Cas pratique d'un tunnel routier
Partie 2 : mesures

La cybersécurité des systèmes industriels

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

Avertissement

Ce document est une étude de cas visant à illustrer les deux guides [SCADA-MTD, SCADA-MSR] publiés par l'ANSSI en janvier 2014. En particulier, il ne s'agit pas d'un document de bonnes pratiques ou de recommandations pour les systèmes industriels des tunnels routiers.
Bien que les auteurs se soient attachés à rendre cette étude la plus réaliste possible, certaines libertés ont été prises à des fins pédagogiques par rapport aux systèmes réellement rencontrés dans les tunnels routiers.

Synthèse

En 2014, le groupe de travail sur la cybersécurité des systèmes industriels (GTCSI), piloté par l'agence nationale de la sécurité des systèmes d'information (ANSSI), a publié deux guides :

- La cybersécurité des systèmes industriels - Méthode de classification et mesures principales [SCADA-MTD]
- La cybersécurité des systèmes industriels - Mesures détaillées [SCADA-MSR]

L'objectif de la présente étude de cas est d'illustrer ces deux guides par un exemple complet et concret : un tunnel routier.

La première partie de cette étude [SCADA-TNL-1] détaille la démarche complète de classification, montrant ainsi comment prendre en compte certains éléments.

Ainsi, après une présentation du périmètre et du contexte de l'étude de cas, les différentes menaces sont analysées en précisant les rapprochements possibles entre cybersécurité et sûreté de fonctionnement [1]. De ces menaces découlent alors la vraisemblance d'une attaque et donc la classe de chaque fonction. Enfin, les différents regroupements possibles entre classes sont comparés pour définir l'architecture finale.

La deuxième partie de l'étude de cas [SCADA-TNL-2] correspond à la déclinaison des mesures présentes dans les deux guides.

L'architecture retenue en fin de première partie est ainsi analysée de façon macroscopique, au regard des mesures principales du premier guide. Une proposition de sécurisation est ensuite faite à l'aide du second guide, en commençant par les mesures organisationnelles suivies des mesures techniques.

Enfin, il convient de rappeler qu'une analyse utilisant cette méthode n'est qu'une première approche permettant d'affirmer certains choix d'architecture et de mesures à appliquer. Elle ne dispense en rien d'une analyse de risque complète, qui est d'ailleurs une des mesures identifiées. De même, d'autres mesures peuvent être retenues de façon tout à fait valable si elles permettent de répondre au besoin de cybersécurité.

1. Voir le glossaire de la méthode de classification pour la définition de ces deux notions.

Table des matières

Chapitre 1

Introduction

Le présent document est issu des réflexions du groupe de travail sur la cybersécurité des systèmes industriels piloté par l'agence nationale de la sécurité des systèmes d'information (ANSSI). L'objectif des travaux de ce groupe, constitué d'acteurs du domaine des systèmes automatisés de contrôle des procédés industriels et de spécialistes de la sécurité des systèmes d'information (SSI), est de proposer un ensemble de mesures pour améliorer le niveau de cybersécurité des systèmes industriels. Les premiers travaux menés ont permis la publication en janvier 2014 de deux guides [SCADA-MTD, SCADA-MSR].

Le présent document est la seconde partie de cette étude de cas. Il décrit une déclinaison possible des mesures de protection présentes dans les deux guides, en l'appliquant au cadre de la sécurisation d'un tunnel routier. Il s'appuie largement sur les éléments de la première partie [SCADA-TNL-1] pour justifier certains choix.

L'étude a été menée par l'ANSSI en coopération avec des acteurs majeurs du domaine, dans la continuité du groupe de travail initial. Elle présente différentes mesures de protection envisageables en fonction d'hypothèses validées conjointement. Le scénario de sécurisation proposé repose tout autant sur des mesures organisationnelles que techniques : en effet, il arrive qu'une mesure technique puisse avantageusement remplacer une mesure organisationnelle ou réciproquement. La bonne articulation entre ces deux aspects permet d'atteindre un niveau de protection adéquat avec un coût acceptable.

Le chapitre 3, est consacrée à l'exploration des mesures de protection principales vues comme les axes de la stratégie de sécurisation.

Les chapitres 4 et 5 forment une proposition de sécurisation suivant les mesures détaillées du second guide, suivant respectivement l'axe organisationnel et l'axe technique.

Enfin deux annexes viennent compléter cette analyse : la première apporte un complément d'information sur certains éléments constituant le tunnel routier et les équipements mis en œuvre alors que la seconde présentent quelques exemples d'autres architectures pouvant répondre au besoin de cybersécurité.

Chapitre 2

Rappel du contexte de l'étude de cas

2.1 contexte

Comme indiqué dans sa première partie, l'étude de cas porte sur la sécurisation du système d'information industriel d'un tunnel routier fictif situé sous le mont Aigoual, sur la route reliant Meyrueis à Notre Dame de la Rouvière. Il s'agit d'un ouvrage neuf dans lequel des équipements de dernière génération pourront être déployés suivant les besoins. Il n'y a donc pas de gestion de l'existant ou de plan de migration à envisager.

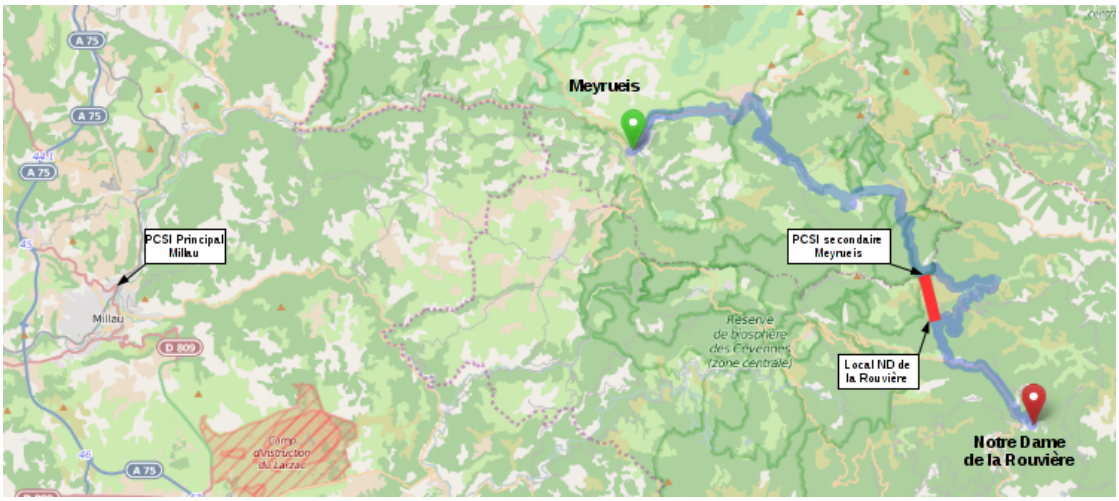

Figure 2.1 – *Tunnel - carte de situation*

2.2 Présentation de la société

Le tunnel routier sera exploité par la société (fictive) Tunnello. La directrice de cette société est Mme Alice et son responsable des opérations est M. Bob.

Pour mener à bien ces différentes tâches, la société Tunnello s'est adjoint les services de plusieurs prestataires [1], eux aussi fictifs, pour certaines tâches qu'elle ne

peut réaliser elle-même :

- Intégro assure la fourniture, l'intégration puis la maintenance du SI industriel ;
- Audito est en charge des différents audits informatiques nécessaires ;
- Formatio est en charge de la formation du personnel ;
- Telco est l'opérateur de télécommunication en charge des accès réseau (accès Internet et liaisons dédiées) ;
- Constructio est l'entreprise en charge du percement du tunnel.

Il est à noter que certaines mesures détaillées dans ce document ont un impact sur le choix des différents prestataires (exigences en matière de labellisation par exemple).

Bien que le nom des prestataires soit indiqué dès ce préambule pour faciliter la lecture du document, les exigences sont supposées avoir été prises en compte lors du choix des prestataires pour chaque scénario.

2.3 Organisation physique du tunnel

Le tunnel, sujet de l'étude, est un tunnel routier de type mono-tube à circulation bidirectionnelle d'une longueur de 2 550 m environ et comportant des locaux techniques (aussi appelés niches) tous les 200m. Du point de vue de la réglementation, il entre dans la catégorie des tunnels à faible trafic de longueur comprise entre 1 500 m et 3 000 m.

En temps normal, ce tunnel est supervisé depuis un poste de contrôle / commande principal distant (PCC) localisé à Millau et sous la responsabilité de la société Tunnello. Il dispose également d'un poste de contrôle / commande sur site, essentiellement utilisé en secours, localisé côté Meyrueis. En cas d'interruption de la circulation dans le tunnel, il faut, depuis le PCC de Millau, 1h30 pour se rendre à l'entrée du tunnel côté Notre-Dame-de-la-Rouvière et 2h côté Meyrueis.

2.4 Fonctions mises en œuvre dans le tunnel

Comme vu dans la première partie de cette étude, il est nécessaire de s'intéresser plus particulièrement aux fonctions suivantes [2], mises en place dans le tunnel :

- l'alimentation et la distribution électrique ;

1. Les noms de ces sociétés ont été choisies de façon à simplifire la compréhension de leur rôle dans la suite du document. Tout rapprochement avec une ou des sociétés existantes serait fortuit.
2. Voir la premère partie de l'étude pour plus d'information sur ces fonctions.

– l'indication des sorties de secours ;
– la ventilation [3] ;
– la signalisation ;
– la détection de véhicules hors gabarit ;
– la vidéo-surveillance ;
– la détection incendie ;
– le réseau d'appel d'urgence ;
– le contrôle de la qualité de l'air.

À cette liste s'ajoute le système de supervision industriel, qui bien qu'indispensable n'est pas traité comme une fonction indépendante dans cette étude. Il regroupe deux sous-fonctions :

– l'acquisition et le traitement des données, notamment de télémesures ;
– le contrôle des équipements par l'envoi de télécommandes et de téléréglages.

Ces deux sous-fonctions sont respectivement appelées *visualisation* et *pilotage* dès lors qu'une distinction est nécessaire dans la suite du document.

La fonction de supervision est assurée par Tunnello qui exploite le tunnel. Dans la suite de cette étude, les termes d'**administrateur métier**, d'**exploitant**, et également, par abus de langage, d'utilisateur de la solution, correspondent à ceux dont le rôle est d'assurer cette fonction de supervision.

Les fonctions de maintenance et d'administration, sur la solution de supervision comme sur les équipements présents dans le tunnel, sont assurées par la société Integro qui intègre et maintient la solution technique, en utilisant ses propres postes ou non. Dans la suite de cette étude, les termes d'**administrateur informatique** et d'**intégrateur**, correspondent à ceux dont le rôle est d'assurer ces fonctions d'administration.

2.5 Catégorisation des différentes fonctions

La première partie de l'étude a permis de déterminer dans un premier temps la classe des différentes fonctions, puis d'analyser la rationalisation apporté par le re-groupement des deux classes les plus élevées, configuration également notée « C1, C2+C3 » dans la première partie.

La figure 2.2 résume la classe de chaque fonction ainsi que les relations entre classes telles qu'elles seront développées dans la suite de l'étude.

3. Tunnello a retenu pour la ventilation et le désenfumage une stratégie transversale avec extraction concentrée.

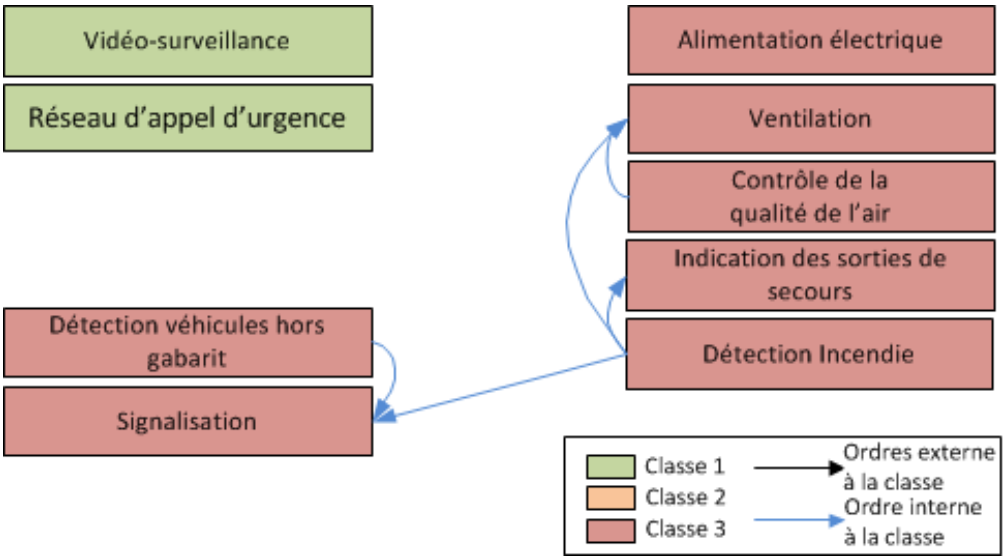

Figure 2.2 – *Schéma de flux - « C1, C2+C3 »*

Chapitre 3

Déclinaison des mesures principales

Après une utilisation macroscopique dans la première partie de l'étude pour choisir le regroupement le plus adapté, il est désormais temps de décliner de façon plus complète l'ensemble des mesures principales présentées dans le guide idoine [SCADA-MTD].

Ce chapitre est volontairement rédigé avec un point de vue plutôt « maîtrise d'ouvrage », c'est-à-dire celui de Tunnello, pour autant que la mesure s'y prête.

Il est rappelé que lorsque deux classes ou plus sont regroupées, ce sont les règles correspondant à la classe la plus sensible qui sont systématiquement appliquées.

3.1 Rôle et responsabilité

L'entreprise Tunnello décide de déléguer à son responsable de la sécurité des systèmes d'information (RSSI), M. Charlie, le rôle de responsable de la sécurité des systèmes industriels du tunnel. Il est assisté dans cette mission par les responsables d'exploitation et de maintenance.

Mme Alice, directrice de l'entreprise, conserve le rôle d'autorité qualifiée pour la sécurité des systèmes d'information (AQSSI).

3.2 Analyse de risque

Une partie des composants étant de classe 3, Tunnello missionne Audito, en sa qualité de prestataire labellisé, pour l'accompagner dans la réalisation de son analyse de risques.

Cette tâche portera sur l'ensemble des systèmes industriels. Tunnello et Audito s'appuieront sur Intégro, et sa connaissance de l'architecture et des équipements déployés, pour comprendre au mieux les besoins de protection pour les équipements essentiels à un fonctionnement du tunnel sans risque pour les usagers et le personnel, et identifier les vulnérabilités des équipements annexes.

Le marché prévoit par ailleurs une revue annuelle de cette analyse de risques.

3.3 Cartographie

Tunnello décide de faire réaliser une cartographie complète du système industriel du tunnel et des équipements qui y ont accès (en particulier depuis le poste de Millau). Cette cartographie couvre les points de vue physique et logique. Tunnello mandate Intégro, en charge de la maintenance du système, pour réaliser cette cartographie et la maintenir à jour. Cette dernière, normalement réalisée à chaque modification, est renforcée par une revue de l'ensemble des équipements de classe 3 (et donc aussi de classe 2) au moins une fois par an.

La démarche de cartographie du SI est lancée le plus en amont possible. Elle couvre l'ensemble des réseaux et permet de s'assurer de l'exhaustivité du résultat. Elle est la source du schéma 2.5.

La documentation est disponible sous format papier dans un local dédié, à côté de la salle de contrôle de Millau et dans le PCC de Meyrueis. Elle est aussi stockée sur deux disques durs chiffrés. Un stockage non chiffré est toléré pour les documents ne faisant apparaître que les équipements de classe 1.

3.4 Formation, contrôle et habilitation des intervenants

Formation et habilitation

Dans le cadre de son processus de gestion prévisionnelle des emplois et des compétences, Tunnello s'assure que les exploitants disposent d'un niveau de formation adapté à leur poste. Dans ce cadre, l'entreprise décide d'inclure un module de sensibilisation à la sécurité des systèmes d'information au cycle de formation interne des nouveaux entrants.

Cette formation initiale est complétée par une habilitation pour toutes les personnes ayant à intervenir sur les systèmes de classe 2 ou 3. Cette habilitation intègre une sensibilisation plus poussée. Les habilitations sont délivrées pour cinq ans, la formation étant rejouée lors des renouvellements. Ces habilitations sont réalisées par un organisme externe certifié lorsqu'elle concernent des équipements de classe 3 (et donc aussi ceux de classe 2).

Par ailleurs, lors de la contractualisation de la partie maintenance, Tunnello a vérifié avec Intégro que la formation des intervenants de ce dernier, suivie au titre de Prestataire qualifié en Intégration et Maintenance Spécialisé en Cybersécurité, n'était pas en désaccord avec la formation de ses propres personnels. Un rappel sur la

cybersécurité reste assuré par Tunnello lors de l'accueil des intervenants.

Contrôle

Afin d'assurer un bon niveau de suivi des intervenants, Tunnello intègre les informations nécessaires (identité, habilitations le cas échéant, équipements sur lesquels il est autorisé à intervenir) dans son système d'information de gestion des ressources humaines (SIRH). Ce dernier est complété d'une branche dédiée à la gestion des intervenants externes : des entrées sont créées suivant les déclarations des prestataires, avec une revalidation/prolongation des comptes par trimestre.

Tunnello transcrit les informations propres au SIRH (identité, comptes, habilitations le cas échéant, équipements sur lesquels Tunnello est autorisé à intervenir) dans des annuaires techniques, un pour la classe 1 et un pour les classes 2 et 3. Du fait du petit nombre de personnes concernés, Tunnello estime qu'une gestion manuelle des mises à jour des annuaires techniques est acceptable, la complexité d'un mécanisme de synchronisation automatique n'étant pas justifiée.

Tunnello demande à Intégro que, autant que possible, les équipements se réfèrent à l'annuaire technique de même niveau pour la gestion des autorisations et journalisent les accès via les mécanismes de supervision.

Pour les équipements de classe 3 (et donc aussi ceux de classe 2) ne pouvant se référer à l'annuaire technique ou ne pouvant journaliser les accès, Tunnello utilise des mesures organisationnelles pour assurer le contrôle et la traçabilité (voir section 3.13).

3.5 Audits

La direction de Tunnello a décidé de confier à Audito, prestataire d'audit labellisé, un contrat d'audit annuel pour 5 ans, sur les équipements de classe 2 et 3 du SI industriel. Ces audits sont réalisés sur des couvertures adaptées à chaque classe. Audito n'étant pas spécialisé dans les systèmes industriels, elle s'associe à un prestataire labellisé dans ce domaine, compétent sur les équipements en place et indépendant de Intégro pour assurer l'objectivité de l'audit.

Le contrat prévoit l'établissement d'un plan d'action formel par le prestataire en collaboration avec les équipes de production. Ce plan d'action est ensuite transmis à la direction de Tunnello pour validation et intégration au plan stratégique de la société.

Afin de limiter le périmètre de la prestation décrite ci-dessus, Intégro charge, après validation de Tunnello, une équipe interne dédiée à ce genre d'activité, d'assurer

l'audit de tout ou partie des équipements de classe 1 lors des évolutions de l'architecture ou le remplacement de matériel.

3.6 Processus de veille

La veille technologique doit s'appliquer aussi bien sur les matériels que sur les logiciels présents dans le système industriel. Régulièrement, un rapport doit être remis à l'AQSSI (cf. mesure 1) pour information du niveau de sécurité des composants.

N'ayant ni les ressources ni les compétences en interne, la direction de Tunnello charge Intégro d'assurer cette veille dans le cadre du contrat de maintenance du système. Pour ce faire, Intégro s'est abonné aux bulletins de sécurité des constructeurs de chacun des équipements du site, ainsi qu'aux bulletins de sécurité du CERT-FR [1].

Pour chaque nouvelle vulnérabilité, Intégro évalue l'exposition du système et les impacts potentiels pour décider avec les équipes d'exploitation et le responsable de la sécurité des systèmes industriels l'action à mener (acceptation et documentation du risque, mise à jour de l'équipement, mise en place de moyens palliatifs, etc.). Intégro est également chargé de remettre à l'AQSSI et au RSSI un tableau de situation pour information du niveau de sécurité des composants.

Le contrat prévoit pour les classes C2 et C3 des délais maximaux pour la mise à jour en cas de vulnérabilité jugée critique (une semaine pour les postes et équipements des PCC, un mois pour les équipements de terrain), ces délais pouvant être modulés par le RSSI.

Intégro s'engage enfin à être force de proposition sur les évolutions devant être envisagées au niveau du SI pour se protéger des nouvelles menaces portant sur tout ou partie des équipements de classe 2 ou 3.

3.7 Plans de reprise et de continuité d'activité

De par sa nature, la sûreté de fonctionnement impose une redondance, dans la mesure du possible, de tous les équipements nécessaires à la sûreté des utilisateurs. Cette redondance permet d'assurer un certain niveau de disponibilité du système, formant de fait les premières briques des PCA et PRA.

Pour l'homologation d'un tunnel routier, il est ainsi demandé à l'exploitant un dossier de sûreté complet, décrivant la gestion des divers scénarios d'incident et le niveau de résilience des composants mis en œuvre.

1. Cf. la page web `www.cert.ssi.gouv.fr`.

Dans le cas présent, Tunnello, avec l'aide de son prestataire Intégro, a mis en place une redondance des automates pour assurer la continuité du fonctionnement. La présence d'un poste de commandement local, permettant une prise en main complète de la supervision, est également à intégrer dans ces plans.

Enfin, la nécessité d'un PCA au delà de la gestion des incidents est limitée par la présence d'une route permettant de contourner le tunnel lorsque celui-ci est indisponible, comme indiqué dans le chapitre « Classification » de la première partie et plus particulièrement l'échelle des impacts en disponibilité.

3.8 Modes d'urgence

Des interrupteurs physiques de type « coup de poing » permettent de déclencher les fonctions vitales de façon manuelle (signalisation, indication des sorties de secours, ventilation en mode désenfumage), sans passer par les consoles de supervision.

Intégro a mis en place un compte administrateur permettant un accès local sur les divers équipements et réservé aux situations d'urgence. Ce compte est protégé par un mot de passe de complexité suffisante et unique par équipement. Ces mots de passe sont conservés dans des enveloppes scellées placées dans les coffres des PCC. Ces comptes administrateur sont utilisables aussi bien par un exploitant que par un intégrateur dès lors qu'il a accès au poste de maintenance et aux mots de passe en question.

Par ailleurs, des équipements de signalisation manuelle (torches, cornes, panneaux de signalisation mobile) sont accessibles sur site et dans les véhicules des intervenants pour pouvoir signifier une fermeture du tunnel ou guider des usagers, y compris lorsqu'il n'est pas possible de prendre la main sur le système industriel.

Le responsable d'exploitation doit s'assurer que le nécessaire est fait en cas d'usage de ces éléments : remplacement des consommables, recharge des batteries, remplacement des mots de passe dévoilés, etc.

Tunnello se charge de vérifier au moins une fois par an la présence et le bon état de ces éléments et les procédures associées.

3.9 Processus d'alerte et de gestion de crise

Dans le cadre du contrat qui le lie à son prestataire Intégro, Tunnello met en place les mécanismes de traitement suivants pour les incidents de sécurité concernant les systèmes d'information industriels :

– Mise en place d'une organisation en plusieurs niveaux, les exploitants de Tunnello assurant les niveaux 1 (qualification de l'incident et description la plus précise possible de l'environnement) et résolutions simples (remplacement d'ampoule, réarmement), ceux d'Intégro assurent les niveaux 2 (mise à jour, configuration) et 3 (ingénierie, gestion des problèmes).
– Mise en place d'un outil de gestion de tickets permettant le suivi des incidents et des problèmes. Les interventions issues du processus de veille, opéré conformément à la section 3.6, y sont également consignées.
– Mise en place d'une « cellule de crise » pouvant réunir rapidement les personnes concernées et compétentes en cas de nécessité. Les procédures afférentes sont consignées sur papier dans les deux postes de contrôle et chez Intégro. Elles sont également mises à disposition des autorités qui peuvent être amenées à faire suivre des remontées d'origines diverses.

Dans le cadre de son dossier de sécurité, Tunnello est tenu décrire ces processus de gestion de crise. De même, une liste à jour des incidents significatifs survenus dans le tunnel ainsi que leur analyse doit être mise à jour. Tunnello s'inscrit donc dans ce processus pour ce qui concerne les incidents de cybersécurité.

Par ailleurs, il est à noter qu'une crise de grande ampleur sera gérée par l'intermédiaire d'un plan tel que le Dispositif Orsec. Ce type de crise concerne toutefois les répercussions d'un incident matériel et humain et non les seuls aspects de sécurité du système d'information industriel.

3.10 Interconnexions réseau

Système d'information de gestion

Le réseau mis en œuvre par Intégro ne possède pas de connexion vers un système d'information de gestion.

Réseau public

De même, le réseau mis en œuvre par Intégro ne possède pas de connexion vers un réseau public, la liaison entre le poste de contrôle principal et le site du tunnel se faisant au travers de tunnels chiffrés et authentifiés. Celui-ci est réalisé au moyen d'une paire de passerelles VPN IPsec qualifiées dédiées à la classe considérée. Les flux y transitant sont par ailleurs protégés par des pare-feux qualifiés, eux aussi dédiés à chaque classe, positionnés de part et d'autre du tunnel VPN.

Ces différents VPN sont ensuite transportés sur une liaison spécialisée (segmentation par MPLS).

Systèmes industriels

Les postes de contrôle/commande, d'une part, et le système de terrain, d'autre part, sont considérés comme deux systèmes distincts au sein de la même architecture. Des pare-feux qualifiés, redondants et distincts, sont donc mis en place de part et d'autre de la liaison pour cloisonner les deux systèmes pour chacune des classes (C2 et C3 étant fusionnées).

3.11 Télédiagnostic, télémaintenance et télégestion

La Supervision permet de modifier le fonctionnement du système par l'intermédiaire de la sous-fonction Pilotage et son action possible sur les paramètres de consigne. En ce sens, la Supervision depuis le PCC de Millau forme un mécanisme de gestion à distance, ou télégestion.

Toutefois, cette Supervision a été intégrée dès le départ de l'analyse, que ce soit dans l'analyse de risque ou dans la définition des classes. De plus, la liaison entre le poste de contrôle principal et le site du tunnel se fait au travers d'un tunnel chiffré et authentifié sur une liaison spécialisée (segmentation par MPLS), comme indiqué plus haut dans ce chapitre (cf 3.10).

Intégrant les problématiques de sécurité des systèmes industriels dès la phase de conception, l'architecture mise en place par Intégro et Tunnello ne comporte pas de réseau d'administration[2]. En effet, Tunnello a estimé, après une première étude menée durant la phase projet, que les coûts et risques liés à ce type de fonctionnalité n'étaient pas justifiés du fait de la faible fréquence des actions de maintenance et du taux de panne habituel de ces équipements. Les modèles des différents matériels ont été choisis en conséquence pour permettre de limiter les ports physiques autorisant des actions d'administration ou de programmation.

Il n'est donc de fait pas possible de réaliser de la télémaintenance ou du télédiagnostic au-delà des informations remontées par les systèmes de supervision et de journalisation. Toute maintenance doit être réalisée au moyen d'une **connexion à un port dédié** de l'équipement depuis un poste nomade lui aussi dédié à la maintenance et sur lequel sont installés les outils dédiés.

2. Les modifications des firmwares, des programmes ou de la configuration sont considérées comme des actions d'administration. En l'absence de réseau d'administration, ces actions sont donc réalisées en connexion directe aux équipements.

La séparation géographique de ces deux fonctions (la Supervision étant réalisée depuis le PCC et la maintenance depuis le tunnel) impose de fait une séparation physique entre les postes permettant la réalisation de ces deux tâches.

La télégestion est assurée depuis des postes situés dans le poste de contrôle de Millau, un poste de supervision (ou plusieurs suivant le besoin) étant dédié à la classe 1, un second étant dédié à la classe 3 (et donc aussi à la classe 2).

3.12 Surveillance et moyens de détection

Journalisation

Pour répondre aux exigences de journalisation du cahier des charges fourni par Tunnello, Intégro a fait le choix d'une infrastructure de type syslog pour assurer la centralisation des journaux pour les équipements de sécurité (pare-feux et passerelles VPN), les postes ainsi que pour les équipements participant à la fonction de supervision.

De par l'architecture mise en œuvre, Intégro prévoit un serveur de journalisation par classe ou groupe de classe (donc un pour C1 et un pour C2+C3). Ceux-ci génèrent un rapport de synthèse à destination du service d'exploitation, sur une base quotidienne pour la classe 3 (et donc aussi pour les équipements de classe 2) et hebdomadaire pour la classe 1.

Au moins une fois par mois, un intervenant se rend sur place pour réaliser une collecte systématique des logs sur l'ensemble des équipements non raccordés au réseau.

Sondes de détection

Tunnello décide de renforcer la protection des équipements les plus sensibles par la mise en place de sondes de détection.

L'analyse de risque (voir section 3.2) indique que le point le plus sensible concerne l'interconnexion entre les ensembles « postes de contrôle/commande » et « système de terrain », tout particulièrement lorsque les équipements sont de classe 3. En effet, les équipements et les modalités de gestion mis en œuvre pour ces deux ensembles sont relativement différents.

Par ailleurs, les protocoles de communication sur la partie « système de terrain » ne pouvant tous être sécurisés malgré un choix attentif des équipements, Tunnello estime nécessaire, au vue de l'analyse de risque, une surveillance accrue de ces échanges.

De ce fait, une sonde est mise en place pour surveiller les échanges entre les deux ensembles de classe 3 (au sens large, c'est à dire recouvrant également C2 dans

le cas présent) par l'intermédiaire d'un miroir de port en aval du pare-feu, mis en place comme décrit précédemment (cf. 3.10). Une seconde sonde de détection est mise en place pour contrôler les échanges permettant l'interconnexion des API et de la détection incendie sur le réseau de terrain.

Les alarmes générées par le système de supervision sont transmises en temps réel à l'équipe d'exploitation, les modalités de prise en compte étant décrites dans le cadre de la gestion d'incidents (cf 3.9).

De même, les alertes générées par la centrale dédiée, et qui correspondent à des intrusions dans les locaux ou coffrets sous contrôle, remontent par un mécanisme approprié différencié. Les modalités de leur prise en compte sont également prévues dans le cadre de la gestion d'incidents (cf 3.9).

3.13 Gestion des interventions

Principes généraux

La gestion des habilitations et les principes du contrôle ont été abordés précédemment dans ce chapitre (cf 3.4).

Pour assurer les aspects opérationnels, Intégro et Tunnello ont mis en place un certain nombre de procédures.

Il est tout d'abord acté que toute intervention engendre la création d'un ticket dans le gestionnaire idoine quels que soient l'équipement concerné et l'intervention. Tunnello considère que ce gestionnaire de tickets fait office de carnet de consignation. Le ticket est renseigné avec date et heure, nom de l'intervenant, but de l'intervention, numéro des scellés retirés et reposés le cas échéant (voir plus loin). Le ticket peut être renseigné à l'avance lorsque l'intervention est prévue (maintenance programmée).

Accès aux locaux

Lorsqu'il se rend sur place, l'intervenant doit se signaler par téléphone au poste de contrôle central en début et fin d'intervention pour désactivation / réarmement des alarmes [3]. Si cela s'avère nécessaire, il doit également récupérer les outils de diagnostic et de maintenance cités ci-dessous, qui sont conservés au poste de contrôle secondaire, et les y redéposer en fin d'intervention.

3. Les alarmes sont remontées en temps réel et tracées dans les deux PCC. De même, les images de vidéo-surveillance sont enregistrées et accessibles en visualisation au niveau des PCC.

Comme l'outil de gestion des tickets a accès aux informations sur les habilitations et autorisations présentes dans l'annuaire technique, l'exploitant présent au poste de contrôle central a la possibilité de refuser l'accès (et ne pas désactiver les alarmes) à l'intervenant le cas échéant.

Tunnello a par ailleurs décidé d'utiliser des colliers numérotés à usage unique en guise de scellés lorsque cela s'avère nécessaire.

Pour assurer la protection physique des équipements de classe 3 (ou de classe 2), Tunnello a prévu lors de la phase de spécification/conception, et en accord avec Intégro, la mise en place de contrôle d'accès aux locaux par badge individuel, d'une alarme et de vidéo-surveillance pour les postes de contrôle principal et secondaire. La politique de sécurité réserve la délivrance de ces badges aux seuls intervenants internes.

Les autres locaux et coffrets, non protégés par le contrôle d'accès mais hébergeant des équipements de classe 3 (ou de classe 2) sont dotés d'une alarme, de scellés et de serrures dont les clés sont conservées dans une boîte à clé au sein du poste de contrôle secondaire. Leur accès nécessite donc indirectement l'utilisation du badge.

De fait, la procédure s'applique également aux équipements de classe 1 lorsqu'ils sont hébergés dans les mêmes locaux ou coffrets qu'un équipement de classe 2 ou 3.

L'obligation d'appeler le poste de contrôle principal est considérée par Tunnello comme un mécanisme de traçabilité suffisant pour les coffrets concernant la vidéo-surveillance (classe 1) dès lors que ces coffrets sont bien sous alarme. Une clé et des scellés sont donc confiés aux intervenants pour ces fonctions. La traçabilité permet par ailleurs à Intégro de pouvoir intervenir sur ces équipements sans la présence d'un exploitant de Tunnello.

Pour les autres coffrets ne contenant que des équipements de classe 1, les clés des coffres dédiés sont confiées aux intervenants en charge de ces fonctions.

Maintenance des équipements

Le cahier des charges stipule que les équipements de classe 2 et 3 doivent être fournis avec tous les outils matériels et logiciels nécessaires au diagnostic et aux interventions, et ce pour couvrir tous les cas de figure, sans tolérance particulière y compris pour les outils dont l'usage reste exceptionnel.

Le contrat de maintenance des équipements doit également couvrir les outils de diagnostic et de maintenance et leur mise à jour. Ces équipements sont acquis par la

société Tunnello et dédiés au site.

3.14 Schémas d'architecture

La liste des composants complémentaires, découlant comme précédemment des mesures principales, est donnée dans le tableau suivant.

Classe	Composants complémentaires
Classe 1	- poste de maintenance pour l'administration technique ; - SAS d'import (optionnel, non nécessairement connecté au réseau) ; - serveur de journalisation centralisé (optionnel) ;
Classe 3 (C2+C3)	- poste de maintenance pour l'administration technique (portable, disjoint du poste de supervision) ; - SAS d'import (non nécessairement connecté au réseau) ; - outils de diagnostic et d'interventions dédiés au site ; - serveur de journalisation centralisé ; - annuaire technique ; - pare-feux ; - VPN entre sites ; - solution de SIEM (optionnel) ; - solution de détection d'intrusion.

Le schéma d'architecture technique de la figure 3.1 représente un réseau de terrain de classe C2+C3 disjoint du réseau de terrain de classe C1. Chaque réseau est indépendant et les réseaux sont étanches entre eux.

Le poste de décontamination est matérialisé par un PC et une clé USB sécurisée par classe. Ce poste n'est raccordé à aucun réseau de supervision. Chaque site possède de manière indépendante son propre poste de décontamination.

Dans le cas des mises à jour, le poste de décontamination et la clé USB sécurisée sont utilisés de la manière suivante :

- l'opérateur dépose sur le poste de décontamination les composants logiciels dans un répertoire dédié dit « non sécurisé » (*sas d'entrée*) ;
- il effectue ensuite une copie du répertoire non sécurisé vers un répertoire sécurisé (*sas de sortie*) en appliquant les moyens de décontamination, c'est-à-dire l'exécution d'un antivirus ;
- à partir du *sas de sortie*, les composants sont ensuite copiés sur la clé sécurisée (cf. les moyens de sécurisation d'une clé USB) ;

– l'opérateur peut appliquer les mises à jour sur chaque composant matériel à l'aide de la clé sécurisée.

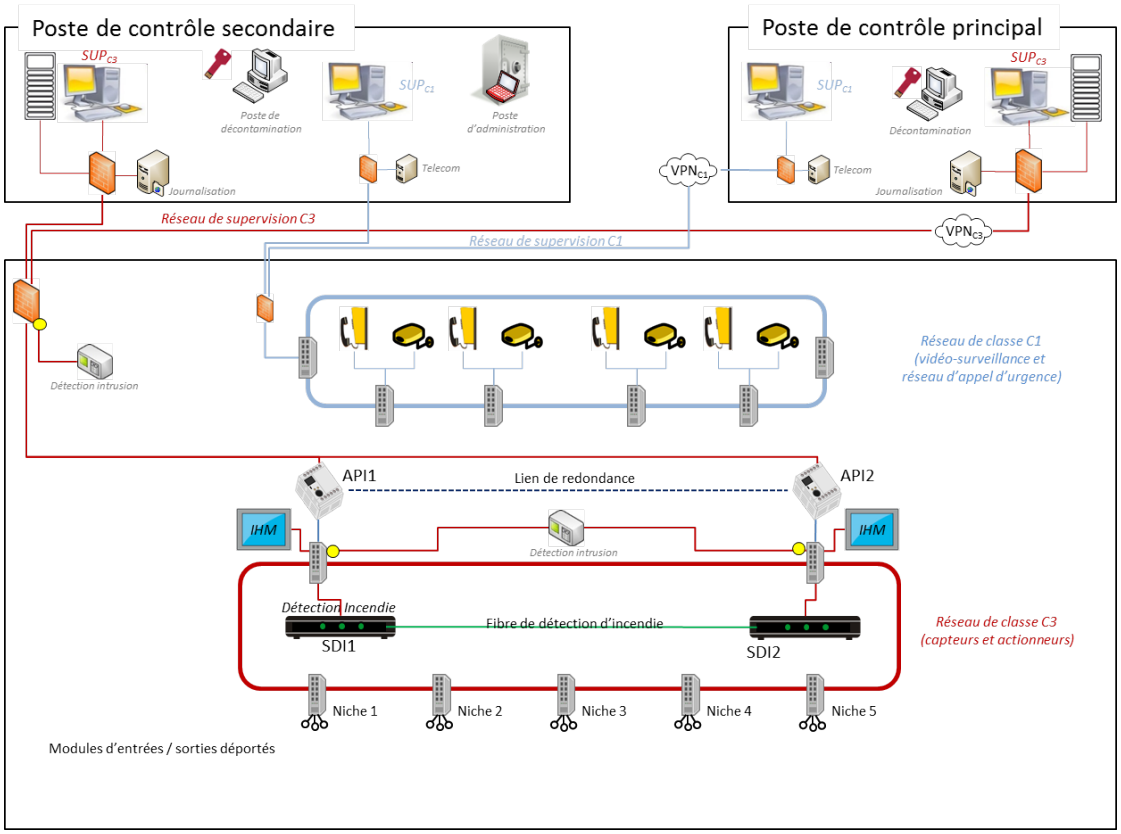

Figure 3.1 – *Système industriel - Architecture technique sécurisée « C1, C2+C3 »*

Chapitre 4

Déclinaison des mesures détaillées de type organisationnelles

Comme nous avons pu le voir dans les chapitres précédents, la méthode de classification permet de dégager trois classes en matière de besoin en cybersécurité.

Suite à l'analyse des mesures principales sur les différentes segmentations envisagées, Tunnello décide de retenir la solution reposant sur le regroupement de deux des trois classes, à savoir C2 et C3 d'un côté et C1 de l'autre.

Le schéma de la figure 4.1 fait apparaître les différents composants logiques (dont les modules applicatifs) qui contribuent à la sécurisation du système industriel.

On se reportera à la figure 3.1 en section 3.14 pour la vue technique de l'architecture.

Ce chapitre a pour but de décliner l'ensemble applicable des directives détaillées, ainsi que les recommandations que Tunnello et Intégro estiment justifiées d'appliquer. Pour faciliter la lecture, l'organisation de ce chapitre est similaire à celle du guide de l'ANSSI, dédié aux mesures détaillées [SCADA-MSR]. Par ailleurs, il reprend, dans un esprit de complétude [1], l'ensemble des mesures principales décrites dans le chapitre précédent, pour les compléter. La reprise de certaines parties du chapitre 3 est donc voulue, dans un objectif de récapitulatif complet concernant la configuration retenue (i.e. « C1, C2+C3 »).

À l'inverse du chapitre 3, ce chapitre est volontairement rédigé avec un point de vue plutôt « maîtrise d'œuvre », c'est-à-dire essentiellement l'intégrateur Intégro dans le cas présent, lorsque les mesures s'y prêtent.

1. Cela inclut par exemple la prise en compte de la cybersécurité dans les phases d'étude ou la justification d'éléments techniques déjà présents dans la figure 3.1.

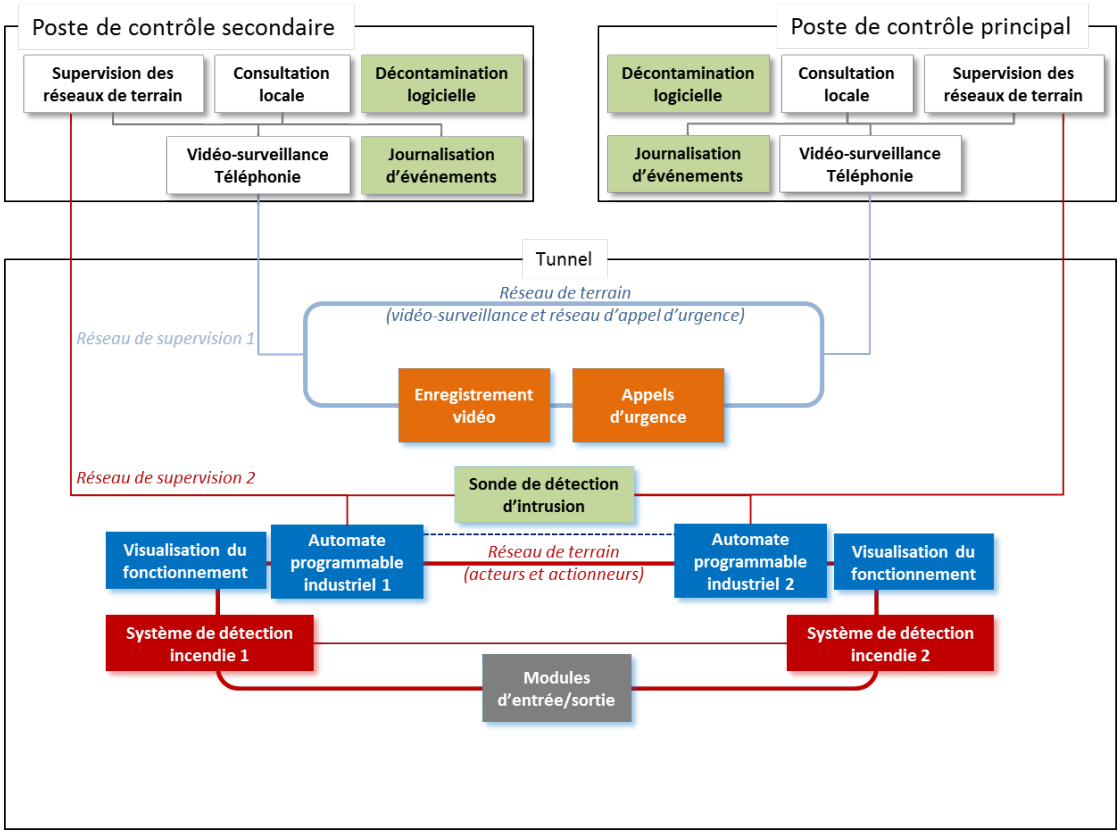

Figure 4.1 – *Système industriel - Architecture logique après déroulé de la méthode*

4.1 Connaissance du système

4.1.1 Rôles et responsabilités

Résumé des mesures détaillées

Une chaîne de responsabilité de la cybersécurité doit être mise en place et couvrir l'ensemble des systèmes industriels.

L'entreprise Tunnello décide de déléguer à son responsable de la sécurité des systèmes d'information (RSSI), M. Charlie, le rôle de responsable de la sécurité des systèmes industriels du tunnel. Il est assisté dans cette mission des responsables d'exploitation et de maintenance.

Mme Alice, directrice de l'entreprise, conserve le rôle d'autorité qualifiée pour la

sécurité des systèmes d'information (AQSSI).

4.1.2 Cartographie

Résumé des mesures détaillées

Une cartographie complète du système industriel doit être produite.

Tunnello décide de faire réaliser une cartographie complète du système industriel du tunnel et des équipements qui y ont accès (en particulier depuis le poste de Millau). Cette cartographie couvre différents points de vue, dont les architectures physique et logique, la carte des rôles et responsabilités et la matrice des flux. Intégro est mandaté par Tunnello pour réaliser cette cartographie et la maintenir à jour suivant les modalités décrites ci-dessous.

La démarche de cartographie du SI est initiée en amont de la présente analyse et couvre l'ensemble des réseaux. Elle doit permettre de s'assurer de l'exhaustivité du résultat. Elle est la source des schémas des figures 4.1 et 3.1.

Il est demandé à Intégro de mettre à jour la cartographie et les inventaires à chaque modification, en lien avec les données de la GMAO (gestion de maintenance assistée par ordinateur). Intégro mènera également une revue de l'ensemble des équipements au moins une fois par an.

La documentation est disponible sous format papier dans un local dédié, à côté de la salle de contrôle de Millau et dans le poste de contrôle de Meyrueis. Elle est aussi stockée sur deux disques durs chiffrés.

4.1.3 Analyse de risque

Résumé des mesures détaillées

Les systèmes industriels doivent faire l'objet d'une analyse de risques détaillée suivant une méthode choisie par l'entité responsable.

Au moins un composant étant de classe 3 quelle que soit la configuration retenue, Tunnello missionne Audito, en sa qualité de prestataire qualifié, pour l'accompagner dans la réalisation de son analyse de risques. Durant cette tâche, qui portera sur

l'ensemble des systèmes industriels, Tunnello et Audito s'appuieront sur Intégro, et sa connaissance des équipements déployés, pour comprendre au mieux les objectifs des biens essentiels et leur fonctionnement, et identifier les vulnérabilités des biens supports.

Le marché prévoit par ailleurs une revue annuelle de cette analyse de risques.

4.1.4 Gestion des sauvegardes

Résumé des mesures détaillées

Une politique de sauvegarde doit être mise en place pour s'assurer de la protection des données importantes et des configurations. Cette politique doit entre autre comporter des tests de restauration réguliers et ne doit pas remettre en cause le cloisonnement entre les classes. La sauvegarde doit de plus reposer sur une infrastructure adaptée.

Intégro met en place une infrastructure de sauvegarde dédiée au tunnel pour la sauvegarde des serveurs de journalisation et des différentes stations. Ils font l'objet d'une sauvegarde complète hebdomadaire et d'une sauvegarde différentielle quotidienne.

Pour les équipements du SI industriel, les procédures précisent que toute modification de configuration ou mise à jour doit être suivie d'une sauvegarde manuelle. La politique de sauvegarde précise que les sauvegardes conservées doivent couvrir les cinq dernières modifications et les trois derniers mois.

4.1.5 Gestion de la documentation

Résumé des mesures détaillées

Une classification de la documentation doit être faite de façon cohérente pour chaque classe. Le stockage et la gestion des accès à la documentation doivent se faire de façon adaptée, de sorte que les intervenants puissent y avoir accès en accord avec leur besoin d'en connaître. Un processus de revue doit être prévu de façon globale.

L'ensemble des documents sont regroupés sur un poste bureautique déconnecté du reste du SI et mis à disposition des intervenants. Chaque intervenant ne peut consulter que les documents concernant les équipements sur lesquels il est habilité à

intervenir. De plus, une copie papier des documents les plus critiques (et nécessaires y compris en cas d'arrêt de service du poste de documentation) est conservée dans un coffre-fort dans le poste de contrôle secondaire. Cela concerne par exemple la documentation nécessaire au redémarrage du SI après un arrêt de service, volontaire ou non, éventuellement les informations utiles issues des contrats de support, etc.

Ce poste de documentation est inclus dans la politique de sauvegarde : s'agissant d'un poste déconnecté du réseau, la sauvegarde est assurée manuellement et gérée suivant les mêmes procédures que pour les équipements réseaux.

La direction opérationnelle prévoit de plus dans son planning une demi-journée par an dédiée à la vérification des documentations et plus particulièrement leur bonne mise à jour.

4.2 Maîtrise des intervenants

4.2.1 Gestion des intervenants

Résumé des mesures détaillées

La classe 3 nécessite la mise en place de procédures de gestion des intervenants, de leurs compétences, et de leur matériel, ainsi que la gestion des comptes et des droits associés. Cette procédure peut être unique et transverse. Par transitivité, cette procédure peut être facilement étendue sur la classe 1, même si elle n'est qu'optionnelle.
La classe 3 impose également une revue annuelle des intervenants et de leurs droits.

Afin d'assurer un bon niveau de suivi des intervenants, Tunnello intègre les informations nécessaires (identité, niveau d'habilitation le cas échéant, équipements sur lesquels l'intervenant est autorisé à intervenir) dans son système d'information de gestion des ressources humaines (SIRH). Ce dernier est complété d'une branche dédiée à la gestion des intervenants externes : des entrées sont créées suivant les déclarations des prestataires, avec une re-validation/prolongation des comptes effectuée par trimestre.

Tunnello transcrit les informations utiles du SIRH (identité, comptes, habilitations le cas échéant, équipements sur lesquels l'intervenant est autorisé à intervenir) dans des annuaires techniques (pour la configuration retenue, un pour les classes 2 et

3, et un pour la classe 1). Du fait du petit nombre de personnes concernées, cette transcription se fait via la création manuelle de comptes.

4.2.2 Sensibilisation et formation

Résumé des mesures détaillées

L'ensemble des intervenants doit être habilité et contrôlé. La formation à la cybersécurité comprise dans l'habilitation devrait être assurée par des prestataires qualifiés en Intégration et Maintenance Spécialisé en Cybersécurité ou à défaut des prestataires respectant les référentiels d'exigences.

Dans le cadre de son processus de gestion prévisionnelle des emplois et des compétences, Tunnello s'assure que les exploitants disposent d'un niveau de formation adapté à leur poste. Dans ce cadre, l'entreprise décide d'inclure un module de sensibilisation à la sécurité des systèmes d'information au cycle de formation interne des nouveaux entrants.

Par ailleurs, pour répondre aux exigences contractuelles mises en place par Tunnello, Intégro, prestataire qualifié, s'assure du bon niveau de formation de ses intervenants. Il s'assure également, par précaution, que cette formation ne contient pas de désaccord majeur avec celle reçue par le personnel de Tunnello. Un rappel sur la cybersécurité reste assuré par Tunnello lors de l'accueil sécurité des intervenants.

La formation initiale des intervenants donne lieu à une habilitation délivrée pour 5 ans, la formation étant dispensée à nouveau lors des renouvellements de personnel. Ces habilitations sont réalisées par un organisme externe certifié lorsqu'elles concernent des équipements de classe 3 (et donc aussi ceux de classe 2), et peuvent être gérées en interne pour les équipements de classe 1.

Enfin, les salariés d'Intégro se voient interdire par Tunnello toute intervention sur les équipements de classe 3 (et de classe 2) avant leur habilitation effective, avec dérogation nominative possible pour les exploitants internes en cours d'habilitation lorsque l'intervention est encadrée par un exploitant habilité. Cette interdiction est de fait également valable pour les autres sous-traitants et les propres exploitants de Tunnello.

4.2.3 Gestion des interventions

Résumé des mesures détaillées

Outre la mise en place de procédures pour encadrer les interventions, la classe 3 impose que la société dispose de l'intégralité des outils et équipements nécessaires aux différentes interventions sur le SI, y compris les équipements de diagnostic spécifiques.

Toute intervention engendre la création d'un ticket dans le gestionnaire idoine quels que soient l'équipement concerné et l'intervention, Tunnello considérant que ce gestionnaire fait office de carnet de consignation. Celui-ci est renseigné avec date et heure, nom de l'intervenant, but de l'intervention, numéro des scellés retirés et posés le cas échéant (voir plus loin). Le ticket peut être renseigné à l'avance lorsque l'intervention fait l'objet d'une maintenance programmée.

Concernant les moyens matériels pour permettre l'intervention sur les équipements, le cahier des charges émis par Intégro auprès de ses propres partenaires et fournisseurs dans le cadre de ce contrat stipule que les équipements de classe 2 et 3 doivent être fournis avec tous les outils matériels et logiciels nécessaires aux diagnostics et aux interventions, et ce pour couvrir tous les cas de figure, sans tolérance particulière y compris pour les outils dont l'usage reste exceptionnel.

Le contrat de maintenance des équipements doit également couvrir les outils de diagnostic et de maintenance et leur mise à jour. Ces équipements sont acquis par la société Tunnello, et dédiés au site.

4.3 Intégration de la cybersécurité dans le cycle de vie du système industriel

4.3.1 Exigences dans les contrats et cahiers des charges

Résumé des mesures détaillées

La classe 3 impose la formalisation dès le cahier des charges d'une liste d'exigences attendues, de documents d'analyse préliminaire et d'un plan de tests sur les aspects de la cybersécurité.

Les procédures d'achat en vigueur au sein de Tunnello indiquent que tout appel d'offre d'études impactant les systèmes industriels doit comporter un volet sur la cybersécurité de ces systèmes, reprenant notamment les directives et recommandations présentées dans le guide sur les mesures détaillées (sans pour autant se limiter à cette liste). Tunnello a décidé de généraliser ce volet à tous ses appels d'offres, quelle que soit la classe des équipements concernés, seule la pondération de ce critère variant suivant qu'il s'agisse d'un équipement de classe 1 ou de classe supérieure.

L'appel d'offre portant sur la réalisation du système équipant le tunnel est donc doté d'un tel volet, en amont des phases de conception et de spécification.

Par ailleurs, M. Charlie, en tant que RSSI, est désigné comme point de contact cybersécurité. Il s'assure donc que le cahier des charges inclut une clause de confidentialité si besoin, ainsi que du respect des règles de cybersécurité dès la phase projet (traçabilité, plan d'assurance sécurité, auditabilité, utilisation d'un environnement de développement sécurisé).

4.3.2 Intégration de la cybersécurité dans les phases de spécification

Résumé des mesures détaillées

Les opérations non nécessaires à la conduite doivent se faire sur un SI séparé. La conception intègre en plus la protection de la configuration et la gestion des vulnérabilités. Les matériels et prestataires doivent être labellisés.

Les procédures d'achat en vigueur au sein de Tunnello indiquent que tout appel d'offres d'études impactant les systèmes industriels doit comporter un volet sur la cybersécurité de ces systèmes, reprenant notamment les directives et recommandations présentées dans le guide sur les mesures détaillées (sans pour autant se limiter à cette liste).

L'appel d'offres portant sur les spécifications du système équipant le tunnel était donc doté d'un tel volet, en amont de la phase de conception.

4.3.3 Intégration de la cybersécurité dans les phases de conception

Résumé des mesures détaillées

La complexité doit être réduite au maximum, et les caractéristiques en terme de cybersécurité doivent être prises en compte dans le choix du matériel. En particulier, la capacité à séparer administrateurs et utilisateurs doit être prise en compte dès la phase de conception.

Les procédures d'achat en vigueur au sein de Tunnello indiquent que tout appel d'offres d'études impactant les systèmes industriels doit comporter un volet sur la cybersécurité de ces systèmes. L'appel d'offres portant sur la conception du système équipant le tunnel est donc doté d'un tel volet.

4.3.4 Audits et tests de cybersécurité

Résumé des mesures détaillées

Des audits réguliers doivent être mis en place et être effectués au moins une fois par an. Ces audits devraient être réalisés par des prestataires indépendants labellisés.

La direction de Tunnello a décidé de confier à Audito, prestataire d'audit labellisé, un contrat d'audit annuel pour 5 ans, sur les équipements de classe 2 et 3 du SI industriel. Audito n'étant pas spécialisé dans les systèmes industriels, elle s'associe à un prestataire labellisé pour la maintenance dans le domaine, compétent sur les équipements en place et indépendant d'Intégro pour garantir l'objectivité de l'audit.

Le contrat prévoit l'établissement d'un plan d'action formel par le prestataire en collaboration avec les équipes de production. Ce plan d'action est ensuite transmis à la direction pour validation et intégration au plan d'évolution des SI de la société Tunnello.

4.3.5 Transfert en exploitation

Résumé des mesures détaillées

Les systèmes doivent être homologués et requièrent une autorisation préalable de mise en service.

Intégro est chargé de mettre en place le dossier d'homologation, conformément à la procédure décrite dans le guide idoine de l'ANSSI [GD-HOMOL]. Le dossier comprend entre autres l'analyse de risque et la cartographie, ainsi qu'une liste des menaces et une analyse des mesures de protection prévues en regard. Il comprend également le rapport d'audit initial réalisé par Audito, réalisé tel que décrit dans la section précédente et utilisé par Intégro pour son plan d'amélioration.

Le dossier est présenté en commission d'homologation SSI. En particulier, l'AQSSI prend la responsabilité d'accepter les risques résiduels relevés avant toute mise en service.

4.3.6 Gestion des modifications et des évolutions

Résumé des mesures détaillées

Les mises à jour doivent être tracées.
Lors d'une mise à jour, il est possible de comparer la version courante et la version à installer pour s'assurer que tous les changements sont nécessaires. Par ailleurs, un contrôle d'intégrité sur les programmes et les fichiers de configuration doit être mené lors de l'exécution. Enfin les tests sont menés sur un environnement dédié.

Dès le cahier des charges, Tunnello a demandé que les problématiques d'intégrité et d'authenticité soient prises en compte, idéalement au moyen d'une signature des binaires par l'équipementier ou l'intégrateur lorsque celui-ci est intervenu pour les personnaliser.

Bien que ne disposant pas au final de l'infrastructure permettant la signature de l'ensemble des binaires, Intégro a néanmoins été considéré comme suffisamment de confiance lors de l'attribution du marché, du fait de son statut de prestataire qualifié.

Tunnello et Intégro sont donc convenus d'une procédure privilégiant un calcul du hash de tous les fichiers livrés au moment du passage par le SAS du poste de dé-

contamination (cf. 3.14), avec vérification visuelle des hashs fournis par un moyen de diffusion différent des binaires (fax, courrier papier et courrier électronique signé sont des moyens acceptés). Intégro devra s'assurer de l'intégrité de tous les fichiers fournis par le constructeur. Si cette procédure est systématiquement mise en œuvre pour les modifications concernant les équipements de classe 2 et 3, les équipements de classe 1 peuvent être gérés en mode *best effort*.

Par ailleurs, l'intégrateur fournit un différentiel entre les versions pour le code dont il a la maîtrise et pour les modifications apportées aux configurations. Il s'engage contractuellement à fournir une note de version présentant de façon exhaustive (mais hiérarchisée dans la mesure du possible) toutes les modifications apportées aux fichiers.

4.3.7 Processus de veille

Résumé des mesures détaillées

Un processus de veille doit être mis en place afin de se tenir informé :
- de l'évolution de la menace et des techniques d'attaque ;
- des vulnérabilités identifiées sur les produits et technologies mis en œuvre sur les systèmes industriels ;
- de l'évolution des mécanismes de protection.

La veille technologique doit s'appliquer aussi bien sur les matériels que sur les logiciels présents dans le système industriel. Régulièrement, un rapport doit être remis à l'AQSSI (cf. mesure 1) pour information du niveau de sécurité des composants.

N'ayant ni les ressources ni les compétences en interne, la direction de Tunnello charge Intégro d'assurer cette veille dans le cadre du contrat de maintenance des équipements. Pour ce faire, Intégro s'est abonné aux bulletins de sécurité des constructeurs de chacun des équipements, ainsi qu'aux bulletins de sécurité du CERT-FR [2].

Pour chaque nouvelle vulnérabilité, Intégro évalue l'exposition du système et les impacts potentiels pour décider, avec les responsables de la sécurité des systèmes industriels, de l'action à mener (acceptation et documentation du risque, mise à jour de l'équipement, moyens palliatifs, etc.).

Enfin, Intégro est chargé de remettre à l'AQSSI et au RSSI un tableau de situation pour information du niveau de sécurité des composants.

2. Cf. le site `www.cert.ssi.gouv.fr`.

Intégro s'engage par ailleurs à être force de proposition sur les évolutions devant être envisagées au niveau du SI pour se protéger des nouvelles menaces portant sur tout ou partie des équipements.

4.3.8 Gestion de l'obsolescence

Résumé des mesures détaillées

L'obsolescence doit être gérée dès la phase de contractualisation, en notifiant notamment une durée maximale de prise en charge.

Tunnello a exigé dès son cahier des charges l'obligation contractuelle d'être prévenu de la fin de vie des équipements déployés dès connaissance de la date de fin de commercialisation et au moins trois ans avant l'arrêt effectif du support.

Par ailleurs, il revient à Intégro de s'assurer qu'il dispose bien des accès suffisants auprès des services de support des différents constructeurs pour assurer la maintenance des équipements déployés jusqu'à l'arrêt effectif du support.

4.4 Sécurité physique et contrôle d'accès aux locaux

4.4.1 Accès aux locaux

Résumé des mesures détaillées

Une politique d'accès doit être mise en place, permettant de s'assurer que les seules personnes disposant des clés et codes d'accès en ont besoin et sont des intervenants internes (sauf s'il est possible de tracer les accès des intervenants externes). Cela implique donc qu'un prestataire ne doit pas intervenir seul, sauf si son accès est traçable.
Les accès doivent être tracés, auditables et protégés par une mise sous alarme et sous vidéoprotection.

Lorsqu'il se rend sur place, l'intervenant doit se signaler par téléphone au poste de contrôle central en début et fin d'intervention pour désactivation/réarmement des alarmes. Si cela s'avère nécessaire, il doit également récupérer les outils de diagnostic

et de maintenance (voir « Gestion des interventions » dans la section), qui sont conservés au PCC secondaire, et les y redéposer en fin d'intervention.

Comme l'outil de gestion des tickets a accès aux informations sur les habilitations et autorisations présentes dans l'annuaire technique, l'exploitant présent au poste de contrôle central a la possibilité de refuser l'accès (et ne pas désactiver les alarmes) à l'intervenant le cas échéant.

Pour assurer la protection physique des équipements de classe 3 (et donc aussi ceux de classe 2), Intégro et Tunnello ont prévu, lors de la phase de spécification / conception, la mise en place d'un contrôle d'accès aux locaux par badge individuel, d'une alarme pour les postes de contrôle principal et secondaire. Ces mesures sont par ailleurs complétés par la vidéo-surveillance présente dans le tunnel. La politique de sécurité réserve la délivrance de ces badges aux seuls intervenants internes.

4.4.2 Accès aux équipements et aux câblages

Résumé des mesures détaillées

Les serveurs doivent être placés dans des locaux protégés comme décrit ci-dessus. Les équipements sensibles du SI industriel doivent être placés sous clé et aucune prise réseau ne doit être accessible dans des espaces publics. L'ouverture des armoires contenant les équipements sensibles du SI industriel doit être tracée (a minima par des alarmes et des scellés).

En complément des points concernant l'accès aux locaux, Tunnello a décidé d'utiliser des colliers numérotés à usage unique en guise de scellés lorsque cela s'avère nécessaire.

Les locaux et coffrets non protégés par le contrôle d'accès mais hébergeant des équipements de classe 2 ou 3 sont dotés d'une alarme, de scellés et de serrures dont les clés sont conservées dans une boîte à clé au sein du poste de contrôle secondaire. Leur accès nécessite donc indirectement l'utilisation d'un badge.

De fait, la procédure s'applique également aux équipements de classe 1 lorsqu'ils sont hébergés dans les mêmes locaux ou coffrets que des équipements de classe 3 (ou de classe 2).

L'obligation d'appeler le poste de contrôle principal est considérée par Tunnello comme un mécanisme de traçabilité suffisant pour les coffrets contenant des équipements de classe 1 dès lors que les coffrets sont bien sous alarme. Une clé et des

scellés sont donc confiés aux intervenants pour ces fonctions. La traçabilité permet par ailleurs à Intégro de pouvoir intervenir sur ces équipements sans la présence d'un exploitant de Tunnello.

Les caméras de vidéo-surveillance sont par ailleurs installées en caissons anti-vandalisme avec scellés.

4.5 Réaction en cas d'incident

4.5.1 Plan de reprise ou de continuité d'activité

Résumé des mesures détaillées

Des plans de reprise ou de continuité d'activité doivent être mis en œuvre et testés au moins annuellement.

De par sa nature, la sûreté de fonctionnement impose une redondance, dans la mesure du possible, de tous les équipements nécessaires à la sécurité des utilisateurs. Cette redondance permet d'assurer un certain niveau de disponibilité du système, formant de fait les premières briques des PCA et PRA.

Avant la mise en service d'un tunnel routier, il est ainsi demandé à l'exploitant un dossier de sûreté complet, décrivant la gestion des divers scénarios d'incident et le niveau de résilience des composants mis en œuvre.

Dans le cas présent, Intégro a mis en place une redondance des automates pour assurer la continuité du fonctionnement, en accord avec les exigences de Tunnello. La présence d'un poste de commandement local permettant une prise en main complète de la supervision, est également à intégrer dans ces plans, de même que l'existence d'une sauvegarde des données régulièrement vérifiée (voir « Gestion des sauvegardes » en section 4.1.4).

Enfin, la nécessité d'un PCA, au delà de la gestion des incidents, est limitée par la présence d'une route permettant de contourner le tunnel lorsque celui-ci est indisponible, comme indiqué au chapitre décrivant les impacts en disponibilité.

4.5.2 Modes dégradés

Résumé des mesures détaillées

Des procédures d'intervention d'urgence et de fonctionnement en mode dégradé doivent être prévues. Ces procédures doivent maintenir la traçabilité des actions.

Des interrupteurs physiques de type « coup de poing » permettent de déclencher les fonctions vitales de façon manuelle (signalisation, indication des sorties de secours, ventilation en mode désenfumage), sans passer par les consoles de supervision.

Intégro a mis en place un compte administrateur technique permettant un accès local sur les divers équipements. Ce compte est protégé par un mot de passe de complexité suffisante et unique par équipement. Ces mots de passe sont conservés sous enveloppe scellée placées dans le coffre de chacun des postes de commandement.

Par ailleurs, des équipements de signalisation manuelle (torches, cornes, panneaux de signalisation mobiles) sont accessibles sur site et dans les véhicules des intervenants pour pouvoir signifier une fermeture du tunnel ou guider des usagers, y compris lorsqu'il n'est pas possible de prendre la main sur le système industriel.

Le responsable d'exploitation doit s'assurer que le nécessaire est fait en cas d'usage de ces éléments : remplacement des consommables, recharge des batteries, remplacement des mots de passe dévoilés, etc.

Tunnello se charge de vérifier au moins une fois par an la présence et le bon état de ces éléments.

4.5.3 Gestion de crise

Résumé des mesures détaillées

Des procédures de gestion de crise doivent être mises en place conformément aux directives D.118 à D.120. Ces procédures doivent être testées annuellement.

Dans le cadre du contrat qui le lie à son prestataire Intégro, Tunnello met en place les mécanismes de traitement suivants pour les incidents de sécurité concernant les systèmes d'information industriels :

- Mise en place d'une organisation en plusieurs niveaux, les exploitants de Tunnello assurant les niveaux 1 (qualification de l'incident, incluant une description la plus précise possible de l'environnement, et résolutions simples tels que remplacement d'ampoule, réarmement, etc.), ceux d'Intégro les niveaux 2 (mise à jour, configuration) et 3 (ingénierie, gestion des problèmes).
- Mise en place d'un outil de gestion de tickets permettant le suivi des incidents et des problèmes. Les interventions issues de remontées du processus de veille y sont également consignées.
- Mise en place d'une « cellule de crise » pouvant réunir rapidement les personnes concernées et compétentes en cas de nécessité. Les procédures afférentes sont consignées sur papier dans les deux postes de contrôle et chez Intégro. Elles sont également mises à disposition de la direction départementale de l'équipement qui peut être amenée à faire suivre des remontées d'origines diverses.

Ces processus de gestion opérationnelle d'incidents et les noms des personnes à contacter en cas d'urgence sont communiqués à l'autorité de cybersécurité.

Il est par ailleurs à noter qu'une crise de grande ampleur sera gérée par l'intermédiaire d'un plan tel que le dispositif ORSEC. Ce type de crise concerne toutefois les répercussions d'un incident matériel et non les seuls aspects de sécurité du système d'information industriel.

Chapitre 5

Déclinaison des mesures détaillées au niveau technique

Dans la continuité du précédant, ce chapitre décrit un ensemble de choix possibles ainsi que leur mise en œuvre.

5.1 Authentification des intervenants : contrôle d'accès logique

5.1.1 Gestion des comptes

Résumé des mesures détaillées

Les utilisateurs doivent utiliser des comptes individuels, supprimés à leur départ, les comptes génériques étant à proscrire sauf contrainte forte. Les comptes d'administration ou à privilèges doivent être protégés par une authentification disjointe de celle des comptes standards. Des rôles seront mis en place pour s'assurer que les droits correspondent aux seuls besoins. Une revue locale ou centralisée des comptes et des droits associés, doit être organisée de façon annuelle.

Intégro configure les composants se trouvant dans les postes de contrôle pour qu'ils se réfèrent pour la gestion des autorisations à l'annuaire technique de leur niveau. Une journalisation des accès est également mise en place.

Pour les équipements de classe 3 des postes de contrôle ne pouvant se connecter à l'annuaire technique ou ne pouvant journaliser les accès, Tunnello utilise des mesures organisationnelles pour assurer le contrôle et la traçabilité (voir « Accès aux locaux » et « Accès aux équipements »).

Hors des postes de contrôle, des comptes individuels sont mis en place pour les équipements du système industriel lorsque cela est possible, les comptes génériques par défaut étant supprimés, ou désactivés lorsque la suppression n'est pas possible.

Le tunnel étant de taille relativement réduite, Tunnello a pris la décision de gérer ces comptes de façon manuelle sur l'ensemble des équipements. Une intervention sur place est donc à prévoir dans le cadre des circuits d'arrivée et de départ des personnels qui sont d'intervention sur site.

5.1.2 Gestion de l'authentification

Résumé des mesures détaillées

L'accès aux équipements ne peut se faire qu'après un processus d'authentification suivant un mécanisme protégeant le mot de passe. Une authentification forte (à facteurs multiples) est à privilégier pour les équipements les plus exposés.
A défaut, des mesures compensatoires, par exemple périmétriques ou organisationnelles, doivent être mises en œuvre pour permettre d'atteindre un niveau de protection équivalent.

La liaison entre les deux postes de contrôle repose sur un tunnel chiffré sur une liaison MPLS, comme détaillé ci-après dans la section 5.2, paragraphe « Accès Internet et interconnexions entre sites distants ». Ce tunnel est authentifié par certificat, ce que Tunnello et Intégro considèrent comme un niveau de protection suffisant pour cette liaison.

Pour le système de supervision industrielle, les postes d'administration technique et les postes de supervision, les comptes individuels utilisent une authentification forte (carte à puce et certificats) en se connectant à l'annuaire technique comme base de référence. Les certificats en question sont gérés au moyen d'une IGC construite dans les règles de l'art.

Enfin, concernant les automates ne pouvant s'appuyer sur l'annuaire technique, le compte générique d'administration est utilisé avec un mot de passe suffisamment robuste (en accord avec le guide ANSSI [NT-MDP]), avec une mise à jour du mot de passe par un intervenant interne à la fin de chaque intervention de maintenance.

5.2 Sécurisation de l'architecture du système industriel

5.2.1 Cloisonnement des systèmes industriels

Résumé des mesures détaillées

Le SI industriel doit être découpé en zones cohérentes, cloisonnées physiquement, avec un filtrage entre zones. L'administration doit de plus être réalisée par l'intermédiaire d'un réseau dédié, non connecté à Internet. L'unidirectionnalité des flux entre C3 et les classes inférieures est assurée par une diode matérielle [1]

.

Les postes de contrôle/commande d'une part et le système de terrain d'autre part sont considérés comme deux sous-systèmes distincts au sein de la même architecture. Des pare-feux qualifiés (redondants et distincts) sont donc mis en place pour les cloisonner pour chacune des classes (C2 et C3 étant fusionnées).

Le système C1 et le système C2+C3 ne sont pas interconnectés dans l'architecture retenue.

5.2.2 Interconnexion avec le système d'information de gestion

Résumé des mesures détaillées

L'interconnexion doit être protégée par un pare-feu et les flux autorisés doivent être réduits au minimum. Une diode matérielle doit protéger le flux unidirectionnel de C3 vers le SI de gestion.

Le réseau mis en œuvre par Intégro ne possède pas de connexion vers un système d'information de gestion.

1. On pourra se reporter à l'annexe A.9 pour plus de précision.

5.2.3 Accès Internet et interconnexions entre sites distants

Résumé des mesures détaillées

La protection des échanges entre SI industriels distants doit être garantie. Chaque site est de plus protégé par un pare-feu. Les échanges directs avec un réseau public sont interdits.

La gestion du système industriel, c'est-à-dire le fait de pouvoir par exemple modifier les paramètres de consigne, fait partie du processus de supervision, qui pour rappel recouvre les capacités de visualisation, de journalisation et de pilotage. De ce fait, il existe un processus de télégestion dans la définition même des besoins dans le sens où le système industriel doit être supervisé depuis le poste de contrôle principal, situé à Millau.

Pour assurer la sécurité de cette télégestion, la liaison entre le poste de contrôle principal et le site du tunnel se fait au travers d'un tunnel chiffré de type IPsec authentifié par certificat [2], le tout transitant sur une liaison spécialisée (segmentation par MPLS).

Par ailleurs, l'architecture mise en œuvre par Intégro ne possède pas de connexion vers Internet ou tout autre réseau public, la liaison entre le poste de contrôle principal et le site du tunnel se faisant au travers d'un tunnel chiffré sur une liaison spécialisée (segmentation par MPLS).

5.2.4 Accès distants

Résumé des mesures détaillées

La télémaintenance est interdite depuis l'extérieur du C3. Lorsqu'elle ne peut être évitée, elle ne peut donc être mise en œuvre qu'en l'intégrant au C3 et en appliquant les règles relatives aux SI industriels distribués (donc pas depuis un réseau public, poste d'administration cloisonné et dédié, etc.).

Après une première étude menée durant la phase projet, Tunnello estime que la faible fréquence des actions de maintenance et du taux de panne habituel de ces équipements ne justifie pas les coûts et risques liés à ce type de fonctionnalité : ainsi,

2. Concernant la mise en place d'un tunnel IPsec, on pourra se référer à la note technique [NT-IPSEC].

l'architecture mise en place par Intégro ne comporte pas de réseau d'administration. Les modèles des différents matériels ont été choisis en conséquence pour permettre de limiter les ports physiques autorisant des actions d'administration ou de programmation.

Il n'est donc de fait pas possible de réaliser de la télémaintenance ou du télédiagnostic au-delà des informations remontées par les systèmes de supervision et de journalisation. Toute maintenance doit être réalisée au moyen d'une connexion locale à l'équipement avec un poste portable dédié à la maintenance sur lequel sont installés les outils dédiés.

Un poste est dédié à la classe 1 et un autre aux classes 2 et 3.

5.2.5 Systèmes industriels distribués

Résumé des mesures détaillées

Des passerelles VPN et des pare-feux doivent être installés aux extrémités des liaisons. Des liaisons dédiées sont systématiquement utilisées.

Tunnello et Intégro ont pris le parti de gérer le poste de contrôle/commande principal, distant, sous la forme d'un point de télégestion plutôt que comme un système industriel distribué.

5.2.6 Communications sans fil

Résumé des mesures détaillées

Une sonde de détection doit être mise en œuvre à l'interconnexion avec le réseau filaire et ses remontées centralisées sont suivies en temps réel.
Ce type de communication est interdit en cas de contrainte forte en disponibilité.

Le réseau mis en œuvre par Intégro ne possède pas d'équipement de communication sans fil.

5.2.7 Sécurité des protocoles

Résumé des mesures détaillées

Les protocoles non sécurisés doivent être désactivés.

Intégro a sélectionné des équipements permettant de désactiver les protocoles non sécurisés pour la supervision et l'administration, hors connexion directe à l'équipement.

5.3 Sécurisation des équipements

5.3.1 Durcissement des configurations

Désactivation des comptes inutiles

Résumé des mesures détaillées

Sur les équipements, les comptes par défaut, les ports inutilisés et les services non indispensables sont désactivés.
Sur les postes utilisateurs, les outils de débogage, de test sont désinstallés et les comptes et services non nécessaires supprimés.
Pour les applications du système de supervision industrielle, les commentaires et mnémoniques ne sont pas chargés sur les équipements.

Comme indiqué dans la section concernant leur gestion, des comptes individuels sont mis en place pour les équipements du système industriel lorsque cela est possible, les comptes génériques par défaut étant supprimés, ou désactivés lorsque la suppression n'est pas possible. Le cas échéant, une intervention sur place pour supprimer le compte devenant obsolète est également prévue dans le cadre du circuit de départ des personnels.

Renforcement des protections

Résumé des mesures détaillées

Les applications doivent s'exécuter avec les privilèges strictement nécessaires. Pour la défense en profondeur, les équipements doivent protéger les accès à leurs ressources matérielles et seules les applications autorisées peuvent s'exécuter.

Lors de la rédaction de son cahier des charges, Tunnello a explicitement demandé à ce que les équipements respectent les critères suivants :

- il existe une procédure d'exécution par liste blanche sur le système de supervision industrielle ;
- les services présents sur les serveurs doivent s'exécuter avec un compte dédié et non en tant qu'administrateur.

Le respect de ces exigences a été pris en compte pour le choix des équipements déployés.

Le cahier des charges prévoit également le durcissement des différents postes utilisateurs. Il est notamment prévu pour le poste de maintenance un contrôle d'accès logique (pas de « AutoLogin ») et un chiffrement intégral du disque dur. Par ailleurs, ses mises à jour et l'évolution des logiciels disponibles suivent les mêmes règles que celles des équipements (cf la section suivante).

Intégrité et authenticité

Résumé des mesures détaillées

Le processus d'approvisionnement doit être contrôlé au maximum et en particulier inclure un contrôle d'intégrité des éléments critiques. Ce contrôle doit s'appuyer sur un processus de signature des éléments et de comparaison des versions des logiciels livrés et historisés.

Dès le cahier des charges, Tunnello a demandé que les problématiques d'intégrité et d'authenticité soient prises en compte, idéalement au moyen d'une signature des binaires par l'équipementier ou l'intégrateur lorsque celui-ci est intervenu pour les personnaliser.

Bien que ne disposant pas au final de l'infrastructure permettant la signature de l'ensemble des binaires, Intégro a néanmoins été considéré comme suffisamment de confiance lors de l'attribution du marché, du fait de son statut de prestataire qualifié.

Tunnello et Intégro sont donc convenus d'une procédure privilégiant un calcul du hash de tous les fichiers livrés au moment du passage par le SAS d'import (cf. 3.14), avec vérification visuelle des hashs fournis par un moyen de diffusion différent des binaires (fax, courrier papier et courrier électronique signé sont des moyens acceptés). Intégro devra s'assurer de l'intégrité de tous les fichiers fournis par le constructeur (cf. section « Gestion des modifications et évolutions »).

De plus, la comparaison entre la version des logiciels livrés par Intégro et la version historisée par Tunnello, permet de s'assurer de l'intégrité des scripts et des binaires déployés sur les composants du tunnel. Les versions précédentes sont historisées soit sur le serveur de supervision, soit sur le poste de décontamination, soit sur un PC dans un coffre sécurisé à l'intérieur du PCC.

Concrètement, le SAS d'import est une machine, connectée à Internet, dont les seules fonctions sont le téléchargement des mises à jour et la vérification de leurs signatures, avant de déposer celles-ci sur clé USB. Le SAS est mutualisé au niveau du PCC principal, mais un support amovible est dédié à chaque réseau de terrain.

Pour ce faire, cette machine utilise un système d'exploitation de type « liveCD », évitant ainsi les attaques persistante (un redémarrage du poste suffit pour repartir sur un système « propre », la base antivirale étant mise à jour dès le démarrage du poste). Intégro fournie, dans le cadre du contrat de maintenance, des mises à jours régulières de la distribution « liveCD ».

5.3.2 Gestion des vulnérabilités

Résumé des mesures détaillées

Les vulnérabilités connues non corrigées (ou vulnérabilités résiduelles) doivent être documentées, de même que les mesures palliatives mises en œuvre pour en limiter l'exposition ou l'impact.
Un plan de gestion des vulnérabilités et des correctifs doit être mis en œuvre, établissant notamment les priorités et un indicateur de suivi du déploiement effectif des correctifs.

N'ayant ni les ressources ni les compétences en interne, la direction de Tunnello charge Intégro d'assurer cette veille dans le cadre du contrat de maintenance des

équipements. Intégro s'engage notamment à être force de conseil sur les évolutions devant être envisagées au niveau du SI pour se protéger des nouvelles menaces, ainsi que sur les mises à jour et moyens palliatifs. (cf. « Processus de veille »).

5.3.3 Interfaces de connexion

Médias amovibles

Résumé des mesures détaillées

Une politique de gestion des médias amovibles doit être mise en œuvre, incluant une station de décontamination et la mise à disposition de médias dédiés au SI industriel.
Les ports pour médias amovibles non nécessaires sont désactivés. La station de décontamination est remplacée par un sas en zone maîtrisée.

La PSSI de Tunnello impose que les seuls médias amovibles acceptés sont des clés USB dédiées qui peuvent être utilisées dans le tunnel routier ou dans les postes de contrôle. De plus chaque média est dédié à une classe donnée pour éviter la propagation d'une éventuelle contamination. Les médias concernés sont identifiés de façon à éviter toute erreur.

Pour permettre la mise à jour des équipements, Intégro a mis en place un poste « durci », c'est-à-dire dont la sécurité est renforcée. Celui-ci a pour rôle de s'assurer de l'innocuité des documents copiés ou importés d'un autre support avant de les déposer sur les clés USB. Ce poste est le seul équipement sur lequel l'ensemble des clés USB dédiées du tunnel peuvent se connecter, indépendamment de la classe. Il est en revanche complètement déconnecté des réseaux utilisés par les postes de contrôle ou dans le tunnel.

Points d'accès réseau

Résumé des mesures détaillées

Une gestion des points d'accès réseau doit être mise en place (identification, désactivation si inutile) et une gestion des alertes doit être mise en place sur événement.
Les points d'accès réseau ne sont accessibles que dans les locaux maîtrisés et dans des coffrets scellés.

Lors de l'installation des équipements du tunnel, Intégro a documenté l'utilisation des ports des différents commutateurs, dans le cadre de la cartographie du système. Cette dernière est régulièrement mise à jour (voir plus haut la section lui étant consacrée) et Intégro est tenu de désactiver les ports non documentés.

De plus, pour assurer une bonne identification des différentes classes, Intégro a mis en œuvre une différenciation des couleurs de câbles ethernet (rouge pour raccorder les équipements de classe C3 - et donc aussi C2 - , vert pour ceux de la classe C1).

En l'absence d'un réseau d'administration dédié (les équipements réseau sont gérés au moyen d'une connexion locale), la remontée d'alerte repose sur la mise sous alarme des coffrets, conformément à ce qui est décrit dans les sections abordant le suivi des interventions et la protection des locaux.

5.3.4 Équipements mobiles

Résumé des mesures détaillées

Une gestion du parc mobile doit être mise en place et l'usage de terminaux mobiles personnels interdit. Lorsque le mobile contient des données sensibles, elles doivent être chiffrées.
Les équipements mobiles utilisés doivent être dédiés au SI industriel et au site, y compris ceux des prestataires.

Deux ordinateurs portables dédiés au tunnel sont mis en place pour se connecter aux équipements et en assurer la maintenance, comme indiqué dans la section consacrée aux accès distants plus haut dans ce chapitre, ainsi que dans la section 3.11. Ils sont conservés à demeure sur le site. Un est consacré à la classe 1 et l'autre aux classes 2 et 3.

En dehors de ces postes de maintenance, ni Tunnello ni ses sous-traitants n'utilisent d'équipements mobiles (ordiphones, tablettes, etc.) pour se connecter aux différents réseaux présents dans le tunnel ou dans les postes de contrôle. Les téléphones portables sont réservés à un usage voix/SMS (les connexions « données » restent tolérées pour des usages annexes mais ne doivent en aucun cas permettre l'accès au SI de Tunnello ou d'Intégro).

5.3.5 Sécurité des consoles de programmation, des stations d'ingénierie et des postes d'administration

Résumé des mesures détaillées

Une gestion des postes d'administration, des stations d'ingénierie et des consoles de programmation doit être mise en place. Les postes d'administration ne doivent pas être utilisés pour la surveillance des SI industriels.

De par l'organisation mise en place, seuls les postes de supervision sont mis en œuvre dans les PCC.

Le site ne disposant pas d'un réseau d'administration technique, cette dernière tâche ne peut être réalisée depuis le PCC par les postes de supervision. Elle n'est possible que grâce aux postes nomades de maintenance décrits plus haut, nécessaires pour obtenir un accès administrateur localement sur un équipement. L'administration technique est donc de fait distincte de l'activité de supervision et respecte la segmentation du système (classe 1 d'une part, classes 2 et 3 de l'autre). Enfin, comme la phase d'ingénierie est réalisée dans les locaux d'Intégro, il y a là aussi séparation de fait.

La sécurité de ces différents postes dépend également de leur mise à jour régulière. Toutefois, cette action peut être contrariée par la nécessité de conserver une version donnée du système d'exploitation des postes pour les outils du système industriel, les deux connaissant des cycles de vie différents.

Le contrat de maintenance des équipements couvre donc également la maintenance des outils associés tels que les logiciels de supervision et d'ingénieurie (comme indiqué dans la section 4.4.1), ce qui permet à Tunnello de disposer d'outils compatibles avec un système d'exploitation à jour.

Intégro est donc en mesure d'assurer les mises à jour des postes de travail et des serveurs sur une base trimestrielle, les postes de maintenance étant quant à eux mis à jour au moins une fois par an (par exemple lors de la visite annuelle de mise à jour de la documentation - cf. section 4.1.5).

La récupération des mises à jour des postes suit par ailleurs un processus similaire aux mises à jour des firmwares décrit à la section 5.3.1.

5.3.6 Développement sécurisé

Résumé des mesures détaillées

Le développement doit être réalisé sur un environnement dédié, en suivant des règles de développement sécurisé. Le code doit être analysé et audité.

Intégro s'engage à ce que le développement soit fait suivant les bonnes pratiques. Un gestionnaire de versions est notamment mis en œuvre par Intégro pour assurer le suivi du développement et des correctifs, la capacité à revenir à n'importe quelle version délivrée et d'en vérifier l'intégrité. Ce gestionnaire de versions couvre à la fois les sources et les binaires délivrés.

Intégro s'est par ailleurs assuré un engagement équivalent de la part de ses fournisseurs.

5.4 Surveillance du système industriel

5.4.1 Journaux d'événements

Résumé des mesures détaillées

Une politique de gestion des événements doit être mise en place, incluant un suivi des modifications de paramètres et la centralisation des journaux. Cette politique doit également inclure une analyse régulière des données collectées.

Durant la phase de conception, Intégro a fait le choix d'une infrastructure de type syslog pour assurer la centralisation des journaux pour les équipements de sécurité (pare-feux et passerelles VPN), les postes ainsi que pour les équipements supportant la fonctionnalité de collecte centralisée de journaux dans le cadre de la fonction de supervision.

Au moins une fois par mois, un intervenant se rend sur place pour réaliser une collecte systématique des logs sur l'ensemble des équipements non raccordés au réseau ou ne permettant pas la centralisation des journaux.

De par l'architecture mise en œuvre, Intégro prévoit un serveur de journalisation pour la classe 1 et un pour la classe « C2+C3 ». Ceux-ci génèrent un rapport de synthèse

à destination du service d'exploitation, sur une base quotidienne pour la classe 3 et hebdomadaire pour la classe 1.

5.4.2 Moyens de détection

Résumé des mesures détaillées

Des moyens de détection d'intrusion doivent être mis en place en périphérie des systèmes industriels et sur les points identifiés comme critiques.
Les moyens de détection utilisés devraient être labellisés.

Intégro décide de renforcer la protection des équipements les plus sensibles par la mise en place de sondes de détection labellisées.

Son analyse de risque sur ce point particulier fait ressortir que le point le plus sensible concerne l'interconnexion entre les (sous-)systèmes de classe 3 « postes de contrôle » et « tunnel ». En effet, les équipements et les modalités de gestion mis en œuvre dans ces deux systèmes sont relativement différents, la partie « postes de contrôle » étant prévue pour une utilisation quotidienne par des utilisateurs, avec des postes pouvant disposer d'interfaces avancées et d'entrées de documents divers (via un SAS d'import), alors que le système « tunnel » repose sur un fonctionnement automatisé, les seules informations entrantes passant par l'interconnexion citée ci-dessus (hors maintenance). De ce fait, une sonde est mise en place pour surveiller les échanges entre les deux ensembles de classe 3 (au sens large, c'est à dire recouvrant également C2 dans le cas présent).

L'analyse de risque montre également que les protocoles de communication sur la partie « système de terrain » ne pouvant tous être sécurisés malgré un choix attentif des équipements, Tunnello estime nécessaire une surveillance accrue de ces échanges. Une seconde sonde de détection est donc mise en place pour surveiller les échanges permettant l'interconnexion des API et de la détection incendie sur le réseau de terrain.

Les sondes sont mises en place par l'intermédiaire de miroirs de port en aval du pare-feu mis en place précédemment (cf 3.10), ainsi que sur les commutateurs permettant l'interconnexion des API et de la détection incendie sur le réseau de terrain.

Les alarmes sont remontées en temps réel à l'équipe d'exploitation, les modalités de prise en compte étant prévues dans le cadre de la gestion d'incidents (cf 3.9).

Annexe A

Description des composants

A.1 Niche d'exploitation

Une niche est un local technique situé à l'intérieur du tunnel. Les niches sont installées tous les 200 m environ.

Chaque niche contient un ou plusieurs modules d'entrées/sorties déportés qui concentrent les connexions des équipements à proximité. Ces derniers sont de deux types :

- les **actionneurs**, qui sont des éléments physiques qui, recevant un ordre de la partie commande, déclenchent une action physique utile. Dans le cas du tunnel, les actionneurs sont à commande informatisée et les ordres transitent par les réseaux de terrain.
- les **capteurs** sont des dispositifs permettant de mesurer une grandeur physique et de la transformer en grandeur utilisable. Dans le cas du tunnel, les grandeurs sont numérisées et transmises de façon informatisée à la partie commande par les réseaux de terrain.

Chaque niche comprend, en plus de ce(s) module(s), un ou plusieurs commutateurs (ou switch) permettant de raccorder les équipements aux réseaux de terrain, chaque commutateur n'étant connecté qu'à un seul réseau. Dans le cas du tunnel, les réseaux de terrain, qui relient les différentes niches avec le PCC local, sont de type Ethernet. Tous les accès nécessaires aux différents réseaux de terrain (informatique, électricité, fluides) peuvent y être aménagés suivant les besoins. On y trouve ainsi des piquages pour les divers fluides, des alimentations électriques ou des commutateurs pour les réseaux informatiques présents.

A.2 Poste de contrôle/commande

Le PCC concentre toute l'activité de supervision des réseaux de terrain. Toutes les informations sont remontées sur les serveurs du système de supervision industrielle à l'aide d'un ou plusieurs réseaux, chacun correspondant à une classe différente (le nombre de réseaux dépendant de la configuration retenue, on se référera au déroulement de l'étude pour plus de précision sur ce point).

À l'intérieur de chaque PCC se trouve un système technique par réseau de supervision. Chacun de ces systèmes techniques se compose des éléments suivants :

- un serveur du système de supervision industrielle ;
- une console de supervision technique ;
- des périphériques.

Le lien entre les deux premiers items est réalisé en mode client/serveur.

Le tableau suivant décrit les fonctions assurées au sein de chaque PCC.

Fonctions	Description
Affichage d'indicateurs	Toutes les informations mesurées par les capteurs sont remontées et agrégées au niveau du serveur de supervision. La console de supervision permet d'afficher les mesures à l'aide de tableaux de bord.
Analyse de la situation	Le système de supervision détermine, en fonction des seuils prédéfinis, le type d'alerte à remonter et sa criticité.
Envoi d'information	Le système de supervision permet l'envoi d'informations à destination des actionneurs des différents réseaux de terrain. On pourra citer par exemple l'augmentation du débit de renouvellement d'air (ventilation) suite au dépassement d'un seuil au niveau des capteurs liés au contrôle de la qualité de l'air.

A.3 Automate programmable industriel

Les automates programmables industriels (API, aussi appelés *Programmable Logic controller* ou *PLC* en anglais) assurent la partie commande automatisée du système industriel.

Pour ce faire, les API, connectés à un réseau de terrain, reçoivent les informations remontées par les capteurs et en déduisent les commandes à envoyer vers les actionneurs suivant une logique pré-programmée.

La mise en marche des ventilateurs suite à la détection de fumée pour assurer le désenfumage est un exemple d'action pilotée par un API.

Pour des raisons de sûreté de fonctionnement, il est fréquent que deux automates soient mis en œuvre sur un réseau de terrain pour assurer une redondance, auquel cas un lien dédié est généralement mis en œuvre pour synchroniser les API. Dans le cas du tunnel, ces API redondants se trouvent aux deux extrémités de celui-ci.

Enfin, bien qu'un écran LCD puisse être présent sur les API pour vérifier la bonne exécution des actions de l'automate, ils sont généralement accompagnés d'une console IHM (voir ci-après) lorsque ce suivi est nécessaire par l'opérateur en suivi régulier.

A.4 Centrale de Détection Incendie

Comme son nom l'indique, la centrale de détection incendie est un équipement dont le rôle est de détecter un incendie de façon aussi précoce que possible. Il s'agit d'un automate programmable de sécurité (APS), c'est à dire un API spécifique dédié à une fonction de sécurité car son fonctionnement est garanti y compris en mode dégradé, par exemple grâce à la redondance interne de certaines chaînes de commande.

La détection incendie peut recevoir des informations de capteurs dédiés à la détection incendie (détecteurs de fumée, capteurs de déformation, etc) et dont les actions peuvent être de donner l'alarme ou de déclencher des actions réflexes via les API standard (par exemple ordonner l'arrêt de la ventilation).

La détection incendie repose notamment sur un composant assez spécifique, le fibro-laser. Celui-ci utilise les propriétés physiques d'une fibre optique, courant sur la longueur du tunnel.

En cas d'augmentation importante de la température, l'équipement sera capable de détecter la dilatation de la fibre pour remonter l'alarme. La localisation de ce point de dilatation, et donc du dégagement de chaleur, est rendue possible par les variations de conductivité qu'il induit dans la fibre. Cette localisation est dès lors utilisée pour réaliser une extraction concentrée à l'endroit supposé de l'incendie.

A.5 Interface homme-machine

Dans le domaine de l'automatisation, le terme d'interface homme-machine (IHM) désigne le plus souvent un écran tactile permettant de centraliser le contrôle d'une fonction ou d'un ensemble de fonctions, en affichant des indicateurs pertinents et en mettant à disposition de l'opérateur des commandes permettant de piloter leur fonctionnement, dans les limites fixées par le programme de l'API.

De ce fait, une IHM peut être assimilée à une version très simplifiée du poste de supervision, déployée au plus près des installations de terrain. Tout comme les postes de supervision, elles ne permettent pas de modifier les programmes au sein des API (au contraire du poste de maintenance).

A.6 Poste de travail

Relié à un serveur de supervision, le poste de travail utilisé par Tunnello est un poste fixe présent dans le PCC. À partir de ce poste de travail, les fonctions suivantes sont assurées :

- **la supervision :** il s'agit de permettre à l'exploitant de surveiller l'activité du tunnel et le cas échéant de piloter certains équipements par exemple en modifiant certaines valeurs de consigne ;
- **l'administration et la maintenance de la solution de supervision :** il s'agit de l'installation, du paramétrage et de la configuration du ou des logiciel(s) nécessaires à la supervision du tunnel ;
- **l'administration et la maintenance des équipements industriels :** il s'agit de l'installation matérielle et logicielle, de la mise à jour des composants présents dans le tunnel et du support informatique par l'intégrateur.

A.7 Poste de maintenance

Aussi appelé console de programmation, son rôle est de permettre des actions de maintenance sur les équipements de terrain (*i.e.* dans le tunnel), à commencer par les API. Plus particulièrement, il permet de se connecter aux équipements du tunnel pour réaliser des opérations privilégiées comme la modification des programmes au sein des API ou la mise à jour des firmwares de l'ensemble des équipements. Ce poste est donc sensible par construction puisque l'ensemble des outils nécessaires pour dialoguer avec les équipements sont installés.

Dans le cas particulier du tunnel sujet de l'étude, l'hypothèse est prise d'utiliser un (ou plusieurs) ordinateur portable pour réaliser ces actions, notamment pour pouvoir se connecter en direct sur les différents équipements, sans dépendre d'un réseau d'administration. De ce fait, ce poste est parfois qualifié de nomade.

Dans cette première approche, ce poste de maintenance est donc potentiellement utilisable à la fois par les personnels de Tunnello (les exploitants) et par les personnels de Integro (les intégrateurs). N'étant pas lié à un groupe d'utilisateurs mais à une fonction et une localisation, ce poste de maintenance peut également être utilisé pour d'autres actions, dès lors qu'il est nécessaire de disposer de droits étendus sur un équipement.

Du fait de sa criticité, les accès à ce poste et les actions effectuées avec doivent être tracés.

A.8 Pare-feu

Le rôle d'un pare-feu est d'assurer un niveau de protection satisfaisant des échanges lors de l'interconnexion de réseaux dont le niveau de confiance ou de sensibilité n'est pas nécessairement équivalente.

La protection apportée par cet équipement est directement liée à sa capacité à repérer des échanges non conformes. De ce fait, un pare-feu générique, adapté à l'analyse des services présents dans un système d'information classique, n'est pas équivalent à un équipement capable d'appréhender les protocoles industriels et les flux métier associés.

De par son rôle, le suivi des alarmes remontées par un pare-feu est primordial. Dans le cadre de l'étude, chaque pare-feu est donc rattaché à la console de supervision technique et au système de journalisation mis en place pour la classe dont il dépend (cf. le contenu de l'étude pour plus de précision sur ce dernier point).

A.9 Diode

Plusieurs des architectures proposées mettent en œuvre une ou plusieurs diodes (matérielles). Le rôle d'une diode est d'assurer l'unidirectionnalité de certains liens.

En effet, comme indiqué dans la section « Dépendances fonctionnelles » du chapitre 2 de la première partie de l'étude de cas [SCADA-TNL-1], il est possible de faire transiter des informations depuis un réseau de classe donnée vers un réseau de classe inférieure, mais il est impératif de bloquer toute commande d'un réseau bas vers un réseau de classe plus élevée.

Dans le cas le plus simple, une information peut se limiter à un simple changement d'état, comme par exemple le déclenchement de l'alarme incendie. Dans ce cas, il est possible d'utiliser des éléments de base pour la réalisation du mécanisme d'échange, comme la mise en place d'un photo-coupleur (ou **optocoupler** en anglais) entre une sortie simple de l'API de classe haute et une entrée de type contacteur sur l'API de classe plus basse. Ce type d'équipement peut aussi être utilisé pour faire transiter des informations un peu plus complexes en les encodant (il est possible de trouver des photo-coupleurs permettant de réaliser une connexion de quelques kbps).

Suivant les protocoles mis en œuvre pour les informations complexes, il est toutefois probable que l'utilisation d'une diode matérielle seule (c'est-à-dire sans aucun élément l'accompagnant) ne soit pas possible, le protocole attendant par exemple des retours d'acquittement. Dans ce cas, il convient de compléter la diode matérielle par deux « guichets », de part et d'autre, qui assurent une compatibilité avec les proto-

coles respectifs des deux réseaux, tout en garantissant le transfert au travers de la diode de façon adaptée (code de correction d'erreur, gestion du débit...).

Dans les architectures évoquées dans ce document, ces deux guichets sont considérés comme faisant partie du composant « diode » pris dans son ensemble et ne sont donc pas matérialisés dans les schémas.

Enfin, comme pour les autres produits de sécurité, une priorité sera accordée aux diodes labelisées par l'ANSSI au fur et à mesure que celles-ci apparaitront sur le marché.

Annexe B

Architectures pour les regroupements alternatifs

Cette annexe regroupe des propositions d'architectures construites à partir des autres regroupements présentés dans le chapitre « Choix de l'architecture » de la première partie de l'étude de cas [SCADA-TNL-1] pour lesquels les mesures principales ont été déclinées.

B.1 Configuration « tout C3 »

En se limitant au déroulé des mesures principales, ces dernières font apparaître la nécessité de mettre en place les composants suivants, en plus des fonctions principales :

Classe	Composants complémentaires
Classe 3	- poste de maintenance pour l'administration technique (disjoint du poste de supervision) ; - outils de diagnostic et d'interventions dédiés ; - SAS d'import (non nécessairement connecté au réseau) ; - serveur de journalisation centralisé ; - annuaire technique ; - pare-feux ; - VPN entre sites ; - solution de SIEM (optionnel) ; - solution de détection d'intrusion.

Le schéma d'architecture de la figure B.1 représente le système industriel qui résulte de l'étude.

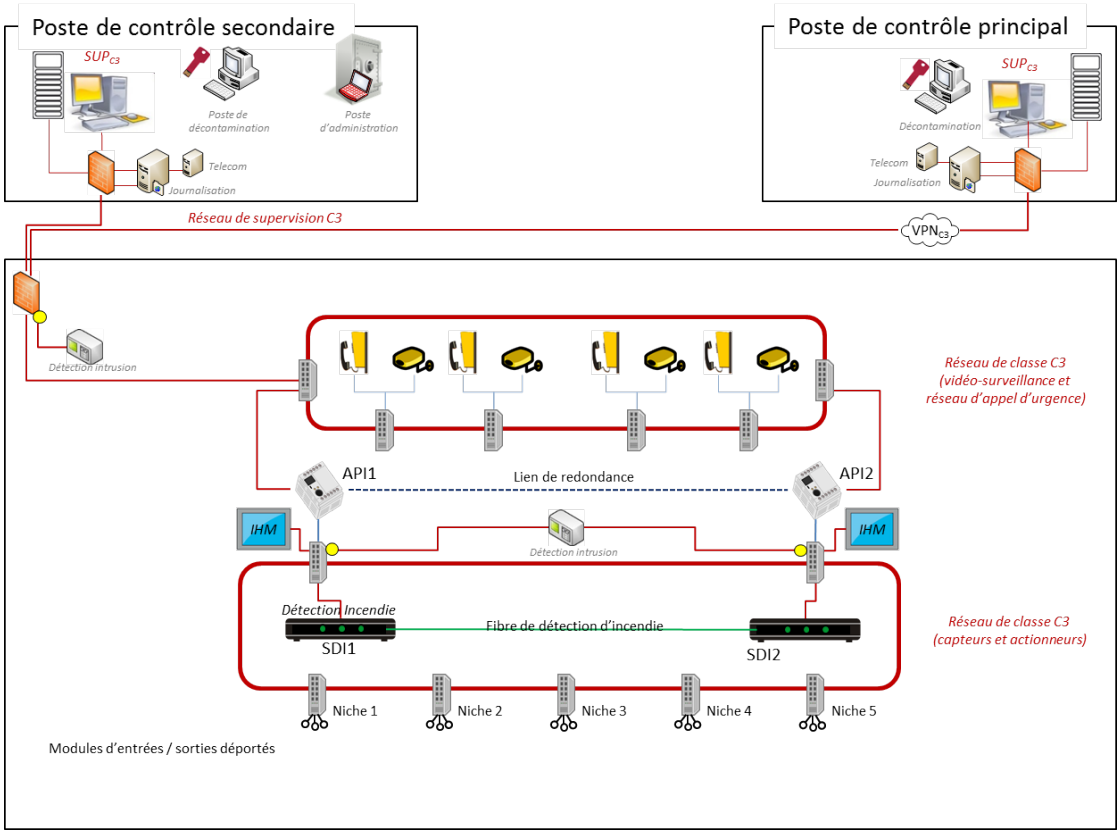

Figure B.1 – *Système industriel - Architecture technique sécurisée « tout C3 »*

Le réseau de terrain ainsi que le réseau de supervision sont classés au niveau de sécurité le plus élevé, C3.

La vidéo-surveillance reste sur un réseau dédié (même principe évoqué précédemment).

Tous les capteurs et actionneurs sont sur la même boucle.

Au niveau des postes de contrôle, une seule console de supervision est suffisante (marquée « Sup C3 ») ; elle est déployée derrière le système de supervision industrielle.

B.2 Configuration « C1, C2, C3 »

En se limitant au déroulé des mesures principales, celles-ci font apparaître la nécessité de mettre en place les composants suivants, en plus de ceux liés aux fonctions principales :

Classe	Composants complémentaires
Classe 1	- poste de maintenance pour l'administration technique ; - SAS d'import (optionnel, non nécessairement connecté au réseau) ; - pare-feux ; - VPN entre sites ; - serveur de journalisation centralisé (optionnel).
Classe 2	- poste de maintenance pour l'administration technique (portable, disjoint du poste de supervision) ; - outils de diagnostic et d'interventions dédiés au site, avec une tolérance lorsque leur usage reste exceptionnel ; - SAS d'import (non nécessairement connecté au réseau) ; - serveur de journalisation centralisé ; - pare-feux ; - VPN entre sites ; - solution de détection d'intrusion (optionnel).
Classe 3	- poste de maintenance pour l'administration technique (portable, disjoint du poste de supervision) ; - outils de diagnostic et d'interventions dédiés au site ; - SAS d'import (non nécessairement connecté au réseau) ; - serveur de journalisation centralisé ; - annuaire technique ; - pare-feux ; - VPN entre sites ; - diode permettant la descente d'informations vers C2 ; - solution de SIEM (optionnel) ; - solution de détection d'intrusion.

Cette configuration schématisée en B.2 est la plus complexe à mettre en œuvre car elle nécessite un réseau spécifique pour chaque classe.

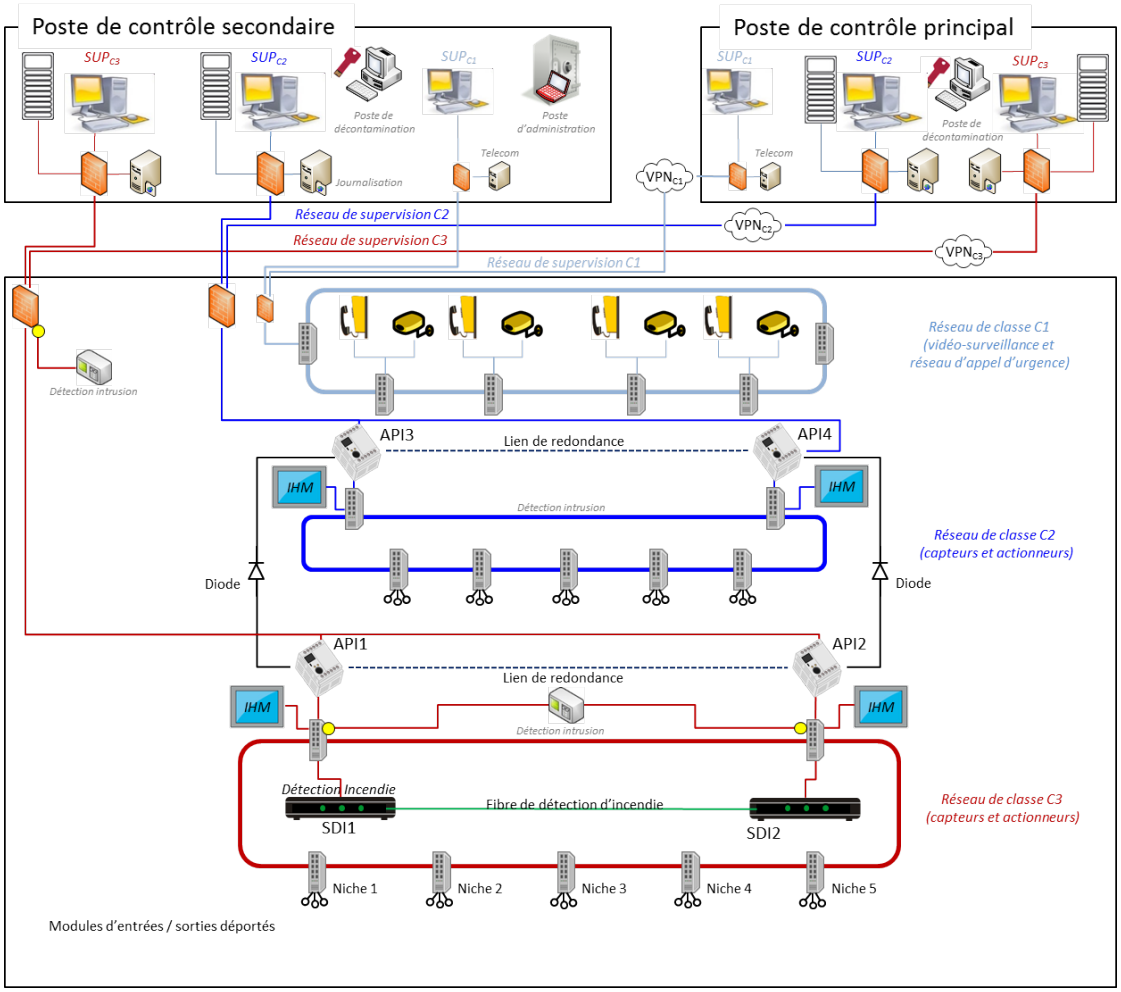

Figure B.2 – *Système industriel - Architecture technique sécurisée « C1, C2, C3 »*

B.3 Configuration « C1+C2, C3 »

En réalisant la même démarche que ci-dessus, la liste des composants complémentaires est donnée dans le tableau suivant.

Classe	Composants complémentaires
Classe 2 (C1+C2)	- poste de maintenance pour l'administration technique (portable, disjoint du poste de supervision) ; - outils de diagnostic et d'interventions dédiés au site, avec une tolérance lorsque leur usage reste exceptionnel ; - SAS d'import (non nécessairement connecté au réseau) ; - serveur de journalisation centralisé ; - pare-feux ; - VPN entre sites ; - solution de détection d'intrusion (optionnel).
Classe 3	- poste de maintenance pour l'administration technique (portable, disjoint du poste de supervision) ; - outils de diagnostic et d'interventions dédiés au site ; - SAS d'import (non nécessairement connecté au réseau) ; - serveur de journalisation centralisé ; - Annuaire technique ; - pare-feux ; - VPN entre sites ; - diode permettant la descente d'informations vers C2 ; - solution de SIEM (optionnel) ; - solution de détection d'intrusion.

La communication entre les réseaux de classes différentes se traduit par la mise en œuvre d'une diode matérielle représentée dans le schéma d'architecture physique de la figure B.3.

Les sites sont reliés entre eux par les VPN de chaque classe. Chaque VPN est sécurisé par un pare-feu en sortie du tunnel et en entrée de chaque poste de contrôle. L'architecture permet donc que toutes les fonctions puissent être exécutées de manière indépendante dans l'un ou l'autre poste de contrôle.

Dans le cas d'une sécurisation maximale, plusieurs options sont possibles :

– installation des serveurs en mode cluster dans les deux sites, tout en faisant attention à la synchronisation des données entre les deux sites,

– déplacement du deuxième membre du cluster de chaque niveau de supervision (SUPcx) dans le second site.

Rappel : il n'y a pas de connexion entre les deux réseaux de supervision C2 et C3.

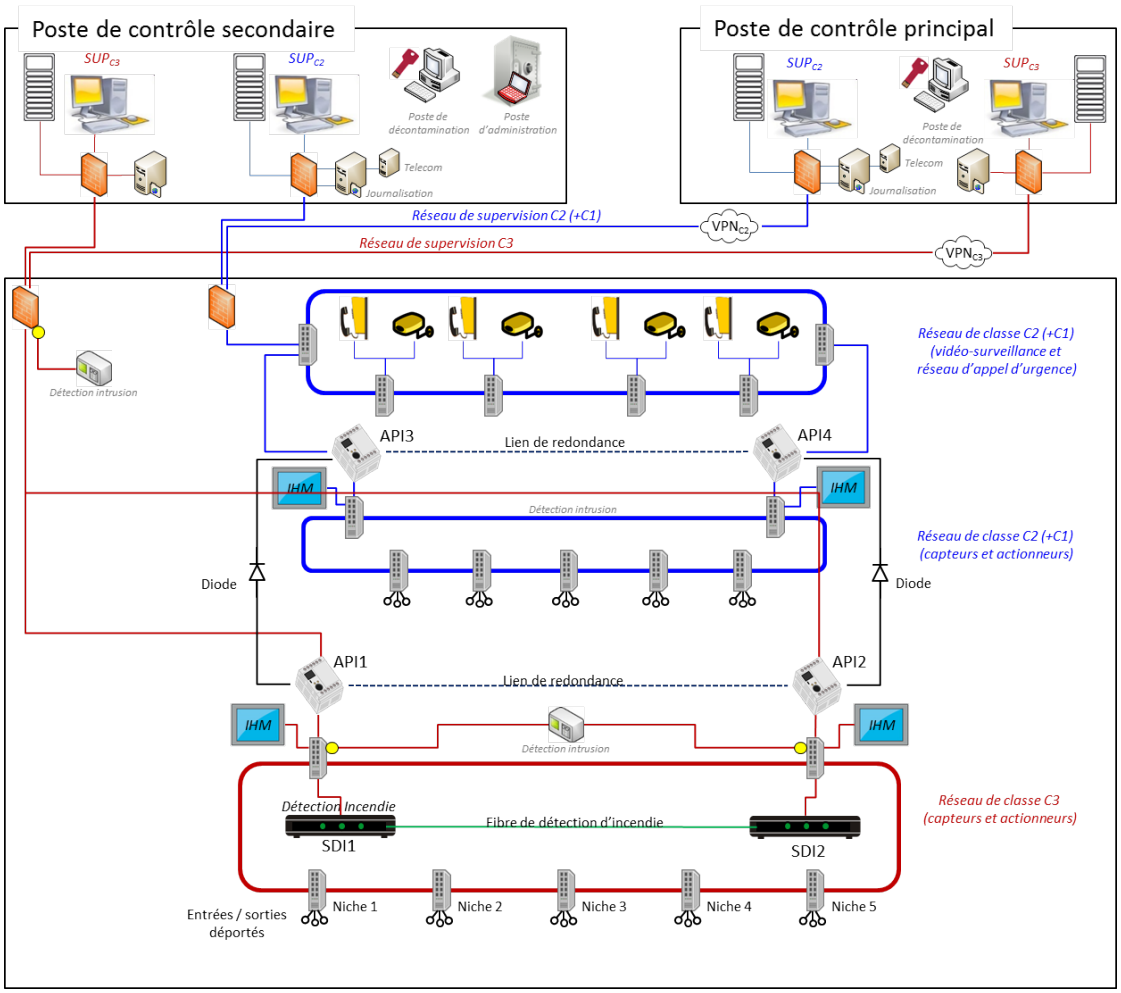

Figure B.3 – *Système industriel - Architecture technique sécurisée « C1+C2 et C3 »*

Bibliographie

[NT-MDP] *Recommandations de sécurité relatives aux mots de passe*.
Note technique DAT-NT-001/ANSSI/SDE/NP, ANSSI, juin 2012.
`http://www.ssi.gouv.fr/mots-de-passe`.

[NT-IPSEC] *Recommandations de sécurité relatives à IPsec*.
Note technique DAT-NT-003/ANSSI/SDE/NP, ANSSI, 2015.
`http://www.ssi.gouv.fr/ipsec`.

[SCADA-MTD] *La cybersécurité des systèmes industriels - Méthode de classification et mesures principales*.
Guide Version 1.0, ANSSI, janv 2014.
`http://www.ssi.gouv.fr/uploads/2014/01/securite_industrielle_GT_methode_classification-principales_mesures.pdf`.

[SCADA-MSR] *La cybersécurité des systèmes industriels - Mesures détaillées*.
Guide Version 1.0, ANSSI, janv 2014.
`http://www.ssi.gouv.fr/uploads/2014/01/securite_industrielle_GT_details_principales_mesures.pdf`.

[SCADA-TNL-1] *Cas pratique d'un tunnel routier - Partie 1 : classification*.
Cas pratique Version 1.0, ANSSI, sept 2016.
`http://www.ssi.gouv.fr/systemesindustriels`.

[SCADA-TNL-2] *Cas pratique d'un tunnel routier - Partie 2 : mesures*.
Cas pratique Version 1.0, ANSSI, sept 2016.
`http://www.ssi.gouv.fr/systemesindustriels`.

[GD-HOMOL] *L'homologation de sécurité en neuf étapes simples*.
Guide Version 1.0, ANSSI, juin 2014.
`http://www.ssi.gouv.fr/guide-homologation-securite/`.

Cette étude de cas sur la cybersécurité des systèmes industriels a été réalisée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) avec le concours des sociétés et organismes suivants :

- CEA,
- Schneider Electric,
- Siemens,
- RATP.

À propos de l'ANSSI

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a été créée le 7 juillet 2009 sous la forme d'un service à compétence nationale.
En vertu du décret n° 2009-834 du 7 juillet 2009 modifié par le décret n° 2011-170 du 11 février 2011, l'agence assure la mission d'autorité nationale en matière de défense et de sécurité des systèmes d'information. Elle est rattachée au Secrétaire général de la défense et de la sécurité nationale, sous l'autorité du Premier ministre.
Pour en savoir plus sur l'ANSSI et ses missions, rendez-vous sur www.ssi.gouv.fr.

Version 1.0 – octobre 2016

Agence nationale de la sécurité des systèmes d'information
ANSSI - 51 boulevard de la Tour-Maubourg - 75700 PARIS 07 SP
Site internet : `www.ssi.gouv.fr`
Messagerie : conseil.technique [at] ssi.gouv.fr