivement pour les acteurs de taille moyenne et petite taille. Conformément à la procédure d'évaluation énoncée au chapitre 4.5, les exigences sont définies à l'aide des différents niveaux de maturité (*Tiers*).

Pour les petits exploitants gaziers, le niveau de protection C ne fixe des prescriptions contraignantes que pour environ quarante des cent huit mesures que comporte cette norme minimale TIC. En raison du principe de proportionnalité, seules les mesures prioritaires dans la hiérarchie doivent être mises en œuvre. Les mesures qui ne sont pas rendues obligatoires restent, cependant, fortement recommandées.

Les niveaux de maturité suivants doivent au moins être atteints :

Mesures	Niveau de protection A	Niveau de protection B	Niveau de protection C
Identifier (ID = Identify)			
ID.AM-1	3	3	3
ID.AM-2	3	3	2
ID.AM-3	3	3	2
ID.AM-4	3	3	–
ID.AM-5	3	3	–
ID.AM-6	3	4	3
ID.BE-1	3	2	–
ID.BE-2	3	2	–
ID.BE-3	3	3	–
ID.BE-4	3	3	–
ID.BE-5	3	2	–
ID.GV-1	3	4	3
ID.GV-2	3	3	3
ID.GV-3	3	4	3

Mesures	Niveau de protection A	Niveau de protection B	Niveau de protection C
ID.GV-4	3	3	–
ID.RA-1	3	2	–
ID.RA-2	3	3	–
ID.RA-3	3	3	–
ID.RA-4	3	3	–
ID.RA-5	3	2	–
ID.RA-6	3	2	–
ID.RM-1	3	2	–
ID.RM-2	2	3	–
ID.RM-3	2	3	–
ID.SC-1	3	3	–
ID.SC-2	3	3	–
ID.SC-3	2	3	3
ID.SC-4	2	2	–
ID.SC-5	3	2	–
Protéger (PR = Protect)			
PR.AC-1	3	3	2
PR.AC-2	3	3	2
PR.AC-3	4	4	3
PR.AC-4	3	3	2
PR.AC-5	3	3	2
PR.AC-6	3	3	2
PR.AC-7	3	3	2
PR.AT-1	4	3	3
PR.AT-2	4	3	3
PR.AT-3	3	3	–
PR.AT-4	4	3	3
PR.AT-5	3	3	–
PR.DS-1	4	2	–
PR.DS-2	3	4	2
PR.DS-3	2	3	–
PR.DS-4	2	2	–
PR.DS-5	3	2	–
PR.DS-6	3	2	–
PR.DS-7	3	2	–
PR.DS-8	2	2	–
PR.IP-1	4	2	2
PR.IP-2	2	3	–
PR.IP-3	3	3	–
PR.IP-4	4	4	3
PR.IP-5	3	4	3
PR.IP-6	2	3	–
PR.IP-7	2	2	–
PR.IP-8	2	2	–
PR.IP-9	3	2	2
PR.IP-10	3	2	–
PR.IP-11	3	2	–

Mesures	Niveau de protection A	Niveau de protection B	Niveau de protection C
PR.IP-12	3	2	–
PR.MA-1	2	3	–
PR.MA-2	2	3	2
PR.PT-1	3	2	–
PR.PT-2	3	4	3
PR.PT-3	3	3	–
PR.PT-4	4	3	3
PR.PT-5	3	2	–
Détecter (DE = Detect)			
DE.AE-1	2	2	–
DE.AE-2	3	2	–
DE.AE-3	3	2	–
DE.AE-4	3	2	–
DE.AE-5	3	2	–
DE.CM-1	3	3	2
DE.CM-2	2	3	2
DE.CM-3	2	2	–
DE.CM-4	3	3	2
DE.CM-5	3	3	2
DE.CM-6	1	2	–
DE.CM-7	3	2	2
DE.CM-8	4	2	–
DE.DP-1	3	4	2
DE.DP-2	3	2	–
DE.DP-3	3	3	–
DE.DP-4	2	2	–
DE.DP-5	3	2	–
Réagir (RS = Respond)			
RS.RP-1	3	3	2
RS.CO-1	2	3	2
RS.CO-2	3	4	2
RS.CO-3	3	2	–
RS.CO-4	2	2	–
RS.CO-5	2	2	–
RS.AN-1	3	3	–
RS.AN-2	2	3	–
RS.AN-3	3	2	–
RS.AN-4	2	2	–
RS.AN-5	2	2	–
RS.MI-1	3	3	2
RS.MI-2	3	2	2
RS.MI-3	3	2	2
RS.IM-1	3	3	–
RS.IM-2	3	3	–
Récupérer (RC = Recover)			
RC.RP-1	3	3	2
RC.IM-1	3	2	–

Mesures	Niveau de protection A	Niveau de protection B	Niveau de protection C
RC.IM-2	3	2	–
RC.CO-1	2	1	–
RC.CO-2	2	1	–
RC.CO-3	2	1	–

Tableau 24 : Exigences à atteindre pour chaque niveau de protection

6 Annexes

6.1 Glossaire

Abréviation	Description
AEP	Approvisionnement économique du pays
AIL	Aziende Industriali di Lugano SA
ASIG	Association Suisse de l'Industrie Gazière
BSI	Bundesamt für Sicherheit in der Informationstechnik (Allemagne)
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
ICS	Industrial Control Systems
IFP	Inspection Fédérale des Pipelines
IP	Internet Protocol
ISA	International Society of Automation
ISO	Organisation internationale de normalisation
IT	Technologie de l'information (Information Technology), ici en particulier Office-IT / bureautique.
ITIGS	Inspection Technique de l'Industrie Gazière Suisse
MELANI	Centrale d'enregistrement et d'analyse pour la sûreté de l'information (Unité de pilotage informatique de la Confédération)
NIST	National Institute of Standards and Technology
OFAE	Office fédéral pour l'approvisionnement économique du pays
OFCS / NCSC	Office fédéral de la cybersécurité / Centre national pour la cybersécurité
OFEN	Office fédéral de l'énergie
OFPP	Office fédéral de la protection de la population
OT	Operational Technology (en particulier systèmes SCADA)
PC	Personal Computer
PDC	Poste de détente et de comptage
PLC	Programmable Logic Controller
Réseau de communication	Réseau de communication interne pour les données et le vocal.
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.
SDL	Société de distribution locale
SMSI	Système de management de la sécurité de l'information
SNPC	Stratégie nationale de protection de la Suisse contre les cyber-risques
SVGW	Association pour l'eau, le gaz et la chaleur

STR	Société de transport régionale
TIC	Technologies de l'information et de la communication
UPIC	Unité de pilotage informatique de la Confédération
VoIP	Voice over IP
VPN	Virtual Private Network
WAN	Wide Area Network

6.2 Liste des images

6.3 Liste des tableaux

Impressum

Auteurs de la première version (2020)

Nom	Prénom	Organisation	Fonction
Peter	Sven	OFAE	Auteur principal / responsable du projet
Caduff	Daniel	OFAE	Co-auteur / expert / assurance qualité
Ernst	Philippe	SVGW	Co-auteur / expert / assurance qualité
Balmelli	Laurent	Cadre de l'AEP	Expert / assurance qualité
Modolell	Diego	SVGW	Expert / assurance qualité
Reichart	Karsten	SVGW	Expert / assurance qualité
Favarger	Hervé	SIG	Expert / assurance qualité
Cornu	Philippe	Holdigaz	Expert / assurance qualité
von Vivis	Marcel	Swisscom	Expert / assurance qualité
Häni	Reto	Deloitte	Expert / assurance qualité
Nyffeler	Gregor	EWZ	Expert / assurance qualité
Martin	Andre	GVM	Expert / assurance qualité
Munaron	Renato	A.EN	Expert / assurance qualité
Henry	Stéphane	OFEN	Expert / assurance qualité
von Ah	Matthias	Swissgas	Expert / assurance qualité
Angelini	Danilo	Transitgas	Expert / assurance qualité
Wolf	Andreas	EGO	Expert / assurance qualité
Rossat	Pierre-André	GAZNAT	Expert / assurance qualité

Auteurs/auteures de la deuxième version (2024)

Nom	Prénom	Organisation	Fonction
Peter	Sven	OFAE	Auteur principal / responsable du projet
Käser	Hans-Peter	OFAE / OFCS	Co-auteur / expert / assurance qualité
Räz	Barabra	OFAE	Co-auteure / experte / assurance qualité
Henry	Stéphane	OFEN	Co-auteur / expert / assurance qualité
Bonvin	Marc	OFEN	Co-auteur / expert / assurance qualité
Angelini	Danilo	Transitgas	Expert / assurance qualité
Bächtiger	Roger	ERI	Expert / assurance qualité
Breitschmied	Sandra	GVM	Experte / assurance qualité
Cavegn	Dominik	EGO	Expert / assurance qualité
Decurtins	Daniela	ASIG	Experte / assurance qualité
Geiger	Christoph	Swissgas	Expert / assurance qualité
Korosec	Wolfgang	Stadt SG	Expert / assurance qualité
Kühni	Marcel	Regionalwerke	Expert / assurance qualité
Marra	Sylvia	Oiken	Experte / assurance qualité
Menard	Caroline	SIG	Experte / assurance qualité
Niehörster	Christof	ASIG	Expert / assurance qualité
Reichart	Karsten	SVGW	Expert / assurance qualité
Monn	Remo	GAZNAT	Expert / assurance qualité
Schäfer	Charles	GVM	Expert / assurance qualité
Schüle	Roman	GVM	Expert / assurance qualité
Spörri	Hans	IBB	Expert / assurance qualité
Von Ah	Matthias	Swissgas	Expert / assurance qualité
Weber	Lukas	EGO	Expert / assurance qualité
Weber	Markus	Swissgas	Expert / assurance qualité
Wolf	Andreas	EGO	Expert / assurance qualité

Éditeur

Association pour l’eau, le gaz et la chaleur SVGW
Grütlistrasse 44, CH-8027 Zürich
info@svgw.ch, https://www.svgw.ch/de
Téléphone +41 44 288 33 33

Organisations impliquées dans l’élaboration :

Office fédéral pour l’approvisionnement économique du pays (OFAE),
Office fédéral de l’énergie (OFEN),
Association suisse de l’industrie gazière (ASIG) et
Association pour l'eau, le gaz et la chaleur (SVGW).