Cas pratique d'un tunnel routier
Partie 1 : classification

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] qui visent à proposer une méthode de classification des systèmes industriels et un ensemble de mesures pour apporter un niveau de sécurité adéquat en fonction de la criticité de ces systèmes.

Le but du présent document est d'illustrer la méthode de classification décrite dans le guide [SCADA-MTD], en l'appliquant au cadre de la sécurisation d'un tunnel routier. Il s'agit de la première partie de cette étude de cas, qui en contient deux.

En accord avec l'objectif affiché par le groupe de travail, cette analyse porte exclusivement sur les aspects de cybersécurité, et certains liens qui peuvent être fait avec la sûreté de fonctionnement, mais cette dernière est supposée traitée par ailleurs.

Dans le détail, le chapitre 2 présente les hypothèses de l'étude de cas avec une description de l'ouvrage et des différents acteurs économiques impliqués.

Le chapitre 3 énumère de manière approfondie les différentes menaces qui pèsent sur les systèmes industriels dans ce type de contexte et les rapprochements qu'il est possible de faire entre les analyses de risque menées au titre de la sûreté de fonctionnement et de la cybersécurité.

Le chapitre 4 décrit le raisonnement complet menant à la classification des fonctions. La démarche s'appuie sur des échelles définies par l'opérateur et sur les résultats de l'analyse de risque de sûreté de fonctionnement. Les relations entre les différentes fonctions portées par les systèmes industriels du tunnel sont également analysées en détail.

Le chapitre 5 décrit quant à lui les regroupements qui peuvent être envisagés entre classes pour faciliter la mise en œuvre et l'exploitation du système d'information con-

cerné. En effet, la démarche de classification décrite dans le guide [SCADA-MTD] laisse la liberté de regrouper les fonctions en sous-systèmes à condition de respecter certains principes.

Chapitre 2

Contexte

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.

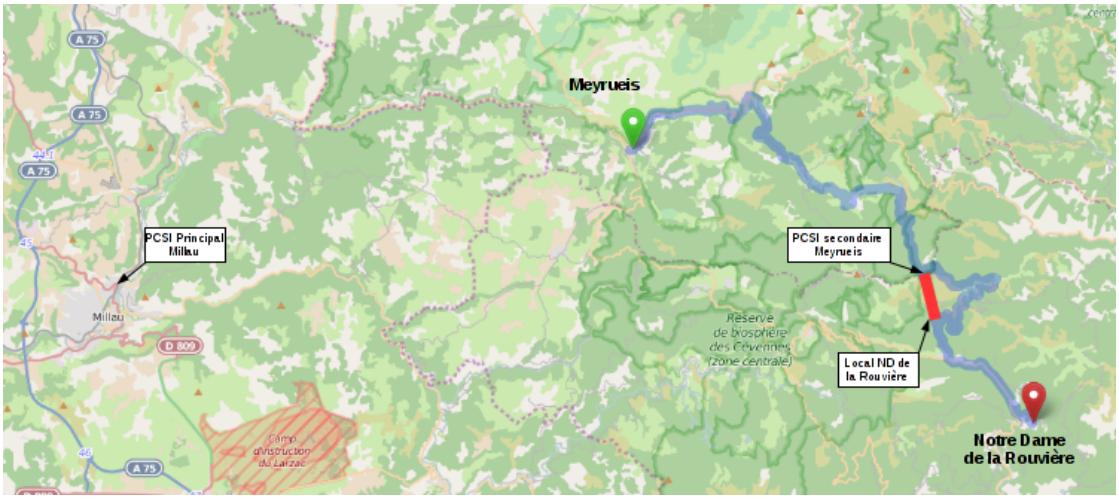

Figure 2.1 – *Tunnel - carte de situation*

2.1 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 adjointe les services de plusieurs prestataires [1], eux aussi fictifs, pour certaines tâches qu'elle ne peut réaliser elle-même :

1. Les noms de ces sociétés ont été choisis de façon à simplifier la compréhension de leur rôle dans la suite du document. Tout rapprochement avec une ou des sociétés existantes serait fortuit.

- 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.

2.2 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. 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 secondaire, sur site, essentiellement utilisé en secours et 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.

Au sein du tunnel, des locaux techniques (aussi appelés niches) sont installés tous les 200 m environ. 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.

2.3 Fonctions mises en œuvre dans le tunnel

Pour commencer cette étude, il convient de réaliser un inventaire des différentes fonctions mises en place dans le cadre du système industriel d'aide à l'exploitation du tunnel.

L'étude de sûreté de fonctionnement, menée par ailleurs, a permis d'identifier que ce type de tunnel doit, pour assurer un niveau de sûreté satisfaisant, mettre en œuvre les fonctions principales suivantes :

- l'alimentation et la distribution électrique ;
- l'indication des sorties de secours [2] ;
- 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 en provenance de sources multiples [4] ;
- 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.

Composants par fonction

D'un point de vue technique, chaque fonction peut impliquer un nombre plus ou moins important de composants. Sans tenir compte de la mutualisation possible de certains équipements (dont les automates et les consoles IHM [5]), la liste des fonctions et des composants associés est résumée dans le tableau suivant.

2. Cette fonction recouvre notamment les systèmes de type TOTEM ainsi que les chevrons dynamiques tels que définis dans le document du CETU sur l'auto-évacuation des usagers [CETU-EVAC]. Elle n'inclue pas les panneaux lumineux réglementaires dont l'alimentation est permanente.

3. Tunnello a retenu pour la ventilation et le désenfumage une stratégie transversale, en accord avec la catégorie du tunnel [CETU-VENT]. Il décide de plus d'utiliser une extraction concentrée.

4. Notamment les télémesures, les télésignalisations ou les téléalarmes.

5. Les automates programmables industriels (API) assurent la partie commande automatisée du système industriel. Voir l'annexe A.3 de la seconde partie de l'étude pour plus de précision.

Fonctions	Composants
Indication des sorties de secours	Automate Disjoncteurs et interrupteurs Capteurs d'état
Ventilation	Automate Moteurs des ventilateurs [6] Capteurs de vitesse de rotation Capteurs anémométriques Trappes d'extraction télécommandées Station météo extérieure pour la gestion des contre-pressions
Signalisation	Automate Signaux lumineux d'affectation de voies Signaux lumineux de déviation pour véhicules hors gabarit Panneaux à message variable Barrières d'accès motorisées Capteurs d'état
Appel d'urgence	Bornes téléphoniques Système de gestion des communications Enregistreur
Détection véhicules hors gabarit	Automate Capteurs de gabarit
Vidéo-surveillance	Système de gestion de la vidéo-surveillance Caméras Enregistreur
Détection incendie	Centrale de détection incendie (automate dédié) Détecteurs de fumée Fibro-laser
Contrôle de la qualité de l'air	Automate Opacimètres Détecteurs monoxyde de carbone et d'azote.
Alimentation et distribution électrique	Automate Disjoncteurs et interrupteurs Centrale de mesure Capteurs d'état
Supervision	Serveurs du système de supervision Poste de supervision Console de vidéo-surveillance

2.4 Dépendances fonctionnelles

En cherchant les relations entre les fonctions, mais sans prendre en compte l'architecture physique, il est possible de dégager les dépendances suivantes :

Fonctions	Dépendances
Indication des sorties de secours	Ordres émis par la détection incendie Remontées de données vers la supervision
Ventilation	Ordres émis par la supervision Ordres émis par la Détection incendie Remontées de données vers la supervision
Signalisation	Ordres émis par la supervision Ordres émis par la Centrale incendie Ordres émis par la Détection de véhicules hors gabarit Remontées de données vers la supervision
Appel d'urgence	Remontées des communications vers l'opérateur téléphonique Remontées de données vers la supervision
Détection véhicules hors gabarit	Remontées de données vers la supervision Ordres envoyés vers la signalisation
Vidéo-surveillance	Ordres émis par la supervision Remontées de données de télémesure vers la supervision Remontées d'images vers la supervision
Détection incendie	Remontées de données vers la supervision Ordres envoyés vers l'Indication des sorties de secours, la Ventilation, la Signalisation.
Contrôle de la qualité de l'air	Remontées de données vers la supervision Ordres envoyés vers la ventilation
Alimentation et distribution électrique	Ordres émis par la supervision Remontées de données vers la supervision
Supervision	Ordres de pilotage manuel émis vers l'ensemble des fonctions Remontées de données depuis l'ensemble des fonctions Remontées des images de vidéo-surveillance

6. La boucle d'asservissement entre le moteur et ses capteurs de vitesse est généralement réalisée par un variateur de vitesse qui en pratique est l'interlocuteur de l'API pour les ordres comme pour les remontées de données. La fonction utilise également des capteurs anémométriques pour mesurer l'efficacité réelle de la ventilation.

Les relations entre les fonctions peuvent se résumer à ceux de la figure 2.2. Ce dernier fait apparaître les deux sous-fonctions de la *surpervision*, à savoir le *pilotage* et la *visualisation* à la seule fin de lisibilité du schéma. Cela ne présume en rien, à ce stade, d'une segmentation de ces deux sous-fonctions par l'emploi d'équipements distincts.

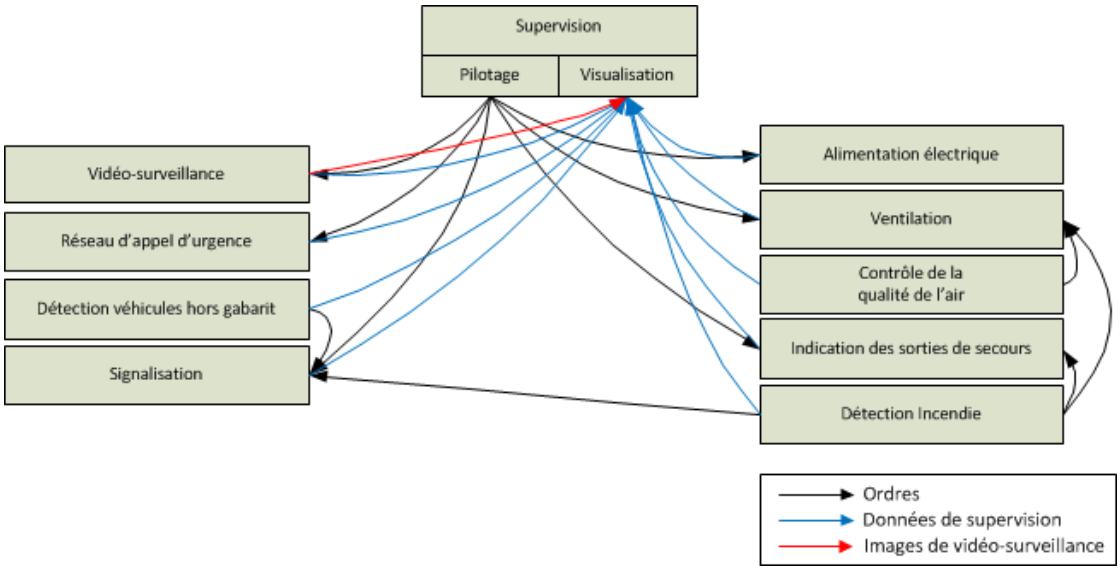

Figure 2.2 – *Système industriel - Graphe des dépendances fonctionnelles*

2.5 Première approche avant le déroulé de l'étude

Au delà des fonctions énumérées dans le paragraphe précédent, la figure 2.3 fait apparaître les différents composants logiques (modules applicatifs) qui interviennent selon les localisations (zones) géographiques : les PCC, le tunnel et les différents réseaux qui les relient.

L'architecture présentée dans la figure 2.4 est issue de l'analyse de sûreté de fonctionnement, avant prise en compte de la cybersécurité. Elle présente ainsi le périmètre du système industriel tel qu'il serait déployé sans prise en compte de la cybersécurité. Elle met en avant :

- les composants et leur localisation géographique ;
- les liaisons entre ces composants.

On retrouve tous les composants présents au niveau des PCC :

- les serveurs du système de supervision industrielle en redondance pour assurer la disponibilité des applications ;

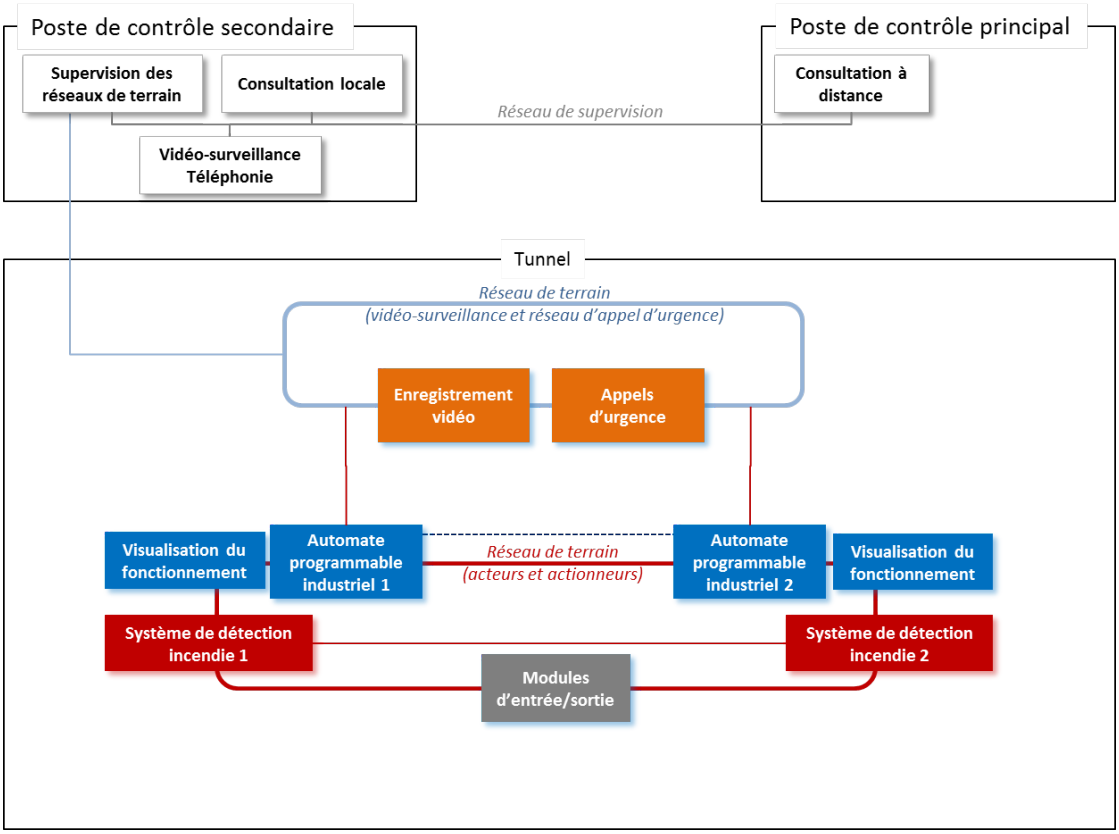

Figure 2.3 – *Système industriel - Première approche logique avant classification et méthode de sécurisation*

- les consoles pour le réseau de supervision ;
- le serveur de téléphonie (IPBX) pour les communications passées à partir des postes dans le tunnel.

En cas de défaillance matérielle, la redondance et la disponibilité des composants et des réseaux assurent le bon fonctionnement des fonctions de sécurité. On note toutefois que s'il y a bien une redondance des serveurs de supervision, celle-ci se limite au PCC secondaire, sans déport vers le PCC principal : en cas de perte du site secondaire, les fonctions de supervision ne peuvent donc plus être assurées par l'équipe d'exploitation présente à Millau. Toutefois, si cela peut poser des problèmes dans le suivi des incidents, cela ne remet pas en cause la sécurité des personnes et des biens (dans le sens sûreté) du tunnel car les automates peuvent continuer de fonctionner sans leur supervision.

La figure 2.4 présente notamment un **poste de travail (console de supervision)** relié à un serveur de supervision. Dans cette première approche technique, ce poste

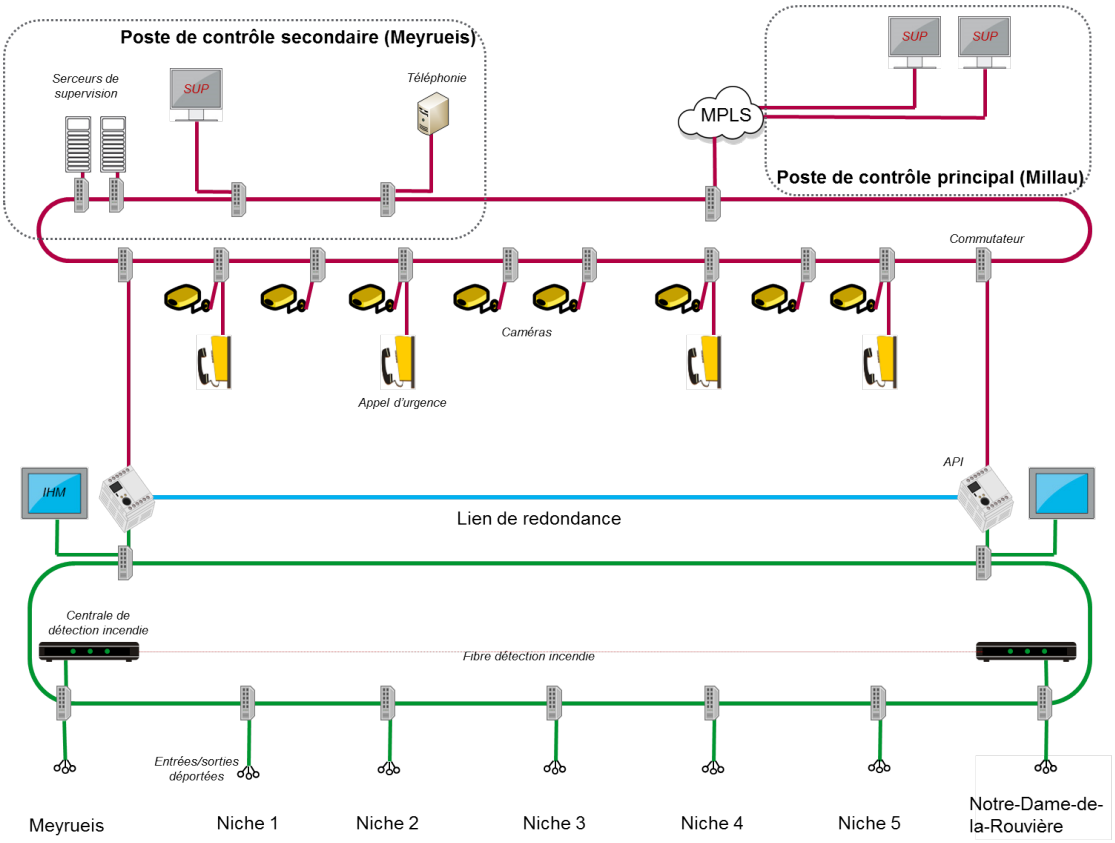

Figure 2.4 – *Système industriel - Première approche technique avant classification et méthode de sécurisation*

de travail 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.

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.

Pour permettre des actions de maintenance sur le terrain (*i.e.* dans le tunnel), un poste mobile est prévu. Ce **poste nomade de maintenance** permet de se connecter aux équipements du tunnel pour réaliser des opérations qui ne seraient pas ou plus réalisables à partir du poste fixe du PCC.

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 localisation, ce poste de maintenance pourra également être utilisé pour d'autres actions, dès lors qu'il est nécessaire de disposer de droits étendus sur un équipement.

Chapitre 3

Scénarios de menace

Bien que cette analyse ne soit pas une véritable analyse de risque, un panorama de la menace reste un pré-requis à toute étude de mise en place de mesures de protection, afin de s'assurer du bien fondé de celles-ci.

Pour réaliser ce panorama, il est bon de se rappeler que cette analyse n'est pas faite de façon isolée. Un dossier de sécurité a en effet été constitué pour l'ouverture du tunnel en exploitation, dossier pour lequel une étude de sûreté de fonctionnement a été faite [1]. Bien que cette dernière ne soit pas suffisante pour mener directement les travaux de renforcement de la cybersécurité, elle constitue une base de départ qu'il ne faut pas sous-estimer.

Il est rappelé que les missions du tunnel sont :

- permettre le transit de véhicules de l'entrée à la sortie du tunnel ;
- assurer la sécurité des usagers et du personnel en fonctionnement nominal ;
- assurer la sécurité des usagers et du personnel en cas d'incendie ou de présence de gaz.

De même, on rapellera les définitions suivantes pour éviter tout malentendu [2] :

La cybersécurité , ou sécurité des systèmes d'information, traite de la protection en disponibilité, intégrité ou confidentialité des données stockées, traitées ou transmises.

La sûreté de fonctionnement vise à s'assurer que le système industriel est apte à accomplir des fonctions dans des conditions définies. La sûreté de fonctionnement traite en particulier les propriétés de fiabilité, maintenabilité, disponibilite et sécurité (FMDS). La sécurité est entendu ici au sens des biens et des personnes.

1. Les deux études peuvent aussi être menées simultanément en fonction de la maturité des intervenants.

2. Voir le glossaire de la méthode de classification [SCADA-MTD] pour les définitions complètes de ces deux notions telles que retenues pour la présente étude de cas.

3.1 Sûreté de fonctionnement et événements redoutés

Dans le cadre de l'étude de sûreté de fonctionnement, Tunnello a notamment mené diverses analyses, dont :

- une analyse et modélisation fonctionnelle ;
- une analyse préliminaire de risques ou de dangers (APR / APD) ;
- une analyse des modes de défaillance, de leurs effets et de leur criticité (AMDEC) ;
- un arbre de défaillances (AdD).

Ces différentes analyses, et plus particulièrement l'arbre de défaillance et l'AMDEC système (ou AMDEC fonctionnelle), ont fait émerger les modes de défaillance fonctionnelle : fonction intempestive, absence de fonction, fonction erronée, non arrêt de la fonction, etc. Elles ont ainsi permis d'identifier et de caractériser la criticité des événements redoutés liés aux défaillances des fonctions du système.

Certains de ces événements redoutés, volontaires ou non, pouvant avoir pour origine un dysfonctionnement au niveau informatique, ils peuvent être repris en entrée de l'analyse de sécurité du système informatique industriel sous la forme d'événements redoutés.

La sécurité des usagers en cas d'incendie

À titre d'exemple, la présente section reprend les éléments concernant la sécurité des usagers en cas d'incendie du point de vue de la sûreté de fonctionnement : les effets des modes de défaillance sur le système y sont déclinés, accompagnés de leurs principaux impacts pour les usagers.

- Rupture de la surveillance de la sécurité incendie
  - En l'absence d'information, des usagers continuent d'avancer vers le foyer et, lorsqu'ils s'en aperçoivent, il leur est difficile de se diriger vers les sorties de secours. Il en résulte potentiellement un nombre important de blessures ou de décès, par brûlure ou par intoxication, parmi les usagers présents.
  - Les secours n'étant pas avertis de façon optimale, leur arrivée tardive peut être un facteur aggravant.
- Dégradation de la surveillance de la sécurité incendie
  - En cas de détection tardive de l'incendie, les impacts sont les mêmes que dans le cas d'une non détection, mais le nombre d'usagers concernés peut être comparativement moins important puisque l'information parvient finalement aux usagers.

  - La mauvaise localisation de l'incendie peut déclencher une ventilation localisée inadaptée. De ce fait, le courant d'air créé attise le feu au lieu de le contenir. De plus, les fumées s'accumulent en quantité trop importante à certains endroits et ralentissent l'évacuation et l'intervention des secours.
- Traitement d'une information "Incendie" en absence d'incendie
  - Le déclenchement intempestif d'une alerte incendie peut mobiliser inutilement des moyens et des personnels.
  - L'indisponibilité du tunnel se prolongera au delà de la levée de doute, afin de prendre en compte les réactions potentiellement incontrôlées des usagers ainsi que le retour de ceux ayant quitté leur véhicules.

3.2 Étude des scénarios de menace

Les éléments décrits dans la section précédente, ainsi que ceux en provenance du travail équivalent sur les autres groupes d'événements redoutés (présence de gaz par exemple) permettent d'initier le panorama des menaces potentielles sur le système industriel, avec les listes des événements redoutés, des vulnérabilités ainsi que des impacts. Ces listes sont ensuite complétées par une réflexion plus axée sur les spécificités de la cybersécurité.

3.2.1 Événements redoutés

Comme indiqué en introduction de ce chapitre, il est possible de dégager une liste d'événements redoutés à partir de l'analyse de sûreté de fonctionnement, complétée par une réflexion sur la cybersécurité.

Dans le cadre de l'étude de cas, les événements redoutés qui ont été retenus pour une étude plus précise dans la suite de cette section sont les suivants :

- la compromission des données de métrologie (supervision) ;
- la modification des ordres de pilotage (supervision) ;
- la modification des données automates ;
- l'altération des données d'historique ;
- l'injection de données de terrain.

Les cinq prochaines sous-sections listent les différents scénarios qui peuvent mener à chacun de ces événements redoutés ainsi que les impacts que peuvent engendrer ces événements.

Ces scénarios seront ensuite décrits dans la section 3.2.2.

Compromission des données de métrologie

Dans le cas de cet événement redouté, les valeurs affichées par la supervision sont modifiées par l'attaquant et ne reflètent donc plus nécessairement la réalité. Par extension, on inclut dans cette catégorie l'altération des images de la vidéo-surveillance.

Les scénarios de menace pouvant conduire à cet événement redouté

Localisation	Scénarios de menace
Au niveau du PCC	Accès non autorisé au poste de travail. Compromission du poste de travail. Accès non autorisé au serveur de supervision. Compromission du serveur de supervision. Accès non autorisé au réseau du PCC.
Au niveau du tunnel	Accès non autorisé aux automates (API). Accès non autorisé aux réseaux de terrain. Compromission des automates. Compromission des consoles IHM[3]. Compromission des capteurs / actionneurs.

Les impacts

La compromission des données de métrologie a pour résultat une vision faussée de la réalité, que ce soit au niveau des opérateurs ou des automates.

Il peut dès lors en découler une absence de réaction appropriée, telle que l'absence de déclenchement du désenfumage en cas d'incendie, ou, à l'inverse, des décisions inappropriées telles que des déclenchements d'alarmes intempestives. L'opérateur peut aussi croire qu'une réaction automatique a bien eu lieu alors qu'il n'en est rien. Plus généralement, l'événement peut s'apparenter à une perte de contrôle à distance du tunnel par les opérateurs d'autant plus grave qu'elle peut passer inaperçue.

L'événement peut également engendrer une altération de la journalisation de l'état du système ou une diffusion de fausses vidéos à destination des écrans de supervision masquant des actions malveillantes.

Modification des consignes de pilotage

3. Les interfaces homme-machines permettent d'assurer une interaction sur le terrain entre les opérateurs et les API. Voir l'annexe A.5 de la seconde partie de l'étude [SCADA-TNL-2] pour plus de précision.

Concernant cet événement redouté, les ordres reçus par les équipements du système industriel ont été altérés par l'attaquant. Ils ne correspondent donc plus nécessairement aux instructions données par les opérateurs.

Les scénarios de menace pouvant conduire à cet événement redouté

Localisation	Scénarios de menace
Au niveau du PCC	Accès non autorisé au poste de travail. Compromission du poste de travail. Accès non autorisé au serveur de supervision. Compromission du serveur de supervision. Accès non autorisé au réseau du PCC.
Au niveau du tunnel	Accès non autorisé aux automates (API). Compromission des automates. Accès non autorisé aux consoles IHM. Compromission des consoles IHM. Accès non autorisé aux réseaux de terrain. Accès non autorisé aux capteurs / actionneurs. Compromission des capteurs / actionneurs.

Les impacts

Les impacts d'une modification des consignes de pilotage sont très significatifs.

Les serveurs de supervision peuvent être dans un état instable, avec des arrêts ou des redémarrages intempestifs, ne permettant plus à l'exploitant d'assurer ses fonctions de pilotage de l'activité du tunnel de manière fiable.

Cet événement est par ailleurs un facteur aggravant lorsqu'il intervient en même temps qu'une compromission des données de métrologie. En effet, l'exploitant ne peut plus se fier ni aux informations qu'il reçoit ni aux ordres qu'il émet (se mettre dans une position d'attente sécurisée par exemple). L'absence de tout contrôle par la supervision peut perturber sérieusement le fonctionnement des installations.

Modification des données automates

Il s'agit ici de considérer le cas d'une modification des données stockées au sein de l'automate par l'attaquant. Il peut s'agir des applicatifs clients, des programmes, de la configuration ou des firmwares des automates.

Les scénarios de menace pouvant conduire à cet événement redouté

Localisation	Scénarios de menace
Au niveau du PCC	Non-applicable.
Au niveau du tunnel	Accès non autorisé aux automates (API). Compromission des automates. Accès non autorisé au poste de maintenance. Compromission du poste de maintenance. Utilisation du poste de maintenance comme pont de connexion. Perte ou vol du poste de maintenance.

Les impacts

Du fait de leur criticité, la modification des données stockées au sein de l'automate est l'événement redouté dont les impacts sont les plus importants.

Il n'est en effet plus possible d'avoir confiance dans le bon fonctionnement de l'automate, notamment dans la cohérence des décisions qu'il peut être amené à prendre en réaction aux informations qui lui parviennent ou dans sa capacité à maintenir les installations dans un état stable et prédictible.

De plus, il est possible pour l'attaquant de mettre en place des actions pré-programmées, se déclenchant sans lien avec la situation réelle ou en les dissimulant de la supervision par les opérateurs.

L'altération des données des automates peut aussi rendre les installations totalement inopérantes ou incontrôlables.

Enfin, il est fréquent que les programmes au sein des automates comprennent des limites admissibles dans les valeurs transmises aux actionneurs pour en garantir le bon fonctionnement. Une altération de ces limitations peut entraîner des actions en dehors des zones de sûreté (exemple d'un moteur tournant sensiblement plus vite que ce que peut supporter ses fixations, ce qui peut entraîner une destruction des installations de ventilation).

Altération des données d'historique

Ici, l'attaquant parvient à effacer ou altérer des données d'historiques. Il peut s'agir de journaux d'activité, de tableaux de bord ou d'alertes.

Les scénarios de menace pouvant conduire à cet événement redouté

Localisation	Scénarios de menace
Au niveau du PCC	Accès non autorisé au serveur de supervision. Compromission du serveur de supervision.
Au niveau du tunnel	Accès non autorisé aux automates (API). Compromission des automates.

Les impacts

La principale conséquence d'une altération des données d'historique est de ne potentiellement plus être en capacité de répondre aux obligations de traçabilité.

Si les missions du tunnel ne sont pas directement remises en cause, cette absence d'historique remet en cause la confiance que l'on peut accorder à l'intégrité des différents éléments du système informatique industriel. Il est dès lors difficile de repérer les éléments précurseurs des événements redoutés ci-dessus, et toute investigation est rendue impossible.

Injection de données de terrain

L'attaquant arrive à propager des informations arbitraires au sein du système industriel. Il peut s'agir de fausses remontées de valeurs supposées venir de capteurs, ou de faux ordres à destination des actionneurs.

Les scénarios de menace pouvant conduire à cet événement redouté

Localisation	Scénarios de menace
Au niveau du PCC	Accès non autorisé au serveur de supervision. Compromission du serveur de supervision. Accès non autorisé au réseau du PCC.
Au niveau du tunnel	Accès non autorisé aux réseaux de terrain. Accès non autorisé aux automates (API). Compromission des automates. Compromission des consoles IHM. Accès non autorisé aux capteurs / actionneurs. Compromission des capteurs / actionneurs. Accès non autorisé au poste de maintenance. Compromission du poste de maintenance. Utilisation du poste de maintenance comme pont de connexion. Perte ou vol du poste de maintenance.

Les impacts

Les impacts de cet événement redouté sont relativement proche des deux premiers, à savoir l'altération des données de métrologie et celle des consignes de pilotage.

3.2.2 Scénarios de menace

Le tableau suivant liste les scénarios de menace possibles dans le PCC. Le détail des vulnérabilités sera précisé dans la section 3.2.3.

Scénario de menace	Vulnérabilité
Accès non autorisé au poste de travail	Pas de verrouillage systématique de la session. Pas de protection des identifiants et des mots de passe. Faiblesse des mots de passe. Faiblesse de la configuration. Vulnérabilité du système d'exploitation.
Compromission du poste de travail	Absence de vérification de l'innocuité des supports amovibles. Navigation Internet et messagerie. [4] Utilisation inappropriée du poste de travail. Application d'une mise à jour compromise.
Accès non autorisé au serveur de supervision	Pas de verrouillage systématique de la session. Pas de protection des identifiants et des mots de passe. Faiblesse des mots de passe. Faiblesse de la configuration. Accès depuis un poste de travail compromis. Vulnérabilité du système d'exploitation. Envoi de trames forgées.
Compromission du serveur de supervision	Application d'une mise à jour compromise. Absence de vérification de l'innocuité des supports amovibles. Accès direct à Internet.
Accès non autorisé au réseau du PCC	Vulnérabilité des équipements réseau. Faiblesse du cloisonnement MPLS. Accès physique aux équipements réseau.

Le tableau suivant liste les scénarios de menace possibles dans le tunnel. Le détail des vulnérabilités sera précisé dans la section 3.2.3.

4. Lorsque ces fonctions sont strictement nécessaires pour le poste en question. Dans le cas contraire, ils sont inclus dans les usages inappropriés du poste.

Scénario de menace	Vulnérabilité
Accès non autorisé aux réseaux de terrain	Accès physique aux équipements réseau. Accès physique au câblage réseau. Vulnérabilité des équipements réseau.
Accès non autorisé aux automates (API)	Utilisation d'un compte par défaut. Pas de verrouillage systématique de la session. Pas de protection des identifiants et des mots de passe. Faiblesse des mots de passe. Faiblesse de la configuration. Vulnérabilité des automates. Envois de trames forgées. Accès depuis un poste compromis.
Compromission des automates	Mise à jour diffusée par le constructeur ou l'intégrateur et comportant des erreurs. Mise à jour compromise diffusée par un attaquant se faisant passer pour l'intégrateur. Mise à jour compromise diffusée par un attaquant ayant accès au réseau. Mise à jour compromise diffusée suite à la compromission du poste de maintenance.
Accès non autorisé aux consoles IHM	Utilisation d'un compte par défaut. Pas de verrouillage systématique de la session. Pas de protection des identifiants et des mots de passe. Faiblesse des mots de passe. [5] Vulnérabilité du programme des consoles IHM. Envoi de trames forgées.
Compromission des consoles IHM	Mise à jour diffusée par le constructeur ou l'intégrateur et comportant des erreurs. Mise à jour compromise diffusée par un attaquant se faisant passer pour l'intégrateur. Mise à jour compromise diffusée par un attaquant ayant accès au réseau. Mise à jour compromise diffusée suite à la compromission du poste de maintenance.
Accès non autorisé aux capteurs / actionneurs	Pas de protection des identifiants et des mots de passe. [6] Vulnérabilité des automates. Envoi de trames forgées. Accès physique.

6. Lorsque ces identifiants et mots de passe existent.

Scénario de menace	Vulnérabilité
Compromission des capteurs / actionneurs	Mise à jour diffusée par le constructeur ou l'intégrateur et comportant des erreurs. Mise à jour compromise diffusée par un attaquant se faisant passer pour l'intégrateur. Mise à jour compromise diffusée par un attaquant ayant accès au réseau. Mise à jour compromise diffusée suite à la compromission du poste de maintenance.
Accès non autorisé au poste de maintenance	Pas de verrouillage systématique de la session. Pas de protection des identifiants et des mots de passe. Faiblesse des mots de passe. Vulnérabilité du système d'exploitation.
Compromission du poste de maintenance	Absence de vérification de l'innocuité des supports amovibles. Vérification antivirale insuffisante sur la messagerie. Navigation internet. Utilisation inappropriée du poste de travail. Faiblesse de la configuration. Application d'une mise à jour compromise.
Utilisation du poste de maintenance comme pont de connexion	Double connexion (par exemple, utilisation d'une clé 3G tout en étant connecté aux installations du tunnel). Une mauvaise configuration peut rendre les installations du tunnel directement accessibles depuis Internet.
Perte ou vol du poste de maintenance	Négligence. Agression. Acte volontaire de l'exploitant ou de l'intégrateur.

3.2.3 Vulnérabilités

Le tableau ci-dessous liste les vulnérabilités pouvant mené à un accès non-autorisé.

Vulnérabilité	Description
Pas de verrouillage systématique de la session	Un utilisateur exploitant ou intégrateur a laissé sa session ouverte. De manière similaire, il n'y a pas de fermeture automatique de session après un laps de temps, laissant la possibilité à quiconque d'utiliser la session.

6. La complexité du mot de passe doit être adaptée à la sensibilité du système industriel, tout en prenant en compte l'environnement et l'utilisabilité de ce type de console.

Vulnérabilité	Description
Pas de protection des identifiants et des mots de passe	Ces informations utilisateur sont, par exemple, inscrites sur un tableau ou un cahier ou tout autre support accessible par une personne non autorisée. De manière similaire, les éléments d'authentification des utilisateurs ne sont pas stockés de manière sécurisée.
Faiblesse des mots de passe	La politique de gestion du mot de passe n'est pas assez forte pour imposer des mots de passe dont la complexité est suffisante.
Faiblesse des protocoles de communication	Les protocoles utilisés ne permettent pas de protection des échanges, que ce soit en confidentialité ou en intégrité, permettant une interception ou une modification des flux. Cela peut concerner par exemple les échanges entre serveur de supervision et poste de travail, ou entre PCC principal et secondaire.
Faiblesse de la configuration.	La configuration du poste ou de l'équipement ne correspond pas aux bonnes pratiques (absence de pare-feu local, poste en « AutoLogin ») et rend de fait le poste inutilement sensible aux attaques.
Vulnérabilité du système d'exploitation	Une vulnérabilité peut être découverte au niveau du système d'exploitation donnant la possibilité à un attaquant d'accéder et de compromettre le système de supervision.
Perte ou vol d'un poste nomade	La probabilité d'une perte ou d'un vol est sensiblement plus importante pour un poste de travail nomade que pour un ordinateur de bureau. Ce point est par ailleurs aggravé lorsque le poste est partagé et n'est pas affecté à un lieu ou une personne : il est en effet possible que la disparition du poste passe inaperçue, laissant un temps plus important à l'attaquant pour récupérer les données sensibles ou les accès pré-configurés à certains équipements qu'il pourrait contenir.
Utilisation d'un compte par défaut	Les constructeurs et éditeurs peuvent mettre en place un ou plusieurs comptes par défaut pour faciliter la prise en main, laissant à quiconque ayant la documentation un accès avec les autorisations accordées à ces comptes.

Vulnérabilité	Description
Accès depuis un poste compromis	Un utilisateur n'a pas conscience que son poste a été compromis et accède à un autre équipement (serveur de supervision, API, etc.). L'attaquant à l'origine de la compromission peut récupérer les identifiants et mots de passe utilisés ou profiter de la connexion établie.
Accès physique aux équipements	L'absence de limitation dans l'accès physique aux équipements (postes de travail, capteurs, actionneurs, etc.) laisse la possibilité à n'importe qui d'y apporter des modifications (piégeage, modification de la configuration, etc.).
Accès physique au réseau	L'absence de limitation dans l'accès physique aux équipements réseaux du PCC ou du tunnel la possibilité à n'importe qui de modifier les connexions existantes ou de connecter un équipement extérieur.

Le tableau suivant liste les vulnérabilités pouvant mener à une compromission.

Vulnérabilité	Description
Absence de vérification de l'innocuité des supports amovibles	En l'absence de restriction sur l'usage des supports amovibles, un utilisateur peut involontairement importer puis transporter un maliciel d'un poste à un autre. Outre les supports amovibles classiques, l'import et la transmission peuvent aussi se faire via un téléphone qu'il connecte sur le port USB de son poste pour le recharger.
Accès direct à internet et aux courriels	Un utilisateur accède directement et sans précaution particulière à un site web compromis depuis son poste de travail ou ouvre une pièce jointe malveillante. Une fois contaminé, il utilise ce même poste pour se connecter à un équipement. Cet accès peut se faire via la connexion réseau usuelle du poste ou via un téléphone connecté en USB.
Utilisation inappropriée du poste de travail	Un utilisateur peut installer des logiciels à usage non professionnel sur son poste de travail (jeux, lecteur audio, etc.).

Vulnérabilité	Description
Manque de vérification des mises à jour	Un utilisateur récupère une mise à jour et la déploie sur l'équipement concerné. L'absence de vérification ne permet pas de s'assurer que la mise à jour correspond bien à celle diffusée par le constructeur ou l'intégrateur.
Accès depuis un poste de travail compromis	Un utilisateur n'a pas conscience que son poste a été compromis et accède à un autre équipement (serveur de supervision, API, etc.). La connexion est alors utilisée pour propager le maliciel à l'origine de la compromission.
Diffusion non maitrisée d'informations sensibles	Dans le cadre d'une action de communication, l'entreprise décrit avec trop de précision les équipements et leur mise en œuvre. L'attaquant n'a plus qu'à s'informer sur les vulnérabilités des équipements en question pour mener son attaque.

3.3 Exemples de scénarios d'attaque

3.3.1 Cas d'une attaque ciblée : installation d'un maliciel

Une attaque ciblée correspond à un acte volontaire avec l'intention de nuire aux missions du tunnel.

C'est le cas, par exemple, d'un employé mal intentionné de l'intégrateur Integro. Il bénéficie d'un poste de travail sur lequel sont installés les outils de maintenance du logiciel de supervision. Il se peut que l'employé introduise un maliciel dans le code source. Si aucune protection ou vérification de code n'est effectuée, soit lors de la compilation en local, soit lors de la copie du code compilé, le logiciel infecté sera copié sur le poste d'administration qui sera ensuite déployé sur le serveur de supervision.

À partir de ce moment, tous les composants du réseau de supervision et du réseau de terrain peuvent être infectés par la propagation du maliciel.

Dans ce cas, l'application de supervision est inopérante. Les alarmes ne sont plus remontées au niveau de la console de l'exploitant. De même, les caméras vidéos ne permettent plus de contrôler visuellement la circulation dans le tunnel. Par conséquent, et par mesure de précaution, le tunnel doit être fermé.

3.3.2 Cas d'une attaque non ciblée : propagation d'un virus

Une attaque non ciblée correspond à un acte, volontaire ou non, sans que celui-ci ne traduise une volonté de nuire aux missions du tunnel.

C'est le cas par exemple, d'un employé de l'exploitant Tunnello qui connecte son poste de travail pour télécharger une mise à jour du firmware d'un équipement. Il en profite pour naviguer sur quelques sites non sécurisés pour son usage personnel, infectant son poste avec un maliciel maquillé en document bureautique. Après sa navigation, l'employé déconnecte son poste d'Internet et le connecte sur le réseau du tunnel pour mettre à jour l'équipement concerné : le maliciel peut alors se propager sur le serveur de supervision.

Si le maliciel n'est pas destiné aux systèmes industriels, il peut simplement rendre inopérant l'ensemble des ordinateurs du PCC, serveur de supervision compris. Cela ne permet plus aux opérateurs de s'assurer du bon fonctionnement du tunnel, et ils décident alors de fermer ce dernier.

Si à l'inverse le maliciel est « typé industriel », il peut se propager sur les équipements du tunnel, envoyant par exemple des commandes STOP dans les différents protocoles courants. Cela a pour effet de rendre le tunnel inexploitable et de provoquer des dégradations au niveau de certains actionneurs.

3.3.3 Cas d'une attaque ciblée indirecte : équipements piégés

Une attaque indirecte consiste à faire intégrer des équipements piégés avant leur arrivée sur le site (en sortie d'usine ou durant son acheminement).

Cette étude de cas exclut néanmoins explicitement l'hypothèse d'un attaquant de niveau étatique capable d'utiliser un tiers (fournisseur, intégrateur ou un transporteur) pour réaliser une attaque de ce type sur le tunnel : la chaîne d'approvisionnement de Tunnello est en effet considérée comme maîtrisée et intègre.

3.4 Analyse de la sécurité relative à l'architecture de première approche avant déroulé de la méthode

L'architecture de la figure 2.4, présentée avant la méthode de sécurisation, montre les composants physiques répartis sur le réseau de supervision et le réseau de terrain. Ce schéma fait apparaître les équipements vidéos directement connectés au réseau de supervision (par l'intermédiaire de switchs).

On constate la redondance pour chaque type de composant :

- les postes de commandement : Meyrueis et Millau ;
- les serveurs de supervision à l'intérieur d'un poste de contrôle/commande ;
- les équipements connectés au réseau de supervision et au réseau de terrain.

La section précédente a mis en avant des exemples d'attaques, volontaires ou non, qui s'appliquent à l'architecture non sécurisée de la figure 2.4. La connexion d'un poste de travail (de l'intégrateur ou de l'exploitant) sur le réseau de supervision est une faille avérée du système industriel. En effet :

- le poste de l'intégrateur n'est pas maîtrisé ;
- le poste de l'exploitant peut a priori se connecter à Internet (que cette connexion soit simultanée ou non avec la connexion aux équipements du tunnel) ;
- le même poste est utilisé pour la maintenance de plusieurs tunnels.

Par ailleurs, le manque de journalisation et de détection d'intrusion ne permet pas de déceler au plus tôt des menaces potentielles.

Enfin, aucun moyen de filtrage ne permet d'assurer un niveau de cloisonnement entre les différents réseaux, ce qui limite la sécurisation (au sens cybersécurité) de cette solution.

Les moyens de sécurisation sont détaillés par scénario dans les chapitres suivants.

Chapitre 4

Classification

D'après la méthodologie formalisée par le groupe de travail, il convient, une fois la liste des fonctions principales établie (cf. la section 2.3), de réaliser la classification de ces dernières suivant leur besoin en termes de cybersécurité.

Il est rappelé que pour les systèmes industriels la méthode propose trois classes numérotées de 1 à 3, par ordre croissant de criticité, dont les couvertures sont :

- Classe 1 : le risque et l'impact d'une attaque sont faibles ;
- Classe 2 : le risque ou l'impact d'une attaque est significatif ;
- Classe 3 : le risque ou l'impact d'une attaque est critique.

La classification est réalisée en fonction de la vraisemblance et de l'impact d'une attaque.

L'impact d'une attaque est mesuré suivant des échelles qui peuvent être suivant les cas normalisés ou propres à l'entreprise, suivant son niveau de résilience et les risques qu'elle estime acceptable. Ces échelles sont généralement validées par la direction en amont des analyses de risques et valables pour l'ensemble des projets. La section 4.1 présente les échelles retenues par Tunnello.

La vraisemblance quant-à elle repose sur les critères suivants :

- E l'exposition, qui reflète les niveaux de fonctionnalité et de connectivité ;
- A le niveau de l'attaquant ;
- I le niveau d'accessibilité du système industriel par les intervenants.

La vraisemblance s'obtient alors avec la formule suivante :

$$V = E + \left\lceil \frac{A + I - 2}{2} \right\rceil$$

On se reportera à la documentation de référence de la méthode de classification [SCADA-MTD] pour une description plus complète des classes (section 2.1) et des critères (section 3.2), ainsi que les relations entre ces derniers.

4.1 Échelles

Au vu de ses obligations et de ses besoins, la société Tunnello a arrêté une échelle de gravité de 1 à 5, reposant sur les échelles d'impact telles qu'indiquées ci-dessous :

	Niveau	Qualificatif	Description des conséquences
Impacts humains	1	Insignifiant	Accident déclaré sans arrêt ni traitement médical.
	2	Mineur	Accident déclaré avec arrêt ou traitement médical.
	3	Modéré	Invalidité permanente.
	4	Majeur	Un décès.
	5	Catastrophique	Plusieurs décès.

	Niveau	Qualificatif	Description des conséquences
Impacts financiers	1	Insignifiant	Accident n'entraînant aucun travail de remise en état
	2	Mineur	Accident entraînant des travaux de remise en état limités
	3	Modéré	Détérioration majeure du tunnel dont la remise en état représente plus de 5% du prix de construction du tunnel
	4	Majeur	Détérioration majeure du tunnel dont la remise en état représente plus de 15% du prix de construction du tunnel
	5	Catastrophique	Détérioration majeure du tunnel dont la remise en état représente plus de 40% du prix de construction du tunnel

	Niveau	Qualificatif	Description des conséquences
Impacts en disponibilité	1	Insignifiant	Accident entraînant une perturbation sur un seul sens de circulation
	2	Mineur	Accident provoquant la fermeture d'un sens de circulation ou perturbant les deux sens de circulation (circulation alternée par exemple) pendant plusieurs heures
	3	Modéré	Détérioration mineure du tunnel représentant plusieurs jours d'indisponibilité pour réparation
	4	Majeur	Détérioration majeure du tunnel représentant plus d'un mois d'indisponibilité pour réparation
	5	Catastrophique	Détérioration majeure du tunnel représentant plus de 6 mois d'indisponibilité pour réparation

Il est à noter que pour simplifier son étude, Tunnello a décidé d'inclure les impacts juridiques et d'image, au sein de l'impact financier qui couvre également les pertes d'exploitation : du fait de son activité, ces derniers se présenteront surtout sous la forme de dommages et intérêts ou de perte d'activité.

Tunnello estime également que les impacts en disponibilité de niveau mineur et modéré ne s'appliquent qu'en cas d'impact sur les périodes de pointe (période de fort transit durant les vacances scolaires), le contournement par la route historique (qui représente une augmentation de trajet de 30 minutes) étant jugé acceptable le reste de l'année.

Tunnello a par ailleurs décidé de prendre les mêmes échelles définissant les niveaux de vraisemblance, d'attaquant et d'intervenant que celles données en exemple dans le guide [SCADA-MTD], celles-ci étant jugées adaptées à la situation.

4.2 Hypothèses de l'étude

Pour l'ensemble de l'analyse, Tunnello retient un attaquant de type organisation privée aux moyens conséquents (terrorisme par exemple), donc de niveau 4 d'après le guide sur la classification.

Par ailleurs, comme la possibilité de traçabilité de l'ensemble des actions sur l'ensemble des composants ne peut être garantie, les intervenants sont supposés de niveau 2, c'est-à-dire autorisés et habilités, pour l'ensemble des fonctions.

Enfin, les fonctions critiques doivent pouvoir être déclenchées de manière autonome et automatique (fonctions réflexes).

4.3 Classification par fonction

Cette analyse s'appuie en grande partie sur l'analyse des risques et des menaces présentée dans le chapitre 3. Dans un premier temps, elle est menée sur les fonctions isolées, c'est-à-dire sans prendre en compte les dépendances décrites dans la section 2.4, qui seront prises en compte par la suite.

Détection incendie

La détection incendie est une fonction de sûreté de fonctionnement particulièrement critique puisqu'elle est chargée de déclencher certaines actions réflexes et de lever des alertes sur incident à destination du poste de contrôle/commande.

L'analyse donne ainsi une fonctionnalité de 2 et une connectivité de 4. Étant données les hypothèses sur les intervenants et les attaquants, on en déduit une exposition de 4, et une vraisemblance de 6.

L'analyse AMDEC de la fonction (section 3.1) permet par ailleurs à Tunnello de quantifier l'impact d'un éventuel dysfonctionnement de la fonction à un niveau catastrophique (5).

On obtient ainsi une fonction de classe 3.

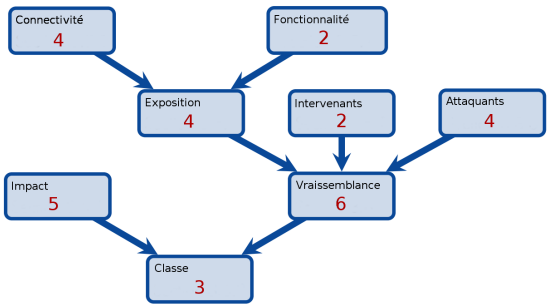

Figure 4.1 – *Classification - Détection incendie*

Contrôle de la qualité de l'air

Cette fonction est destinée à repérer des concentrations trop importantes de gaz toxiques, et tout particulièrement les gaz d'échappement. Comme pour la détection incendie, elle est chargée de déclencher certaines actions réflexes et de lever des alertes sur incident à destination du poste de contrôle/commande.

Cette première analyse donne donc une fonctionnalité de 2 et une connectivité de 4. Étant données les hypothèses sur les intervenants et les attaquants, on en déduit une exposition de 4, et une vraisemblance de 6.

L'analyse AMDEC de la fonction permet par ailleurs à Tunnello de quantifier l'impact d'un éventuel dysfonctionnement de la fonction à un niveau majeur (4) en cas d'accumulation non détectée à temps (et donc non prise en compte par les autres fonctions).

On obtient ainsi une fonction de classe 3.

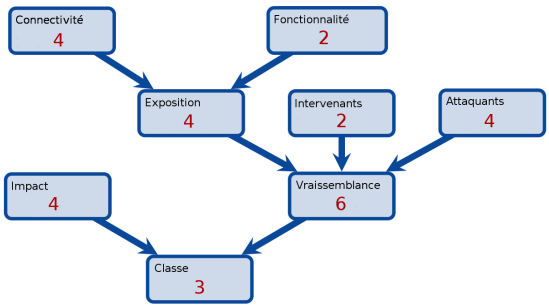

Figure 4.2 – *Classification - Contrôle de la qualité de l'air*

Indication des sorties de secours

Disposant d'une batterie pour pallier un éventuel arrêt de l'alimentation électrique, la fonction d'indication des sorties de secours peut être mise en œuvre de deux façons :

- déconnectée et autonome, elle reste allumée en permanence ;
- connectée comme les autres composants du tunnel, elle est pilotée par la centrale incendie ou la supervision.

Dans le premier cas, la fonction n'est pas à proprement parlé un système industriel et peut être exclue de la suite de l'analyse.

Dans le second cas, on retrouve une fonctionnalité de 1 et une connectivité de 4. Étant données les hypothèses sur les intervenants et les attaquants, on en déduit une exposition de 4, et une vraisemblance de 6.

L'impact direct est insignifiant (l'arrêt de la fonction alors que le tunnel est en mode nominal n'a pas de conséquence), mais l'impact indirect, comme facteur aggravant d'un incident, est de niveau 5 (mort de plusieurs personnes n'ayant pas trouvé la sortie de secours).

On obtient ainsi une fonction de classe 3.

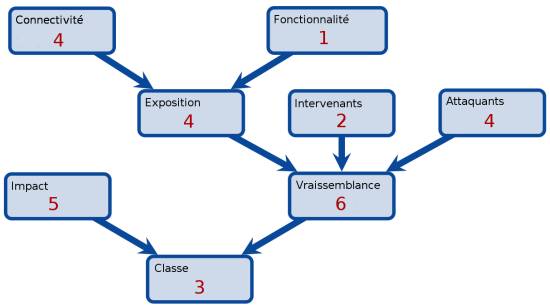

Figure 4.3 – *Classification - Indication des sorties de secours*

Ventilation

La ventilation du tunnel est une fonction vitale tant en mode nominal que suite à un incident. Il s'agit en effet, dans le premier cas, d'éviter l'accumulation de gaz d'échappement (toxiques pour les personnes) et, dans le deuxième cas, d'évacuer les fumées (mais sans attiser les flammes d'un incendie).

La ventilation fonctionne donc à la fois en mode réflexe et sur pilotage du poste de contrôle/commande, qui la supervise.

L'analyse donne donc une fonctionnalité de 2 et une connectivité de 4. Étant données les hypothèses sur les intervenants et les attaquants, on en déduit une exposition de 4, et une vraisemblance de 6.

L'impact d'un dysfonctionnement peut être catastrophique, tant en fonctionnement nominal (asphyxie par l'accumulation des gaz d'échappement) que suite à un accident (asphyxie par les fumées non évacuées, activation d'un incendie, etc).

On obtient ainsi une fonction de classe 3.

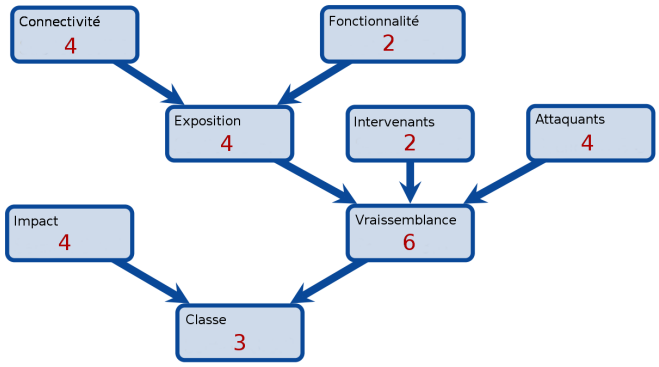

Figure 4.4 – *Classification - Ventilation*

Signalisation

Cette fonction correspond à la fois aux panneaux à message variable et aux divers signaux (signaux lumineux d'affectation de voies, barrières d'accès motorisées, etc.) qui peuvent être utilisés dans le tunnel. Ces signaux sont essentiellement pilotés par le poste de contrôle/commande.

L'analyse donne donc une fonctionnalité de 2 et une connectivité de 4. Étant données les hypothèses sur les intervenants et les attaquants, on en déduit une exposition de 4, et une vraisemblance de 6.

Leur dysfonctionnement peut entraîner un accident mais les conducteurs devant rester maîtres de leurs véhicules, l'impact est considéré comme modéré (3).

On obtient ainsi une fonction de classe 2.

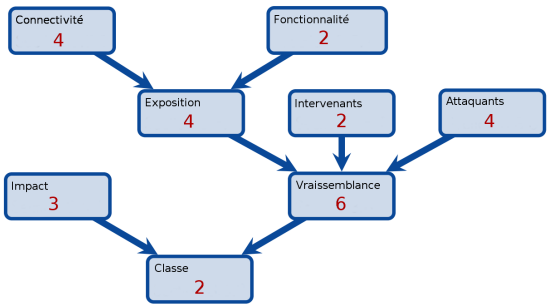

Figure 4.5 – *Classification - Signalisation*

Réseau d'appel d'urgence

Cette fonction correspond à la possibilité pour les personnes circulant dans le tunnel de pouvoir prendre contact avec le poste de contrôle/commande ou à défaut les secours pour signaler une urgence ou une difficulté (par exemple une panne du véhicule rendant impossible la fin de son trajet au sein du tunnel).

L'analyse donne donc une fonctionnalité de 2 et une connectivité de 4. Étant données les hypothèses sur les intervenants et les attaquants, on en déduit une exposition de 4, et une vraisemblance de 6.

Ce dispositif a pour but premier de permettre à un usager de demander de l'assistance pour résoudre un problème le concernant. De plus ce dispositif vient en complément d'autres dispositifs permettant d'alerter le PCC de la survenue d'un incident. Son impact est donc considéré comme de niveau 1.

On obtient ainsi une fonction de classe 1.

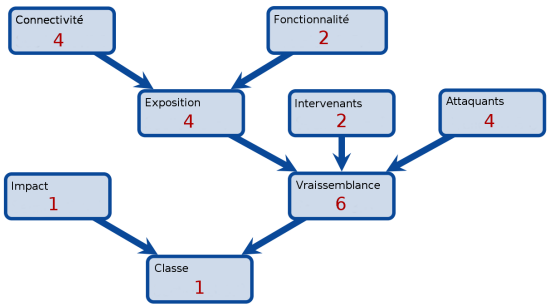

Figure 4.6 – *Classification - Réseau d'appel d'urgence*

Détection de véhicules hors gabarit

Cette fonction correspond aux équipements permettant de détecter des véhicules qui pourraient éventuellement bloquer le trafic à l'entrée ou à l'intérieur du tunnel (remorques hors norme par exemple), pour les inciter à utiliser un autre itinéraire.

Ces équipements sont supervisés par le poste de contrôle/commande. L'analyse donne donc une fonctionnalité de 2 et une connectivité de 4. Étant données les hypothèses sur les intervenants et les attaquants, on en déduit une exposition de 4, et une vraisemblance de 6.

Le dysfonctionnement de ce mécanisme, complémentaire aux panneaux routiers de sorte qu'un conducteur respectant le code de la route ne s'engagera pas, entraînera au pire la fermeture du tunnel, donc un impact de niveau 1.

On obtient ainsi une fonction de classe 1.

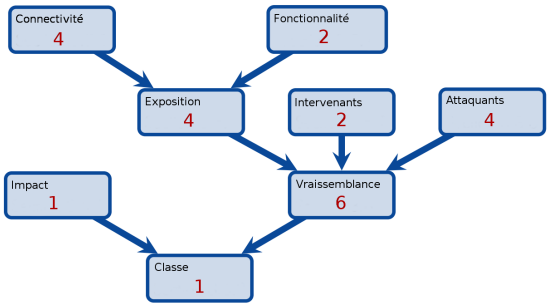

Figure 4.7 – *Classification - Détection de véhicules hors gabarit*

Vidéo-surveillance

La vidéo-surveillance permet aux opérateurs du poste de contrôle/commande de suivre l'état du trafic à l'aide de caméras situées à l'intérieur du tunnel.

L'analyse donne donc une fonctionnalité de 2 et une connectivité de 4. Étant données les hypothèses sur les intervenants et les attaquants, on en déduit une exposition de 4, et une vraisemblance de 6.

La vidéo-surveillance étant essentiellement utilisée comme une aide à l'exploitation du tunnel en complément des autres fonctions, un dysfonctionnement est considéré comme ayant un impact de 1.

On obtient ainsi une fonction de classe 1.

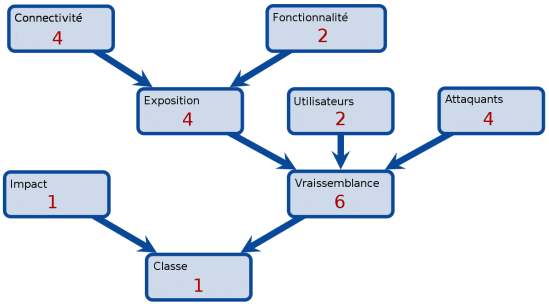

Figure 4.8 – *Classification - Vidéo-surveillance*

Alimentation et distribution électrique

Cette fonction regroupe les capteurs et actionneurs en charge de la stabilité de l'alimentation électrique, en particulier sa bascule en mode secouru (l'installation dispose d'un groupe électrogène et d'un onduleur). La supervision de cette fonction peut également déclencher un mode dégradé (par exemple la fermeture du tunnel tout en maintenant les fonctions nécessaires à une évacuation sans incident). On en déduit donc un niveau de fonctionnalité de 2.

L'alimentation et la distribution étant supervisées par le poste de contrôle principal, sa connectivité est de 4. Il est à noter que suivant les cas, la supervision au moins partielle par le fournisseur d'énergie peut entraîner un niveau de connectivité plus important (soit un niveau de 5).

Étant données les hypothèses, on en déduit pour cette fonction une exposition de niveau 4 (ou 5 si supervision par le fournisseur d'énergie) et donc une vraisemblance de 6 (dans les deux cas).

Une attaque contre l'alimentation aura un impact direct modéré (au plus un départ d'incendie). Toutefois, dans le cas d'une alimentation automatisée, la fonction à protéger est bien la disponibilité de la fourniture d'énergie et non son automatisation. En l'absence de procédures de contournement satisfaisantes (pas de présence sur place permettant la mise en place rapide d'une alimentation de secours), l'impact indirect correspond au niveau le plus élevé en cas d'indisponibilité d'une des fonctions nécessitant une alimentation électrique. La ventilation, remplissant cette condition, induit donc un impact de 5.

On en conclut donc que l'alimentation électrique est de classe 3.

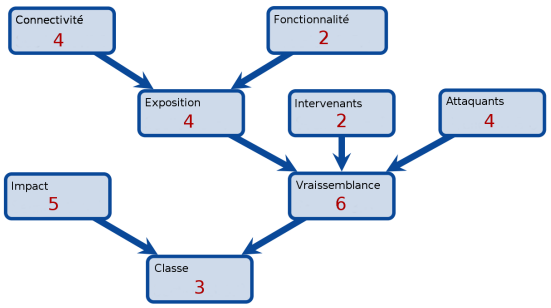

Figure 4.9 – *Classification - Alimentation et distribution électrique*

4.4 Dépendances fonctionnelles et classes

Au delà de la classification des fonctions de manière unitaire, il convient de compléter l'analyse par l'étude des relations entre ces fonctions.

En effet, un des principes fondateurs de l'analyse des dépendances fonctionnelles est qu'une information fournie par un équipement de classe haute peut être transmise à un équipement de classe inférieure, mais qu'une information issue d'un équipement de classe basse ne peut être transmise vers un équipement de niveau supérieur.

Dit autrement, un équipement de classe 2 peut transmettre des alertes et éléments de supervision vers un équipement de classe 1, mais son fonctionnement ne devrait dépendre que d'informations en provenance d'équipements de classe 2 ou 3. Un équipement de classe 3 ne peut quant à lui ne dépendre que d'informations fournies par d'autres équipements de même classe.

Ce principe est une directive dans le cas où la classe de niveau haut est la classe 3 (D.159), et une recommandation dans le cas où la classe supérieure est 2 (R.157).

Ainsi, en application de ce principe, l'analyse des dépendances fonctionnelles du chapitre précédent (et résumée dans la figure 2.2) impose de reclasser la détection hors gabarit en classe 2 du fait de sa relation avec la signalisation.

De même, il découle de ce cloisonnement entre les différentes classes la nécessité d'instancier la fonction « poste de contrôle » pour chaque classe présente dans le système d'information industriel, comme on peut le voir apparaître dans la figure 4.10.

4.5 Classification finale

En conclusion, le résultat de l'analyse est présenté dans le tableau suivant. Cette classification des fonctions sera utilisée pour la suite de l'analyse.

Classe	Fonctions
Classe 1	Vidéo surveillance Réseau d'appel d'urgence
Classe 2	Détection des véhicules hors gabarit Signalisation
Classe 3	Alimentation et distribution électrique Indication des sorties de secours Ventilation Détection incendie Contrôle de la qualité de l'air

En partant du principe qu'une fonction commune à plusieurs classes, comme c'est le cas de la Supervision, ne peut être mutualisée, on obtient le schéma de dépendances fonctionnelles 4.10.

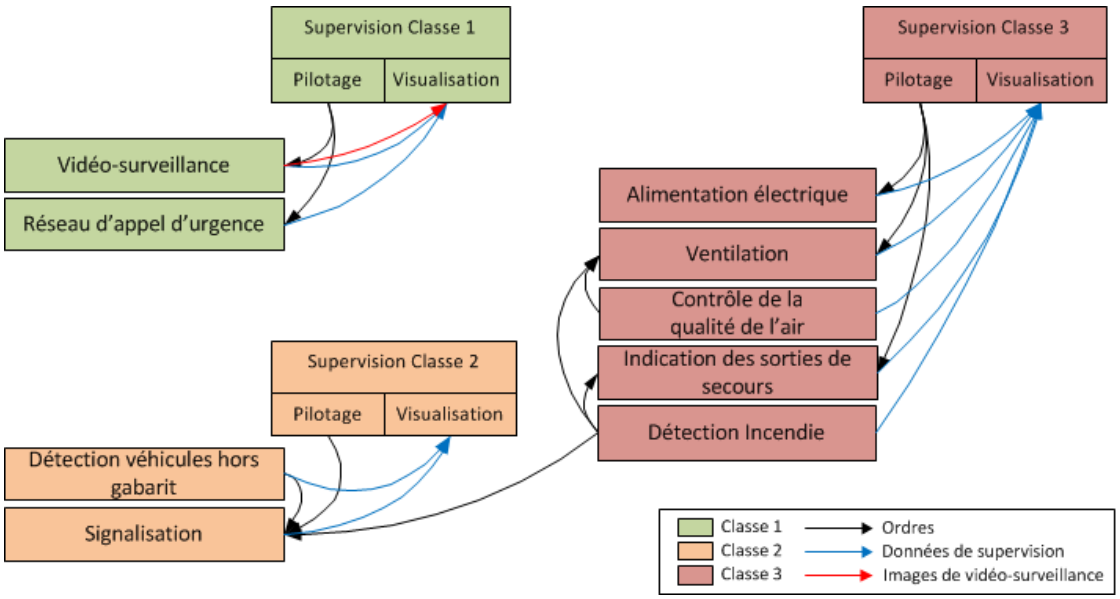

Figure 4.10 – *Système industriel - Graphe des dépendances fonctionnelles*

En pratique, il est possible de conserver un cloisonnement fort entre les différentes classes ou de réaliser certains regroupements, les préconisations à respecter étant

alors celles de la classe la plus élevée du regroupement. Dans le chapitre suivant, les différentes mesures principales [SCADA-MTD] seront déclinées suivant plusieurs configurations correspondant aux regroupements suivants :

1. toutes les fonctions sont regroupées au sein d'un même ensemble de classe C3 ;
2. les fonctions sont réparties en trois ensembles distincts suivant leur classe (C1, C2 et C3) ;
3. les fonctions de classe C1 et C2 sont regroupées, les fonctions de classe C3 formant un second ensemble ;
4. les fonctions de classe C2 et C3 sont regroupées, les fonctions de classe C1 formant un second ensemble.

Chapitre 5

Possibilités de regroupement des classes

Le chapitre précédant nous a permis de réaliser une première classification théorique des différentes fonctions, suivant les besoins en cybersécurité. Cette classification est résumée en section 4.5.

Il apparaît que des fonctions sont présentes dans chacune des trois classes. Partant de ce constat, Tunnello décide donc de regarder si une certaine rationalisation est envisageable en regroupant certaines classes sans pour autant baisser le niveau de cybersécurité. Pour se faire, Tunnello et son intégrateur passent en revue les différences essentielles qui existent dans la déclinaison des mesures principales pour chacun des regroupements envisagés.

A des fins didactiques, cette revue des regroupements envisageables est présenté séparément de la déclinaison des mesures principales (on se référera au chapitre idoine de la seconde partie de cette étude [SCADA-TNL-2]). Dans une analyse réelle, ces deux étapes sont réalisées de façon conjointe, au moins dans un premier temps : les avantages et inconvénients des différents regroupements se dégagent au fur et à mesure que sont affinées les mesures principales. Le présent chapitre se concentre exclusivement sur les points de divergences ayant une influence sur le choix d'un possible regroupement, on se reportera au chapitre idoine pour une déclinaison complète des mesures principales.

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. En d'autre termes, les classes plus basses s'alignent sur la classe la plus haute au sein du regroupement.

5.1 Les différentes configurations envisagées

Configuration	Commentaires
« C1, C2, C3 »	Ce regroupement correspond à une application directe de la classification issue du chapitre précédent. Les mesures sont ainsi appliquées en segmentant l'architecture par classe, pour n'appliquer que les mesures nécessaires à chaque classe. Ce cas est par la suite noté « C1, C2, C3 »
« Tout C3 »	A l'inverse du regroupement précédent, le système d'information est considéré dans sa globalité, sans prendre en compte la classification des fonctions. Les règles sont ainsi sur une architecture ne comportant pas de segmentation liée aux classes. Les règles applicables sont alors celles de la classe la plus élevée présente dans le système, soit la classe 3 dans le cas présent. Ce cas est par la suite noté « tout C3 »
« C1+C2, C3 »	Le but est de dérouler l'ensemble des règles sur une architecture intermédiaire, regroupant deux des trois classes. Elle regroupe donc C1 et C2 d'un coté, C3 de l'autre. Ce cas est par la suite noté « C1+C2, C3 »
« C1, C2+C3 »	Comme précédemment, le but est de dérouler l'ensemble des règles sur une autre architecture intermédiaire, regroupant deux des trois classes. Cette configuration regroupe ainsi C2 et C3 d'un coté et C1 de l'autre. Ce cas est par la suite noté « C1, C2+C3 »

Avant de procéder au choix de la meilleure configuration, il peut être utile, pour mieux comprendre le mode de fonctionnement du tunnel, de modéliser les flux entre les différentes classes sous la forme d'un schéma d'architecture logique simplifiée, décliné du graphe de dépendance des fonctions (cf. figure 4.10).

Les figures 5.1 à 5.4 correspondent à ces schémas d'architecture pour les quatre configurations envisagées.

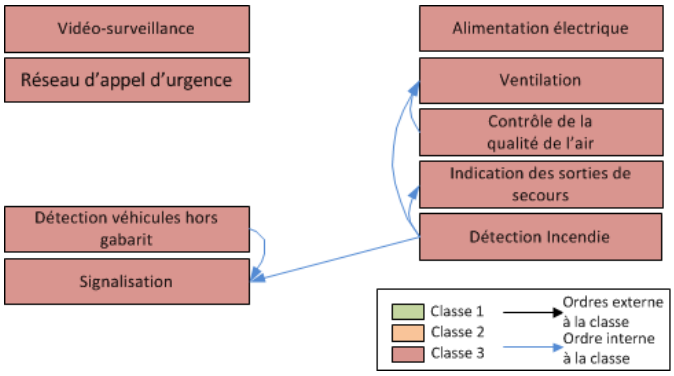

Figure 5.1 – *Schéma de flux - « tout C3 »*

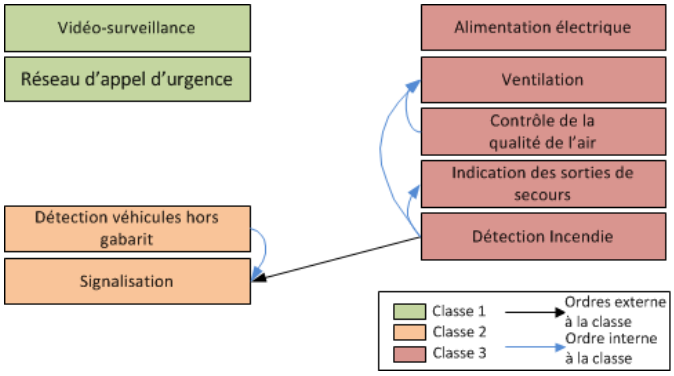

Figure 5.2 – *Schéma de flux - schéma réseaux « C1, C2, C3 »*

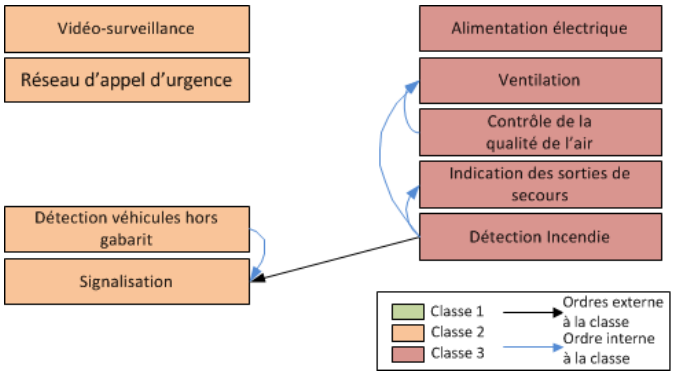

Figure 5.3 – *Schéma de flux - « C1+C2, C3 »*

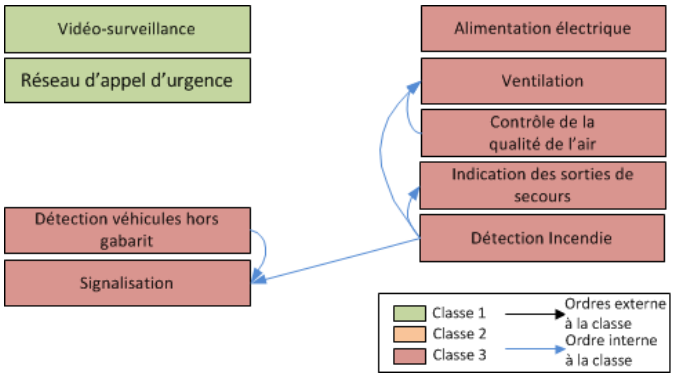

Figure 5.4 – *Schéma de flux - « C1, C2+C3 »*

5.2 Les principaux éléments différenciants

5.2.1 Formation, contrôle et habilitation des intervenants

Formation et habilitation :

Dans le cadre de ses processus RH, Tunnello s'assure que les exploitants disposent d'un niveau de formation adapté à leur poste, qui inclut un module de sensibilisation à la cybersécurité. Cette formation initiale est complétée, pour toutes les personnes concernées, par une habilitation réalisée en interne pour intervenir sur les équipements de classe 2 et réalisée par un organisme externe certifié lorsqu'elles concernent des équipements de classe 3.

Contrôle :

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 par classe. Ceux-ci sont utilisés autant que possible par les équipements de la classe correspondante pour la gestion des autorisations et journalisent les accès via les mécanismes de supervision.

De ce fait, un regroupement de certaines classes permet une mutualisation des annuaires correspondants et donc une simplification de l'ensemble de l'exploitation.

5.2.2 Audits

Des audits sont nécessaires pour les différentes classes, comme cela sera précisé lors de la déclinaison des différentes mesures. On peut toutefois noter que ces derniers sont d'autant plus importants que la classe concernée est élevée.

De plus, un audit interne réalisé par une équipe dédiée à ce type d'activité peut s'avérer suffisant pour les infrastructures de classe 1, alors que l'appel à un prestataire labellisé est obligatoire pour les infrastructures de classe 3.

Maintenir la séparation lorsque cela est possible permet donc de fait de limiter les impacts financiers et sur l'exploitation, puisque les contraintes de la classe 3 ne sont pas répercutées sur les classes inférieures.

5.2.3 Processus de veille

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 de l'action à mener (acceptation et documentation du risque, mise à jour de l'équipement, mise en place de moyens palliatifs, etc.).

Les contraintes, notamment en terme de délais, pour la réalisation de cette évaluation et, le cas échéant, l'application des correctifs, sont liés à la classe des équipements. Ce processus aura donc un impact d'autant plus important que les classes « hautes » regrouperont un nombre important d'équipements.

5.2.4 Interconnexions réseau

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

De même, pour chacune des classes, les communications entre ces deux ensembles sont réalisées au travers d'une paire de passerelles VPN IPsec qualifiées dédiées à la classe considérée.

Le regroupement de certaines classes aurait pour effet une réduction de ces équipements de sécurité au niveau réseau.

5.2.5 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.

Ce mécanisme repose notamment sur des communications entre le PCC et le site du tunnel, communications qui sont réalisées au travers d'un tunnel chiffré et authentifié sur une liaison spécialisée (segmentation par MPLS), comme indiqué plus haut dans ce chapitre (cf 5.2.4).

Par ailleurs, comme cela sera détaillé dans les chapitres consacrés à la déclinaison des différentes mesures, il n'existe pas de réseau d'administration à proprement parlé. Ceci impose de fait l'utilisation d'un poste nomade par classe pour la maintenance des équipements industriels.

Là encore, une réduction du nombre d'infrastructures par le regroupement de certaines classes permettrait de réduire le nombre de liaisons MPLS nécessaires et de postes nomades dédiés à la maintenance.

5.2.6 Surveillance et moyens de détection

De par l'architecture mise en œuvre, Intégro prévoit un serveur de journalisation par classe, au moins pour les équipements permettant une remontée automatique. Ceux-ci génèrent un rapport de synthèse à destination du service d'exploitation, sur une base quotidienne pour la classe 3, bihebdomadaire pour la classe 2 et hebdomadaire pour la classe 1.

Les anomalies et alarmes remontées sont par ailleurs prises en compte suivant des modalités prévues dans le cadre de la gestion des incidents, détaillées plus loin dans la section idoine. Cette gestion est, entre autre, pilotée par la classe des équipements concernés.

Concernant la journalisation, on constate qu'une réduction du nombre de classes simplifie l'exploitation en uniformisant les procédures correspondantes. Dans le même temps, ne pas regrouper des équipements dans une classe haute lorsque cela n'est pas nécessaire évite de lui appliquer des procédures inutilement contraignantes.

5.2.7 Gestion des interventions

Principes généraux

Il est considéré comme acquis que toute intervention engendre la création d'un ticket dans le gestionnaire idoine quels que soient l'équipement concerné et l'intervention. Tunnello considère donc que ce gestionnaire de tickets fait office de carnet de consignation.

Accès aux locaux

Du fait de la présence d'équipements de classe 3, Tunnello a prévu 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, 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.

L'obligation d'appeler le poste de contrôle principal pour lever l'alarme est considérée par Tunnello comme un mécanisme de traçabilité suffisant pour les coffrets contenant des équipements de classe 2 ou concernant la vidéo-surveillance (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.

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.

Cette rapide analyse montre qu'en ne regroupant pas des équipements dans une classe haute lorsque cela n'est pas nécessaire, Tunnello évite de lui appliquer des procédures inutilement contraignantes, comme par exemple la nécessaire présence d'un salarié Tunnello pour réaliser ou accompagner une opération de maintenance simple.

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, avec toutefois une tolérance pour les outils dont l'usage reste exceptionnel dans le cas des équipements de classe 2.

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.

Comme pour le point précédent, un regroupement inutile des équipements dans une classe haute pourrait avoir un impact financier important.

5.3 Choix de la configuration

L'analyse des éléments différenciants ci-dessus montrent que si regrouper des classes pour rationnaliser les infrastructures peut présenter quelques avantages tant dans la conception que dans l'exploitation de l'ensemble, cela présente également des inconvénients.

Ainsi, le réflexe classique qui consisterait à rassembler l'ensemble des équipements dans une unique infrastructure de classe 3 permet effectifement de limiter le nombre d'équipements mais impose des contraintes importantes au niveau de l'exploitation des éléments les moins sensibles : l'obligation de dédier au site un ensemble complet des outils de maintenance et de diagnostique pour le réseau d'appel d'urgence ou le suivi renforcé des alertes pour cette fonction peuvent sembler sur-dimensionnés. De ce fait, Tunnello ne retient pas la configuration « tout C3 ».

Pour des raisons similaires, Tunnello émet une préférence pour la configuration « C1, C2+C3 » à la configuration « C1+C2, C3 », car il lui parait un peu plus simple de factoriser les procédures dans le premier cas que dans le second.

L'analyse des figures 5.1 à 5.4 montre par ailleurs que les configurations « tout C3 » et « C1, C2+C3 » semblent, du point de vue des schémas de flux, plus simples que les deux autres du fait de l'indépendance des différents regroupements.

À l'inverse, les configurations « C1+C2, C3 » et « C1, C2, C3 » font apparaître un lien entre les deux réseaux de terrain C3 et C2 dans un sens. En effet, à partir de données collectées sur les capteurs du réseau de terrain C3 (notamment Détection incendie et Contrôle de la qualité de l'air), certaines informations doivent être envoyées aux actionneurs du réseau de terrain C2 (signalisation).

Ces éléments viennent donc conforter le fait d'écarter la configuration « C1+C2, C3 » au profit de la configuration « C1, C2+C3 ».

Enfin, la configuration « C1, C2, C3 », qui présente une infrastructure différente par classe évite effectivement des contraintes inutiles mais présente une architecture plus couteuse et plus complexe à maintenir en raison des deux réseaux de terrain.

Dans le cas particulier du tunnel, la séparation de C1 d'un coté et C2+C3 de l'autre permet de limiter les contraintes sur les équipements de classe 2 tout en réduisant la complexité technique et organisationnelle. Les contraintes supplémentaires appliquées aux équipements de classe 2 sont relativement limitées du fait de la nature des fonctions de classe 2 et de la possibilité de mutualiser les fonctions de sécurité avec les équipements de classe 3.

Tunnello décide donc de mettre en œuvre la configuration « C1, C2+C3 ».

Bibliographie

[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`.

[CETU-EVAC] *Signalisation et dispositions d'accompagnement de l'auto-évacuation des usagers dans les tunnels routiers*.
Guide Version 1.0, CETU - Centre d'études des tunnels, septembre 2010.
`http://www.cetu.developpement-durable.gouv.fr/IMG/pdf/CETU_Doc_info_AEV_2010-10-15_cle0765fa_cle57299f.pdf`.

[CETU-VENT] *Les dossiers pilotes - ventilation*.
Guide Version 1.0, CETU - Centre d'études des tunnels, novembre 2003.
`http://www.cetu.developpement-durable.gouv.fr/IMG/pdf/DP_ventilation_cle557d66-3.pdf`.

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