

Practical Case of a Road Tunnel

Part 1: Classification

Cybersecurity for Industrial Control Systems



Warning

This document is a case study aimed at illustrating the two guides [ANS14a, ANS14b] published by ANSSI in January 2014. In particular, it is not a document of best practices or recommendations for the industrial control systems of road tunnels.

Although the authors have endeavoured to make this study as realistic as possible, certain liberties were taken for pedagogical purposes with respect to systems actually encountered in road tunnels.

Executive Summary

In 2014, the working group on Industrial Control System cybersecurity (GTCSI), led by the French Network and Information Security Agency (ANSSI), published two guides:

- Cybersecurity for Industrial Control Systems - Classification Method and Key Measures [ANS14a]
- Cybersecurity for Industrial Control Systems - Detailed Measures [ANS14b]

The objective of this case study is to illustrate these two guides with a complete and concrete example: a road tunnel.

The first part of this study [ANS16q] provides details on the complete method of classification, as such showing how to take certain elements into account.

After a presentation of the scope and the context of the case study, the various threats are analysed by specifying the possible links between cybersecurity and dependability¹. From these threats then stem the likelihood of an attack and therefore the class of each function. Finally, the various possible groupings between classes are compared in order to define the final architecture.

The second part of the case study [ANS16b] corresponds to the implementation of measures present in the two guides.

The architecture retained at the end of the first part is thus analysed macroscopically, with regard to the main measures of the first guide. A proposal for securing the tunnel is then made using the second guide, by starting with the organisational measures followed by the technical measures.

Finally, remember that an analysis that uses this method is only an initial approach that makes it possible to assert certain choices of architecture and measures to be applied. This in no way removes the need for a comprehensive risk analysis, which is moreover one of the measures identified. Likewise, other measures can be retained in an entirely valid manner if they make it possible to respond to the need for cybersecurity.

¹See the classification method glossary for the definition of these two notions.

Table of contents

1	Introduction	7
2	Context	9
2.1	Presentation of the company	9
2.2	Physical organisation of the tunnel	10
2.3	Functions implemented in the tunnel	10
2.4	Functional dependencies	13
2.5	Initial approach before the conducting of the study	14
3	Threat scenarios	19
3.1	Dependability and feared events	20
3.2	Study of threat scenarios	21
3.2.1	Feared events	21
3.2.2	Threat scenarios	26
3.2.3	Vulnerabilities	28
3.3	Examples of attack scenarios	31
3.3.1	Case of a targeted attack: installation of malware	31
3.3.2	Case of a non-targeted attack: spread of a virus	31
3.3.3	Case of an indirect targeted attack: trapped devices	32
3.4	Security analysis pertaining to the initial approach architecture before conducting the method	32
4	Classification	35
4.1	Scales	36
4.2	Hypotheses of the study	37
4.3	Classification by function	38
4.4	Functional dependencies and classes	44

4.5 Final classification	45
5 Possibilities of regrouping classes	47
5.1 The various configurations considered	48
5.2 The main differentiating elements	50
5.2.1 User Training, Control and Certification	50
5.2.2 Audits	50
5.2.3 Monitoring process	51
5.2.4 Network Segmentation and Segregation	51
5.2.5 Remote Diagnosis, Remote Maintenance and Remote Management	51
5.2.6 Surveillance and Intrusion Detection Methods	52
5.2.7 Intervention Management	52
5.3 Choice of the configuration	53
Bibliography	55

Chapter 1

Introduction

This document is based on the findings of the working group on Industrial Control System cybersecurity, directed by the French Network and Information Security Agency (ANSSI). Composed of actors in the field of automated industrial process control systems and specialists in IT Security, the group has undertaken to draft a set of measures to improve the cybersecurity of industrial control systems (ICS). The initial work carried out has allowed for the publication in January 2014 of two guides [ANS14a, ANS14b] that aim to propose a classification method for ICSs and a set of measures in order to provide an adequate security level according to the criticality of these systems.

The purpose of this document is to illustrate the classification method described in the guide [ANS14a], by applying it to the scope of securing a road tunnel. This is the first part of this case study, which contains two parts.

In accordance with the objective put forth by the working group, this analysis exclusively concerns the aspects of cybersecurity, and certain links that can be made with dependability, but the latter is assumed to be covered elsewhere.

In detail, chapter 2 presents the hypotheses of the case study with a description of the project and the various economic stakeholders involved.

Chapter 3 lists in an in-depth manner the various threats which weigh on ICSs in this type of context and the links that can be made between the risk analyses conducted in terms of dependability and cybersecurity.

Chapter 4 describes the comprehensive reasoning leading to the classification of the functions. The method is based on scales defined by the operator and on the results of the risk analysis of dependability. The relationships between the various functions supported by the ICSs of the tunnel are also analysed in detail.

Chapter 5 describes the groupings that can be considered between classes in order to facilitate the implementation and the operation of the information system concerned. Indeed, the classification method described in the guide [ANS14a] leaves the freedom to group the functions into subsystems as long as certain principles are complied with.

Chapter 2

Context

The case study concerns the securing of the industrial information system of a fictitious road tunnel located under Mont Aigoual, on the road linking Meyrueis with Notre Dame de la Rouvière. This is a new structure in which latest-generation devices can be deployed according to need. There is therefore no management of what exists or migration plan to be considered.



Figure 2.1: Tunnel - location map

2.1 Presentation of the company

The road tunnel will be operated by the (fictitious) company Tunnello. The director of this company is Mrs Alice and her operations manager is Mr Bob.

In order to successfully carry out these various tasks, Tunnello has called upon the services of several providers¹, which are also fictitious, for certain tasks that it cannot carry out itself:

¹The names of these companies are chosen in such a way as to simplify the understanding of their role in the rest of the document. Any resemblance with one or more existing companies would be purely coincidental.

- Integro provides the supply, integration and then maintenance of the ICS;
- Audit is responsible for the various IT audits required;
- Formatio is responsible for training the personnel;
- Telco is the telecommunications operator responsible for network access (Internet access and dedicated connections);
- Constructio is the company responsible for digging the tunnel.

Note that some of the measures outlined in this document affect the choice of the various service providers (requirements in terms of labelling for example).

Although the name of the service providers are indicated in the preamble in order to facilitate the reading of the document, the requirements are assumed to have been taken into account when choosing the service provider for each scenario.

2.2 Physical organisation of the tunnel

The tunnel, the subject of the study, is a road tunnel of the single-tube bidirectional type with a length of about 2,550 m. From a regulatory standpoint, it falls within the category of low-traffic tunnels with a length between 1,500 m and 3,000 m.

Normally, this tunnel is supervised from a remote main control center (PCC - poste de contrôle-commande), located in Millau and under the responsibility of Tunnello. It also has a secondary control center, on the site, primarily used as a backup and located on the Meyrueis side. If traffic flow is interrupted in the tunnel, from the Millau PCC, 1h30 is required to reach the entrance of the tunnel on the Notre-Dame-de-la-Rouvière side and 2h on the Meyrueis side.

Within the tunnel, technical rooms (also called recesses) are installed about every 200 m. All of the accesses required for the various field networks (IT, electricity, fluids) can be arranged therein according to need. Here, there are also tapping points for the various fluids, electrical power supplies or switches for the IT networks present.

2.3 Functions implemented in the tunnel

To begin this study, an inventory needs to be taken of the various functions in place within the scope of the ICS for assistance in operating the tunnel.

The dependability study, conducted upstream, has made it possible to identify that this type of tunnel must, in order to ensure a satisfactory level of safety, implement the following main functions:

- electrical power supply and distribution;
- indication of emergency exits²;
- ventilation³;
- signalling;
- detection of oversize vehicles;
- video surveillance;
- fire detection;
- emergency call network;
- air quality control.

To this list is added the industrial supervision system which, although indispensable, is not treated as an independent function in this study. It brings together two subfunctions:

- acquisition and processing of data from multiple sources⁴;
- control of devices by sending controls and settings remotely.

These two subfunctions are respectively referred to as **visualisation** and **operation** when a distinction is necessary in the rest of the document.

²This function in particular covers systems of the TOTEM type as well as dynamic chevrons such as defined in the CETU document on the self-evacuation of drivers [CET10]. It does not include the regulatory lighted signs for which the power supply is permanent.

³Tunnello retained for ventilation and smoke extraction a transversal strategy, in accordance with tunnel category [CET03]. It decided in addition to use a concentrated extraction.

⁴In particular remote measurements, remote signalling or remote alarms.

Components by function

From a technical standpoint, each function can involve a more or less substantial number of components. Without taking the pooling into account that is possible with certain devices (including PLCs and HMI consoles⁵), the list of functions and associated components is summarised in the following table.

Functions	Components
Indication of emergency exits	PLC Circuit breakers and switches Condition sensors
Ventilation	PLC Fan motors ⁶ Rotation speed sensors Wind speed sensors Remote-controlled extraction dampers Outside weather station for managing counter-pressures
Signalling	PLC Lane assignment lighted signs Lighted diversion sign for oversize vehicles Variable message signs Motorised access barriers Condition sensors
Emergency call	Telephone posts Communication management system Recording devices
Detection of oversize vehicles	PLC Oversize sensors
Video surveillance	Video surveillance management system Cameras Recording devices
Fire detection	Fire detection unit (dedicated PLC) Smoke detector FibroLaser
Air quality control	PLC Opacimeters Nitrogen and carbon monoxide detectors

⁵Programmable Logic Controllers (PLCs) ensure the automated control portion of the industrial system. See appendix A.3 of the second part of the study for more details.

Functions	Components
Electrical power supply and distribution	PLC Circuit breakers and switches Measuring unit Condition sensors
Supervision	Servers of the supervision system Supervision workstation Video surveillance console

2.4 Functional dependencies

By searching for the relationships between the functions, but without taking the physical architecture into account, it is possible to indicate the following dependencies:

Functions	Dependencies
Indication of emergency exits	Commands issued by fire detection Data roll up to supervision
Ventilation	Commands issued by supervision Commands issued by Fire detection
Signalling	Commands issued by supervision Commands issued by Fire detection Commands issued by Oversize vehicle detection Data roll up to supervision
Emergency call	Communications roll up to the telephone operator Data roll up to supervision
Detection of oversize vehicles	Data roll up to supervision Commands sent to signalling
Video surveillance	Commands issued by supervision Remote measurement data roll up to supervision Image roll up to supervision
Fire detection	Data roll up to supervision Commands sent to indication of emergency exits, Ventilation, Signalling.
Air quality control	Data roll up to supervision Commands sent to ventilation

⁶The control loop between the motor and its speed sensors is generally carried out by a variable speed drive which in practice is the contact of the PLC for commands as well as for data roll up. The function also uses wind speed sensors to measure the actual effectiveness of the ventilation.

Functions	Dependencies
Electrical power supply and distribution	Commands issued by supervision Data roll up to supervision
Supervision	Manual operation commands issued to all of the functions Data roll up from all of the functions Roll up of video surveillance images

The relations between the functions can be summarised as those in figure 2.2. The latter shows the two subfunctions of the *supervision*, namely the *operation* and the *visualisation* solely for the purposes of legibility of the diagram. This does not make any assumption whatsoever as to the segmentation of these two subfunctions by the use of separate devices.

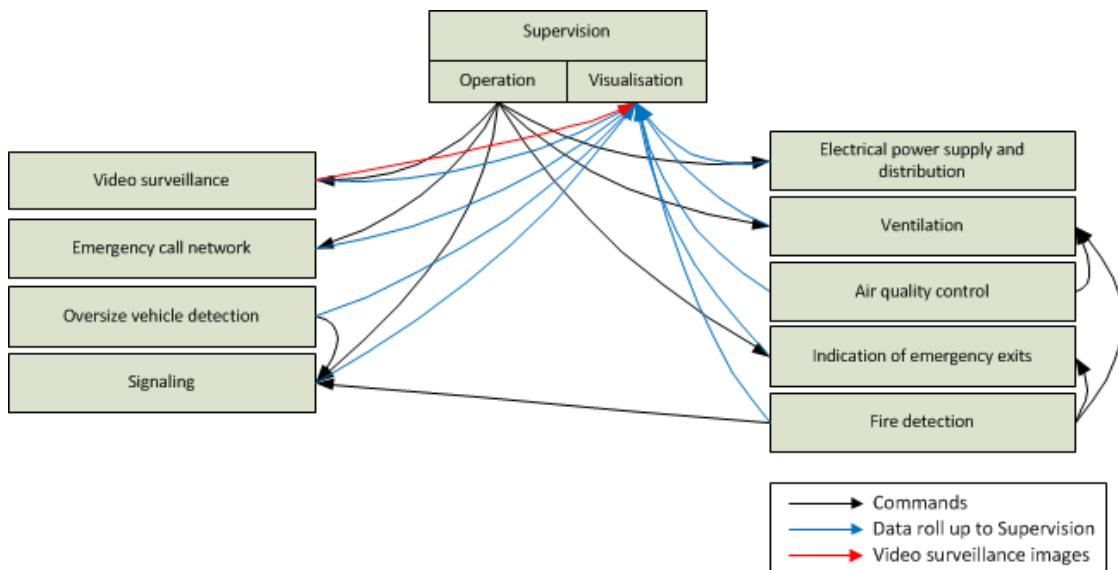


Figure 2.2: ICS - Graph of functional dependencies

2.5 Initial approach before the conducting of the study

Beyond the functions listed in the preceding paragraph, figure 2.3 shows the various logical components (application modules) that intervene according to the geographical locations (zones): the PCCs, the tunnel and the various networks that connect them together.

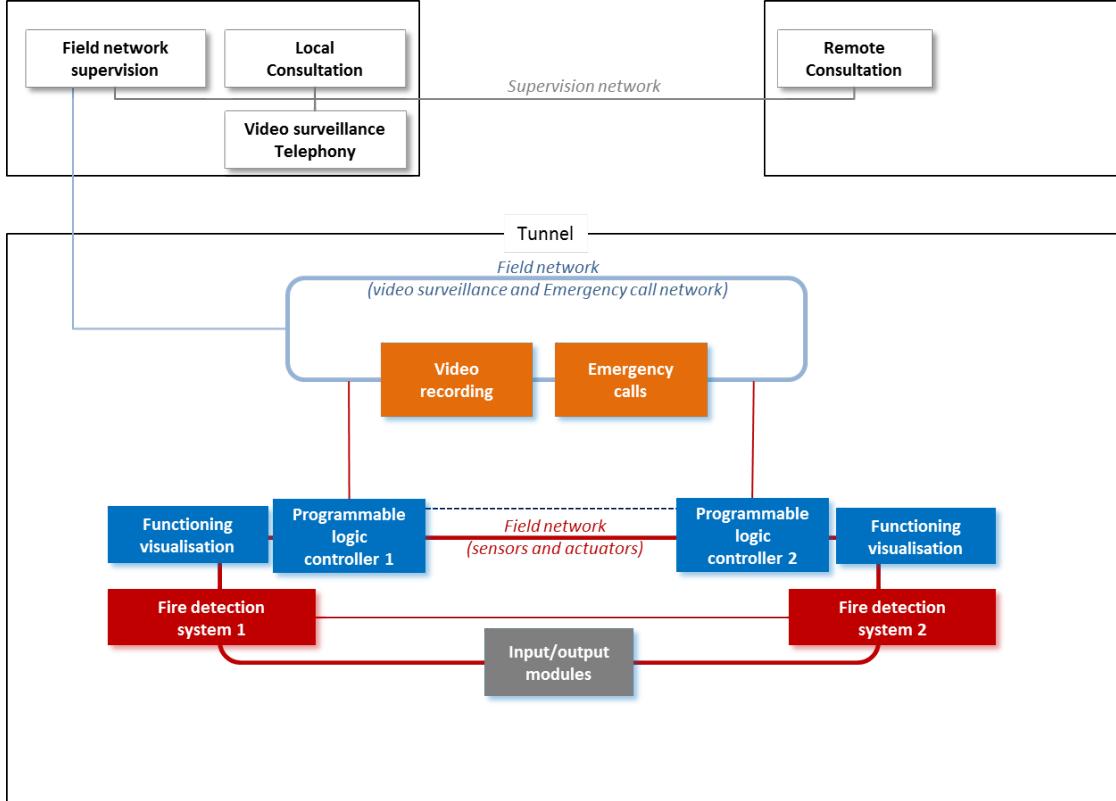


Figure 2.3: ICS - Initial logical approach before classification and securing method

The architecture presented in figure 2.4 stems from the analysis of dependability, before taking cybersecurity into account. It thus presents the perimeter of the ICS as it would be deployed without taking cybersecurity into account. It emphasises:

- the components and their geographical location;
- the connections between these components.

It has all of the components present at the level of the PCCs:

- the redundant servers of the industrial supervision system in order to ensure application availability;
- the consoles for the supervision network;
- the telephone server (IPBX) for the communications made from the posts in the tunnel.

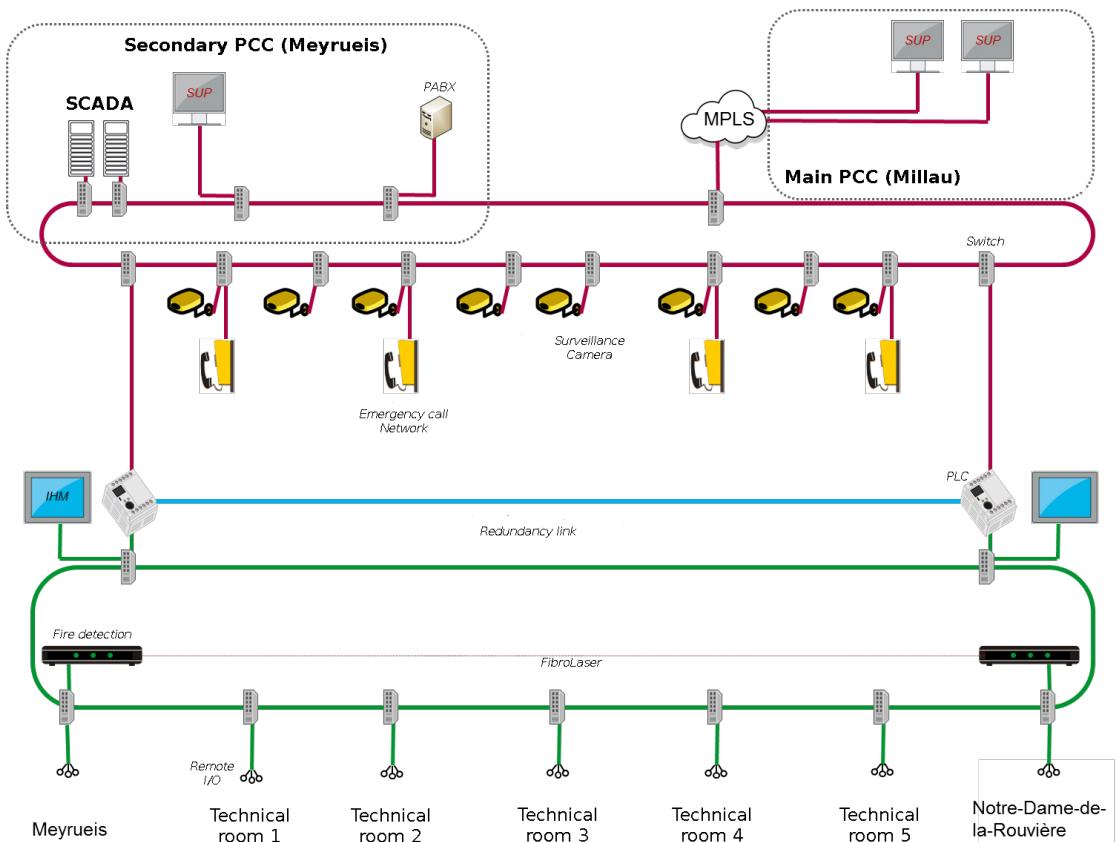


Figure 2.4: ICS - Initial technical approach before classification and securing method

In the event of a hardware failure, redundancy and availability of components and networks ensure the proper operation of the safety functions. Note however that although there is indeed redundancy for the supervision servers, the latter is limited to the secondary PCC, without any offset to the main PCC: in case of a loss of the secondary site, the supervision functions may then not be able to be ensured by the operating team present at Millau. However, although this can give rise to problems in monitoring incidents, it does not call the safety of people and assets into question (in terms of safety) in the tunnel as the PLCs can continue to operate without their supervision.

Figure 2.4 in particular shows a **workstation (supervision console)** connected to a supervision server. In this initial technical approach, this workstation is a fixed station present in the PCC. From this workstation, the following functions are provided:

- **supervision:** this entails allowing the operator to monitor the activity of the tunnel and where applicable to operate certain devices for example set values;

- **administration and maintenance of the supervision solution:** this is the installation, setting and configuration of the software required to supervise the tunnel;
- **administration and maintenance of the industrial devices:** this entails the software and hardware installation, updating the components present in the tunnel and the IT support by the integrator.

The supervision function is provided by Tunnello which operates the tunnel. In the rest of this study, the terms **functional administrator**, **operator** and also, through misuse of language, user of the solution, correspond to those of whom the role is to ensure this supervision function.

The functions of maintenance and administration, on the supervision solution as on the devices present in the tunnel, are provided by the Integro company that integrates and maintains the technical solution, by using its own stations or not. In the rest of this study, the terms **IT administrator** and **integrator**, correspond to those of whom the role is to provide these administration functions.

In this study, the term **user** corresponds either to an operator or to an integrator, or more generally to any people with a valid access to the information system or working for Tunnello ; the term **driver** corresponds to anyone passing through the tunnel.

In order to allow for maintenance actions in the field (i.e. in the tunnel), a mobile workstation is provided. This **maintenance laptop** makes it possible to connect to the tunnel's devices in order to perform operations that would not be or that would no longer be possible from the fixed station of the PCC.

In this initial approach, this maintenance laptop can therefore be used potentially both by the personnel of Tunnello (the operators) and by the personnel of Integro (the integrators). As it is not linked to a group of users but to a location, this maintenance laptop can also be used for other actions, as soon as it is necessary to have extended rights on a device.

Chapter 3

Threat scenarios

Although this analysis is not a genuine risk analysis, an overview of the threat remains a pre-requisite for any study for setting up protective measures, in order to ensure the appropriateness of the latter.

In order to carry out this overview, it should be reminded that this analysis is not carried out in an isolated manner. A security dossier was indeed compiled for the opening of the tunnel for operation, a dossier for which a dependability study was conducted¹. Although the latter is not enough to directly lead the work of reinforcing cybersecurity, it does form a base to start from that must not be underestimated.

It is reminded that the missions of the tunnel are:

- to allow for the transmit of vehicles from the entrance to the exit of the tunnel;
- to ensure the safety of the drivers and of the personnel during nominal operation;
- to ensure the safety of the drivers and of the personnel in case of fire or the presence of gas.

Likewise, the following definitions will be recalled in order to prevent any misunderstanding²:

Cybersecurity, or security of information systems, addresses protection in terms of availability, integrity or confidentiality of the data stored, processed or transmitted.

Dependability strives to ensure that the ICS is able to accomplish the functions in the defined conditions. In particular, dependability addresses the properties of Reliability, Availability, Maintainability and Safety (RAMS). In this context, dependability concerns people and assets.

¹The two studies can also be conducted simultaneously according to the maturity of the users.

²See the classification method glossary [ANS14a] for the full definitions of these two notions such as retained for this case study.

3.1 Dependability and feared events

In the framework of a dependability study, Tunnello has in particular conducted several analyses, including:

- a functional analysis and modelling;
- a preliminary analysis of the risks or hazards (PRA / PHA);
- a failure modes, effects and criticality analysis (FMECA);
- a fault tree analysis (FTA).

These various analyses, and more particularly the fault tree analysis and system FMECA (or functional FMECA), have revealed the functional failure modes: untimely function, absence of function, erroneous function, non-stopping of the function, etc. They have as such made it possible to identify and to characterise the criticality of feared events linked to the failures of the functions of the system.

Some of these feared events, whether voluntary or involuntary, can have as an origin a malfunction at the IT level, they can be included as input for the security analysis of the ICS in the form of feared events.

Safety of drivers in case of fire

As an example, this section includes the elements concerning the safety of drivers in case of fire from a dependability standpoint: the effects of the failure modes on the system are evaluated here, along with their main impacts for drivers.

- Interruption in the monitoring of fire safety
 - If there is no information, drivers continue to move towards the fire and, when they see it, it is difficult for them to move to the emergency exits. This potentially results in a substantial number of injuries or death, through burns or intoxication, among the drivers present.
 - If emergency teams are not alerted in an optimal manner, their late arrival can be an aggravating factor.
- Degradation in the monitoring of fire safety
 - In case of a late detection of the fire, the impacts are the same as in the case of non-detection, but the number of drivers concerned can be comparatively lower since the information reached the drivers in the end.

- The incorrect location of the fire can trigger local inappropriate ventilation. Because of this, the draft created fans the fire instead of containing it. In addition, smoke accumulates in excessive quantities in certain locations and slows down the evacuation and the intervention of the emergency teams.
- Processing “fire” information in the absence of a fire
 - The untimely triggering of a fire alert can needlessly mobilise resources and personnel.
 - The unavailability of the tunnel will extend beyond the lifting of the doubt, in order to take into account the potentially uncontrolled reactions of the drivers as well as the return of those that had left their vehicles.

3.2 Study of threat scenarios

The elements described in the preceding section, as well as those from the equivalent work on the other groups of feared events (presence of gas for example) make it possible to initiate the overview of potential threats on the industrial system, with the lists of feared events and vulnerabilities as well as impacts. These lists are then supplemented with thought that focuses more on the specificities of cybersecurity.

3.2.1 Feared events

As indicated in the introduction to this chapter, it is possible to produce a list of feared events from the analysis of dependability, supplemented by thought given to cybersecurity. In the framework of the case study, the feared events that were retained for a more precise study in the rest of this section are as follows:

- alteration of metrology data (supervision);
- modification of control commands (supervision);
- modification of PLC data;
- alteration of history data;
- injection of field data.

The next five subsections list the various scenarios that can lead to each one of these feared events as well as the impacts that can generate these events.

These scenarios will then be described in section 3.2.2.

Alteration of metrology data

In the case of this feared event, the values displayed by the supervision are modified by the attacker and therefore no longer necessarily reflect reality. By extension, this category includes the altering of video surveillance images.

The threat scenarios can lead to this feared event

Location	Threat scenarios
At the PCC level	Unauthorised access to the workstation. Compromising of the workstation. Unauthorised access to the supervision server. Compromising of the supervision server. Unauthorised access to the PCC network.
At the tunnel level	Unauthorised access to PLCs. Unauthorised access to the field networks. Compromising of PLCs. Compromising of HMI consoles ³ . Compromising of sensors / actuators.

Impacts

The result of jeopardized metrology data is a potentially false view of reality, whether at the operator or at the PLC level.

This can then develop into an absence of an appropriate reaction, such as the absence of triggering of smoke extraction in case of fire, or, on the contrary, inappropriate decisions such as the untimely triggering of alarms. The operator can then think that an automatic reaction has indeed occurred when this is not the case at all. More generally, the event can be seen as a loss of remote control of the tunnel by the operators all the more serious given that this can go unnoticed.

The event can also trigger an alteration in the logging of the state of the system or a broadcasting of false videos intended for the supervision screens that are masking malicious actions.

Modification to control commands

³The human-machine interfaces that make it possible to ensure interaction in the field between the operators and the PLCs. See appendix A.5 of the second part of the study [ANS16b] for more details.

Concerning this feared event, the commands received by the devices in the ICS have been altered by an attacker. They therefore no longer necessarily correspond to the instructions given by the operators.

The threat scenarios can lead to this feared event

Location	Threat scenarios
At the PCC level	Unauthorised access to the workstation. Compromising of the workstation. Unauthorised access to the supervision server. Compromising of the supervision server. Unauthorised access to the PCC network.
At the tunnel level	Unauthorised access to PLCs. Compromising of PLCs. Unauthorised access to HMI consoles. Compromising of HMI consoles. Unauthorised access to the field networks. Unauthorised access to sensors/actuators. Compromising of sensors / actuators.

Impacts

The impacts of a modification to the operating settings are very significant.

The supervision servers can be in an unstable state, with untimely shutdowns and restarts, which no longer allow the operator to ensure his functions of operating the activity of the tunnel reliably.

This event is moreover an aggravating factor when it occurs at the same time as a compromising of metrology data. Indeed, the operator can no longer trust the information that he receives or the commands that he issues (switch to a secure holding position for example). The absence of any control by supervision can seriously disturb the operation of the installations.

Modification of PLC data

This entails considering the case of a modification of the data stored within the PLC by the attacker. This can be client applications, programs and the configuration or firmware of the PLCs.

The threat scenarios can lead to this feared event

Location	Threat scenarios
At the PCC level	Not applicable.
At the tunnel level	Unauthorised access to PLCs. Compromising of PLCs. Unauthorised access to the maintenance station. Compromising of the maintenance station. Use of the maintenance station as a connection bridge. Loss or theft of the maintenance station.

Impacts

Due to their criticality, the modification of data stored in the PLC is the feared event for which the impacts are the most substantial.

It is indeed no longer possible to trust the proper operation of the PLC, in particular in terms of the coherency of the decisions that it can take as a reaction to the information that it receives or in its ability to maintain the installations in a stable and predictable state.

In addition, it is possible for the attacker to set up pre-programmed actions, that can be triggered without any link to the actual situation or by hiding them from the supervision by the operators.

The altering of PLC data can also render the installations entirely inoperable or uncontrollable.

Finally, it is common for the programs inside PLCs to contain permissible limits in the values sent to the actuators in order to guarantee correct operation. Altering these limitations can result in actions outside the safety zones (example of a motor rotating substantially faster than what its fastenings can handle, which can result in the destruction of the ventilation installations).

Alteration of history data

Here, the attacker succeeds in erasing or in altering the data history. This can be an activity log, dashboards or alerts.

The threat scenarios can lead to this feared event

Location	Threat scenarios
At the PCC level	Unauthorised access to the supervision server. Compromising of the supervision server.

Location	Threat scenarios
At the tunnel level	Unauthorised access to PLCs. Compromising of PLCs.

Impacts

The main consequence of an alteration of data history is to potentially no longer be able to respond to the obligations of traceability.

Although the missions of the tunnel are not directly at risk, this absence of history jeopardises the trust that can be granted to all of the various elements of the ICS. It is then difficult to detect the precursor elements of the feared events hereinabove, and any investigation is rendered impossible.

Injection of field data

The attacker succeeds in spreading arbitrary information within the ICS. This can be false roll ups of values that are assumed to come from sensors, or false commands intended for actuators.

The threat scenarios can lead to this feared event

Location	Threat scenarios
At the PCC level	Unauthorised access to the supervision server. Compromising of the supervision server. Unauthorised access to the PCC network.
At the tunnel level	Unauthorised access to the field networks. Unauthorised access to PLCs. Compromising of PLCs. Compromising of HMI consoles. Unauthorised access to sensors / actuators. Compromising of sensors / actuators. Unauthorised access to the maintenance station. Compromising of the maintenance station. Use of the maintenance station as a connection bridge. Loss or theft of the maintenance station.

Impacts

The impacts of this feared event are relatively close to the first two, namely the altering of metrology data and that of operating settings.

3.2.2 Threat scenarios

The following table lists the possible threat scenarios in the PCC. The detail of the vulnerabilities will be specified in section 3.2.3.

Threat scenarios	Vulnerability
Unauthorised access to the workstation	No systematic locking of the session. No protection of identifiers and passwords. Weak passwords. Weak configuration. Vulnerability of the operating system.
Compromising of the workstation	Absence of verification of the innocuousness of the removable media. Internet browsing and email ⁴ Inappropriate use of the workstation. Compromised application of an update.
Unauthorised access to the supervision server	No systematic locking of the session. No protection of identifiers and passwords. Weak passwords. Weak configuration. Access from a compromised workstation. Vulnerability of the operating system. Sending of forged frames.
Compromising of the supervision server	Compromised application of an update. Absence of verification of the innocuousness of the removable media. Direct access to Internet.
Unauthorised access to the PCC network	Vulnerability of the network devices. Weakness of MPLS partitioning. Physical access to network devices.

The following table lists the possible threat scenarios in the tunnel. The detail of the vulnerabilities will be specified in section 3.2.3.

Threat scenarios	Vulnerability
Unauthorised access to the field networks	Physical access to network devices. Physical access to network wiring. Vulnerability of the network devices.

⁴When these functions are strictly required on the workstation, for operational purpose. In the opposite case, they are included in the inappropriate uses of the station.

Threat scenarios	Vulnerability
Unauthorised access to PLCs	Use of a default account. No systematic locking of the session. No protection of identifiers and passwords. Weak passwords. Weak configuration. Vulnerability of the PLCs. Sending of forged frames. Access from a compromised station.
Compromising of PLCs	Update distributed by the manufacturer or the integrator and comprising errors. Compromised update distributed by an attacker impersonating the integrator. Compromised update distributed by an attacker gaining access to the network. Compromised update distributed following the compromising of the maintenance station
Unauthorised access to HMI consoles	Use of a default account. No systematic locking of the session. No protection of identifiers and passwords. Weak passwords ⁵ . Vulnerability of the program of the HMI consoles. Sending of forged frames.
Compromising of HMI consoles	Update distributed by the manufacturer or the integrator and comprising errors. Compromised update distributed by an attacker impersonating the integrator. Compromised update distributed by an attacker gaining access to the network. Compromised update distributed following the compromising of the maintenance station
Unauthorised access to sensors/actuators	No protection of identifiers and passwords ⁶ . Vulnerability of the PLCs. Sending of forged frames. Physical access.

⁵Password complexity must be adapted to the sensitivity of the industrial system, while taking into account the environment and usability of this type of console.

⁶When these identifiers and passwords exist.

Threat scenarios	Vulnerability
Compromising of sensors / actuators	Update distributed by the manufacturer or the integrator and comprising errors. Compromised update distributed by an attacker impersonating the integrator. Compromised update distributed by an attacker gaining access to the network. Compromised update distributed following the compromising of the maintenance station.
Unauthorised access to the maintenance station	No systematic locking of the session. No protection of identifiers and passwords. Weak passwords. Vulnerability of the operating system.
Compromising of the maintenance station	Absence of verification of the innocuousness of the removable media. Insufficient antivirus verification in the email system. Internet browsing. Inappropriate use of the workstation. Weak configuration. Compromised application of an update.
Use of the maintenance station as a connection bridge	Double connection (for example, use of a 3G key while connected to the installations of the tunnel). An incorrect configuration can render the installations of the tunnel directly accessible from Internet.
Loss or theft of the maintenance station	Negligence. Aggression. Voluntary act of the operator or of the integrator.

3.2.3 Vulnerabilities

The table hereinbelow lists the vulnerabilities that can lead to unauthorised access.

Vulnerability	Description
No systematic locking of the session	An operating user or integrator left their session open. Similarly, there is no automatic closing of a session after a period of time, leaving the possibility for anyone to use the session.

Vulnerability	Description
No protection of identifiers and passwords	This user information is, for example, listed on a board or notebook or any other media that can be accessed by an unauthorised person. Similarly, the authentication elements of the users are not stored securely.
Weak passwords	The password management policy is not strong enough to impose passwords of which the complexity is sufficient.
Weakness of communication protocols	The protocols used do not make it possible to protect the exchanges, whether in terms of confidentiality or in terms of integrity, allowing for an interception or modification of the flows. This can concern for example exchanges between the supervision server and workstation, or between the main and secondary PCC.
Weak configuration	The configuration of the station or of the device does not correspond to best practices (absence of a local firewall, station in "AutoLogin") and in fact needlessly renders the station sensitive to attacks.
Vulnerability of the operating system	A vulnerability can be discovered on the operating system that gives the attacker the possibility to access and to compromise the supervision system.
Loss or theft of a mobile station	The probability of a loss or theft is substantially greater for a mobile workstation than for a desktop computer. This point is further aggravated when the station is shared and is not assigned to a location or to a person: it is indeed possible that the disappearance goes unnoticed, providing the attacker with more time to recover the sensitive data or pre-configured accesses to certain devices that it could contain.
Use of a default account	The manufacturers and publishers can set up one or several accounts by default in order to facilitate remote control, providing anyone who has the documentation access with the authorisations that are granted to these accounts.
Access from a compromised workstation	A user is not aware that his station has been compromised and accesses another device (supervision server, PLC, etc.). The attacker at the origin of the compromise can recover the identifiers and passwords used or take advantage of the connection established.

Vulnerability	Description
Physical access to the devices	The absence of limitation of physical access to devices (workstations, sensors actuators, etc.) provides anyone with the possibility to make modifications (trapping, modification of the configuration, etc.).
Physical access to the network	The absence of a limitation in terms of the physical access to the network devices of the PCC or of the tunnel gives anyone the possibility of modifying the existing connections or of connecting an external device.

The table hereinbelow lists the vulnerabilities that can lead to unauthorised access.

Vulnerability	Description
Absence of verification of the innocuousness of the removable media	In the absence of a restriction on the use of removable media, a user can involuntarily import and then transport malware from one station to another. In addition to conventional removable media, the importing and transmission can also be done via a telephone that he connects to the USB port of his station in order to charge it.
Direct access to internet and email	A user directly accesses and without special precaution a compromised website from his workstation or opens a malicious attachment. Once contaminated, he uses this same station to connect to a device. This access can be done using the normal network connection of the station or via a telephone with a USB connection.
Inappropriate use of the workstation	A user can install software for non-professional use on his workstation (games, audio player, etc.).
Lack of verification for updates	A user recovers an update ad deploys it on the device concerned. The absence of verification does not make it possible to ensure that the update corresponds to that distributed by the manufacturer or the integrator.
Access from a compromised workstation	A user is not aware that his station has been compromised and accesses another device (supervision server, PLC, etc.). The connection is then used to spread the malware at the origin of the compromise.

Vulnerability	Description
Uncontrolled distribution of sensitive information	In the framework of a communication action, the company describes in excessive detail the devices and their implementation. The attacker only has to seek information on the vulnerabilities of the devices in question in order to carry out his attack.

3.3 Examples of attack scenarios

3.3.1 Case of a targeted attack: installation of malware

A targeted attack corresponds to a voluntary act with intention to harm the missions of the tunnel.

This is the case, for example, of an ill-intentioned employee of the integrator Integro. He benefits from a workstation whereon is installed the maintenance tools of the supervision software. It may be that the employee introduces malware into the source code. If no protection or verification of the code is carried out, either during the local compilation, or during the copying of the compiled code, the infected software will be copied to the administration station which will then be deployed on the supervision server.

Starting from this moment, all of the components of the supervision network and of the field network can be infected by the spreading of the malware.

In this case, the supervision application is inoperative. Alarms no longer roll up to the console of the operator. Likewise, the video cameras no longer make it possible to visually control the circulation in the tunnel. Consequently, and as a precautionary measure, the tunnel has to be closed.

3.3.2 Case of a non-targeted attack: spread of a virus

A non-targeted attack corresponds to an act, whether or not voluntary, without the latter revealing any desire to harm the missions of the tunnel.

This is the case for example, of an employee of the operator Tunnello who connects his workstation to download a firmware update for a device. He takes advantage of this to browse a few unsecured websites for his own personal use, infecting his station with malware disguised as a document. After browsing, the employee disconnects his station from the Internet and connects it to the network of the tunnel in order to update the device in question: the malware can then spread over the supervision server.

If the malware is not intended for ICSs, it can simply render all of the computers of the PCC inoperable, including the supervision server. This no longer makes it possible for operators to ensure the proper operation of the tunnel, and they therefore decide to shut down the latter.

If on the contrary the malware is of the “industrial type”, it can spread over the devices of the tunnel, sending for example STOP commands in the various common protocols. This renders the tunnel inoperable and causes deterioration at the level of some actuators.

3.3.3 Case of an indirect targeted attack: trapped devices

An indirect attack consists in integrating trapped devices before they arrive on the site (when leaving the factory or during transit).

This case study however explicitly excludes the hypothesis of an attacker at the State level able to make use of a third party (supplier, integrator or carrier) to carry out an attack of this type on the tunnel: the supply chain of Tunnello is indeed considered to be controlled and intact.

3.4 Security analysis pertaining to the initial approach architecture before conducting the method

The architecture of figure 2.4, presented before the securing method, shows the physical components distributed over the supervision network and the field network. This diagram shows the video devices that are directly connected to the supervision network (by the intermediary of switches).

Note the redundancy for each type of component:

- the control centers: Meyrueis and Millau;
- the supervision stations inside a control center;
- the devices connected to the supervision network and to the field network.

The preceding section emphasised examples of attacks, whether voluntary or not, that apply to the unsecured architecture of figure 2.4. The connecting of a workstation (of the integrator or of the operator) to the supervision network is a proven breach of the ICS. Indeed:

- the station of the integrator is not controlled;
- the station of the operator can a priori connect to the Internet (whether or not this connection is simultaneous with the connection to the devices of the tunnel);
- the same station is used for the maintenance of several tunnels.

Moreover, the lack of logging and detection of intrusions does not make it possible to detect potential threats as early as possible.

Finally, no means of filtering makes it possible to provide a level of partitioning between the various networks, which limits the securing (in cybersecurity terms) of this solution.

The means for securing are detailed via the scenario in the following chapters.

Chapter 4

Classification

According to the methodology formalised by the working group, once the list of main functions has been established (cf. section 2.3), the classification of the latter should be carried out according to their needs in terms of cybersecurity.

Recall that for ICSs the method proposes three classes numbered from 1 to 3, in increasing order of criticality, of which the coverage is:

- Class 1: the risk and impact of an attack are low;
- Class 2: the risk or impact of an attack is significant;
- Class 3: the risk or impact of an attack is critical.

Classification is carried out according to the likelihood and the impact of an attack.

The impact of an attack is measured according to scales that can be normalised or specific to the company, according to its level of resilience and the risks that it deems are acceptable. These scales are generally validated by the management upstream of the analysis of risks and are valid for all of the projects. The section 4.1 presents the scales retained by Tunnello.

The likelihood (L) is based on the following criteria:

- E the exposure, which reflects the levels of functionality and of connectivity;
- A the level of the attacker;
- U the level of accessibility of the ICS by the users.

The likelihood is then obtained with the following formula:

$$L = E + \left\lceil \frac{A + U - 2}{2} \right\rceil$$

Consult the reference documentation of the classification method [ANS14a] for a more complete description of the classes (section 2.1) and criteria (section 3.2), as well as the relations between the latter.

4.1 Scales

In light of its obligations and its needs, Tunnello has set down a severity scale from 1 to 5, based on the impact scales such as indicated hereinbelow:

	Level	Qualifying	Description of the consequences
Human impacts	1	Insignificant	Accident reported, no medical leave or treatment.
	2	Minor	Accident reported, with medical leave or treatment.
	3	Moderate	Permanent disability.
	4	Major	A death.
	5	Catastrophic	Multiple deaths.

	Level	Qualifying	Description of the consequences
Financial impacts	1	Insignificant	Accident that does not require any refurbishing work
	2	Minor	Accident requiring limited refurbishing work
	3	Moderate	Major deterioration of the tunnel of which the refurbishing represents more than 5% of the construction price of the tunnel
	4	Major	Major deterioration of the tunnel of which the refurbishing represents more than 15% of the construction price of the tunnel
	5	Catastrophic	Major deterioration of the tunnel of which the refurbishing represents more than 40% of the construction price of the tunnel

	Level	Qualifying	Description of the consequences
Impacts on availability	1	Insignificant	Accident resulting in a disturbance over a single direction of travel
	2	Minor	Accident causing the closing of one direction travel or disturbing both directions of travel (alternating circulation for example) for several hours
	3	Moderate	Minor deterioration of the tunnel representing several days of unavailability for repairs
	4	Major	Major deterioration of the tunnel representing more than a month of unavailability for repairs
	5	Catastrophic	Major deterioration of the tunnel representing more than 6 months of unavailability for repairs

Note that in order to simplify its study, Tunnello decided to include the legal and image impacts, within the financial impact that also covers operating losses: due to its activity, the latter will especially have the form of damages or loss of activity.

Tunnello also deems that the impacts in terms of availability of a minor and moderate level apply only in the case of impact on peak periods (period of high transit during the school holidays), with the bypass via the historical road (which represents an increase in travel time of 30 minutes) being deemed as acceptable during the rest of the year.

Tunnello moreover decided to use the same scales that define the levels of likelihood, attacker and user as those given as an example in the guide [ANS14a], with the latter deemed as adapted to the situation.

4.2 Hypotheses of the study

For the analysis as a whole, Tunnello retains an attacker of the private organisation type that does not have any substantial means (terrorism for example), therefore of level 4 according to the guide on classification.

In addition, as the possibility of traceability of all the actions over all the components cannot be guaranteed, the users are assumed to be of level 2, i.e. authorised and certified, for all of the functions.

Finally, the critical functions must be able to be triggered autonomously and automatically (reflex functions).

4.3 Classification by function

This analysis is mostly based on the risk and threat analysis presented in chapter 3. Initially, it is carried out on the isolated functions, i.e. without taking into account the dependencies described in section 2.4, which will be taken into account in what follows.

Fire detection

Fire detection is a particularly critical dependability function since it is in charge of triggering certain reflex actions and raising alerts on an incident intended for the control center.

The analysis as such gives a functionality of level 2 and a connectivity of level 4. Given the hypotheses on the users and attackers, an exposure of 4 is deduced and a likelihood of 6.

The FMECA analysis of the function (section 3.1) in addition makes it possible for Tunello to quantify the impact of a possible malfunction of the function at a catastrophic level (5).

A function of class 3 is as such obtained.

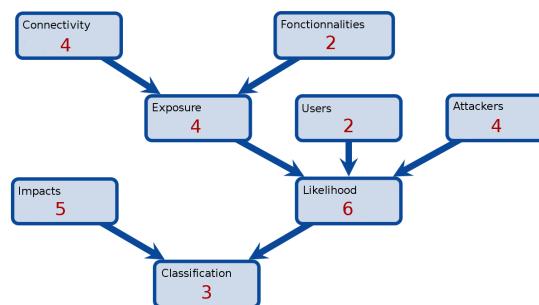


Figure 4.1: Classification - Fire detection

Air quality control

This function is intended to detect excessive concentrations of toxic gases, and especially exhaust gases. As with fire detection, it is in charge of triggering certain reflex actions and raising alerts on an incident intended for the control center.

This preliminary analysis therefore gives a functionality of level 2 and a connectivity of level 4. Given the hypotheses on the users and attackers, an exposure of 4 is deduced and a likelihood of 6.

The FMECA analysis of the function in addition allows Tunnello to quantify the impact of a possible malfunction of the function at a major level (4) in case of an accumulation that is not detected in time (and therefore not taken into account by the other functions).

A function of class 3 is as such obtained.

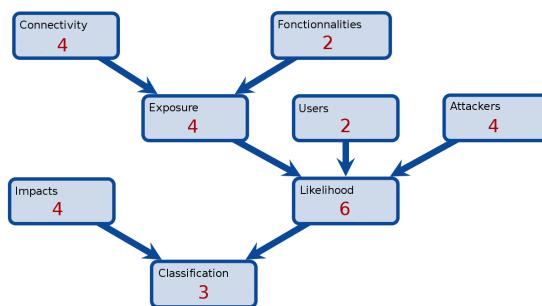


Figure 4.2: Classification - Air quality control

Indication of emergency exits

As exposed in section 2.3, the function of indicating emergency exits in two ways:

- regulatory lighted signs that remains lit permanently;
- dynamic lightning to help self-evacuation, which can be triggered.

In the first case, the function is provided with a battery in order to overcome any cut-off in the electrical power supply, and is not strictly speaking an ICS and can be excluded from the rest of the analysis.

In the second case, there is a functionality of level 1 and a connectivity of level 4. Given the hypotheses on the users and attackers, an exposure of 4 is deduced and a likelihood of 6.

The direct impact is insignificant (the stopping of the function while the tunnel is in nominal mode is of no consequence), but the indirect impact, as an aggravating factor of an incident, is of level 5 (death of several people who did not find the emergency exit).

A function of class 3 is as such obtained.

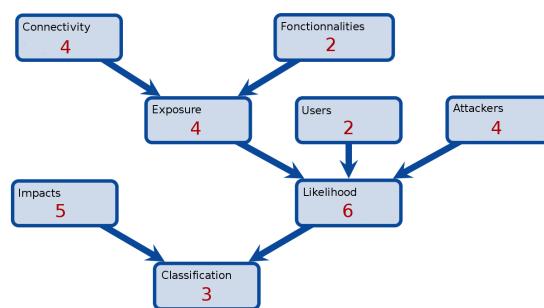


Figure 4.3: Classification - Indication of emergency exits

Ventilation

The ventilation of the tunnel is a vital function either in nominal mode or following an incident. This indeed entails, in the first case, avoiding the accumulation of exhaust gas (toxic for people) and, in the second case, evacuating the smoke (but without fanning the flames of a fire).

Ventilation therefore operates both in reflex mode and via control of the control center, which supervises it.

The analysis therefore gives a functionality of level 2 and a connectivity of level 4. Given the hypotheses on the users and attackers, an exposure of 4 is deduced and a likelihood of 6.

The impact of a malfunction can be catastrophic, whether in nominal operation (asphyxiation by the accumulation of exhaust gases) or following an accident (asphyxiation by un-evacuated smoke, activation of a fire, etc.).

A function of class 3 is as such obtained.

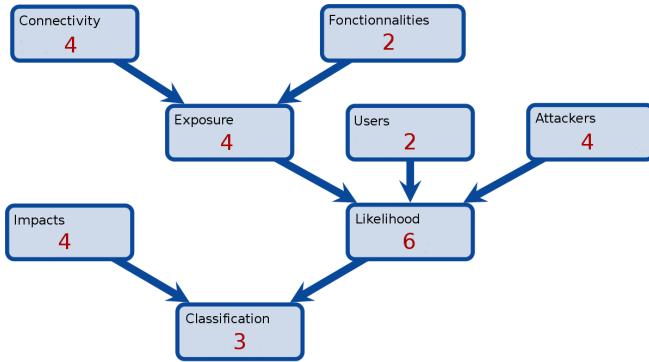


Figure 4.4: Classification - Ventilation

Signalling

This function corresponds both to the variable message signs and to the various signals (lane assignment lighted signs, motorised access barriers, etc.) that can be used in the tunnel. These signals are essentially controlled by the control center.

The analysis therefore gives a functionality of level 2 and a connectivity of level 4. Given the hypotheses on the users and attackers, an exposure of 4 is deduced and a likelihood of 6.

Their malfunction can result in an accident but as the drivers must remain in control of their vehicles, the impact is considered as moderate (3).

A function of class 2 is as such obtained.

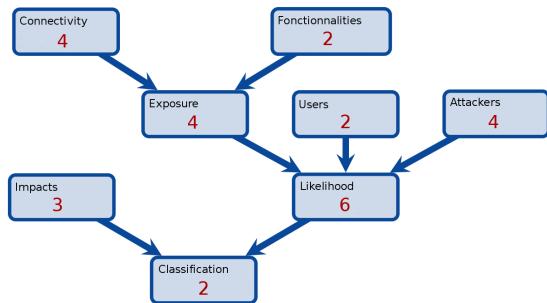


Figure 4.5: Classification - Signalling

Emergency call network

This function corresponds to the possibility for the people driving in the tunnel to be able to contact the control center or, lacking this, the emergency teams in order to report an emergency or a difficulty (for example a vehicle breakdown that makes it impossible to complete the transit through the tunnel).

The analysis therefore gives a functionality of level 2 and a connectivity of level 4. Given the hypotheses on the users and attackers, an exposure of 4 is deduced and a likelihood of 6.

The first purpose of this system is to allow a driver to request assistance in order to solve a problem involving this user. In addition, this system is complementary with other systems that make it possible to alert the PCC of the occurrence of an incident. Its impact is therefore considered to be level 1.

A function of class 1 is as such obtained.

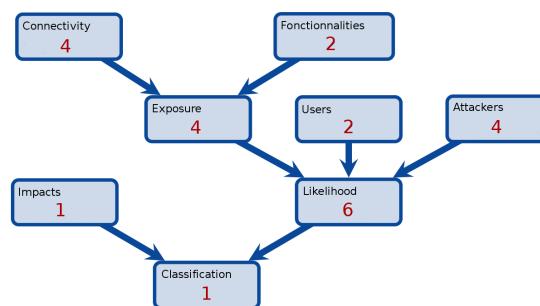


Figure 4.6: Classification - Emergency call network

Detection of oversize vehicles

This function corresponds to devices that make it possible to detect vehicles that could possibly block traffic at the entrance or inside the tunnel (non-standard trailers, for example), in order to encourage them to use another itinerary.

These devices are supervised by the control center. The analysis therefore gives a functionality of level 2 and a connectivity of level 4. Given the hypotheses on the users and attackers, an exposure of 4 is deduced and a likelihood of 6.

The malfunction of this mechanism, complementary to the road signs in such a way that a driver complying with traffic regulation would not go into the tunnel, would result at worst in the closing of the tunnel, therefore an impact of level 1.

A function of class 1 is as such obtained.

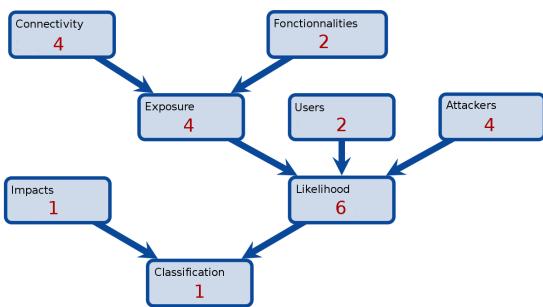


Figure 4.7: Classification - Detection of oversize vehicles

Video surveillance

Video surveillance allows the operators of the control center to follow the state of the traffic using cameras located inside the tunnel.

The analysis therefore gives a functionality of level 2 and a connectivity of level 4. Given the hypotheses on the users and attackers, an exposure of 4 is deduced and a likelihood of 6.

As video surveillance is primarily used as assistance in operating the tunnel, supplementing the other functions, a malfunction is considered as having an impact of level 1.

A function of class 1 is as such obtained.

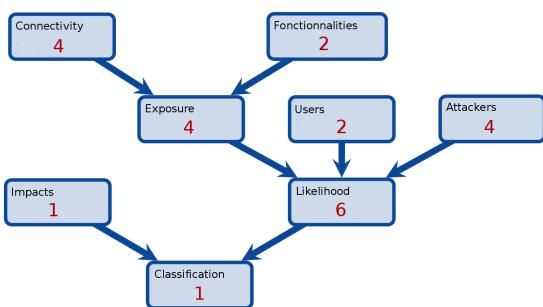


Figure 4.8: Classification - Video surveillance

Electrical power supply and distribution

This function groups together the sensors and actuators responsible for the stability of the electrical power supply, in particular the switching of it to backup mode (the installation has a power generator and an inverter). The supervision of this function

can also trigger a degraded mode (for example the closing of the tunnel while still maintaining the functions required for an evacuation without incident). From this a functionality level of 2 is deduced.

As the power supply and distribution are supervised by the main control station, its connectivity is level 4. Note that if the power distribution is also supervised (and so operated, at least in some cases) by the energy supplier, it can result in a higher level of connectivity (i.e. a level of 5).

Given the hypotheses, an exposure of level 4 (or 5 if supervision by the energy supplier) is deduced for this function and therefore a likelihood of 6 (in both cases).

An attack against the power supply will have a moderate direct impact (at most the break out of a fire). However, in the case of an automated power supply, the function to be protected is indeed the availability of the supply of energy, not the automation of it. In the absence of satisfactory work-around procedures (no presence on site that allows for quickly setting up a backup power supply), the indirect impact corresponds to the highest level in case of unavailability of one of the functions that requires electrical power. Ventilation, which satisfies this condition, therefore induces an impact of level 5.

We can conclude from this that the electrical power supply is of class 3.

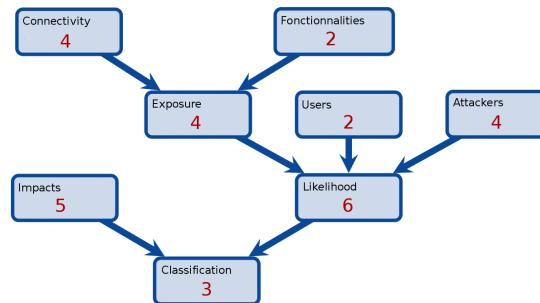


Figure 4.9: Classification - Electrical power supply and distribution

4.4 Functional dependencies and classes

Beyond the classification of the functions in a unitary manner, the analysis should be supplemented by the study of the relationships between these functions.

Indeed, one of the founding principles of the analysis of functional dependencies is that information supplied by a device of a high class can be transmitted to a device of

a lower class, but information coming from a low class device cannot be transmitted to a device of a higher level.

In other words, a class 2 device can transmit alerts and supervision elements to a class 1 device, but its operation must depend solely on information coming from a class 2 or 3 device. A class 3 device can only depend on information supplied by other equipment of the same class.

This principle is a directive in the case where the higher class is class 3 (D.159), and recommendation in the case where the higher class is 2 (R.157).

As such, in application of this principle, the analysis of functional dependencies of the preceding chapter (and summarised in figure 2.2) imposes reclassifying the oversize detection as class 2 due to its relationship with signalling.

Likewise, from this partitioning between the various classes stems the need to instantiate the “control station” function for each class present in the industrial information system, as can be seen appearing in figure 4.10.

4.5 Final classification

In conclusion, the results of the analysis are presented in the table hereinbelow. This classification of the functions will be used for the rest of the analysis.

Class	Functions
Class 1	Video surveillance Emergency call network
Class 2	Detection of oversize vehicles Signalling
Class 3	Electrical power supply and distribution Indication of emergency exits Ventilation Fire detection Air quality control

Taking the principle that a function that is shared by several classes, as is the case with Supervision, cannot be mutualised, we obtain the functional dependencies diagram 4.10.

In practice, it is possible to retain a strong partitioning between the various classes or to carry out certain groupings, the recommendations to be complied with being those of the highest class in the grouping.

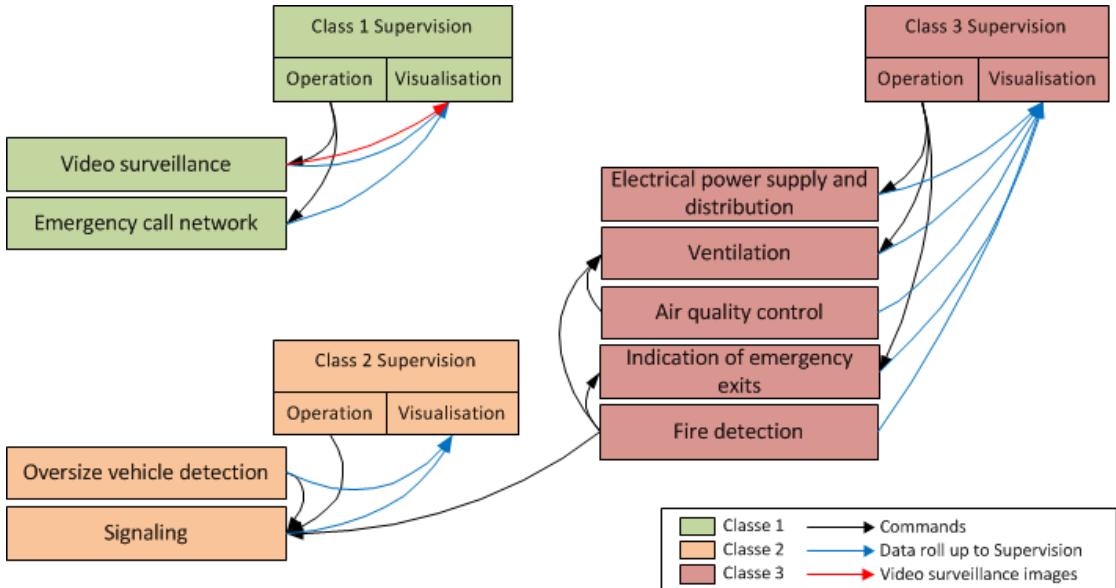


Figure 4.10: ICS - Graph of functional dependencies

In the following chapter, the various main measures [ANS14a] will be broken down according to several configurations corresponding to the following groupings:

- all of the functions are grouped together in the same class set C3;
- the functions are distributed into three separate sets according to their class (C1, C2 and C3);
- the functions of class C1 and C2 are grouped together, with the functions of class C3 forming a second set;
- the functions of class C2 and C3 are grouped together, with the functions of class C1 forming a second set.

Chapter 5

Possibilities of regrouping classes

The preceding chapter allowed us to carry out a first theoretical classification of the various functions, according to the cybersecurity needs. This classification is summarised in section 4.5.

It appears that functions are present in each one of the three classes. With this observation, Tunello therefore decided to see if a certain rationalisation could be considered by grouping certain classes together without however lowering the level of cybersecurity. To do this, Tunello and its integrator reviewed the main differences that exist in the breakdown of the main measures for each one of the groupings under consideration.

For didactic purposes, this review of the groupings that can be considered is presented separately from the breakdown of the main measures (reference will be made to the appropriate chapter of the second part of this study [ANS16b]). In an actual analysis, these two steps are carried out jointly, at least initially: the advantages and disadvantages of the various groupings will appear as the main measures are refined. This chapter focuses exclusively on the points of divergences that have an influence on the choice of a possible grouping, reference will be made to the appropriate chapter for a complete breakdown of the main measures.

Recall that when two or more classes are grouped together, it is the rules that correspond to the most sensitive class that are systematically applied. In other terms, the lower classes are aligned with the highest class within the grouping.

5.1 The various configurations considered

Configuration	Comments
"C1 , C2 , C3"	This grouping corresponds to a direct application of the classification stemming from the preceding chapter. The measures are as such applied by segmenting the architecture by class, in order to apply only the measures required for each class. This case is noted in what follows as "C1 , C2 , C3"
"All C3"	Unlike the preceding grouping, the information system is considered as a whole, without taking the classification of the functions into account. Thus, the rules concern an architecture that does not comprise any segmentation linked to the classes. The rules that can be applied are then those of the highest class present in the system, i.e. class 3 in the case at hand. This case is noted in what follows as "all C3"
"C1+C2, C3"	The purpose is to unfold all of the rules over an intermediate architecture, grouping together two of the three classes. It therefore groups C1 and C2 together on one side and C3 on the other. This case is noted in what follows as "C1+C2, C3"
"C1, C2+C3"	As above, the purpose is to unfold all of the rules over an intermediate architecture, grouping together two of the three classes. This configuration as such groups C2 and C3 together on one side and C1 on the other. This case is noted in what follows as "C1, C2+C3"

Before proceeding with choosing the best configuration, it can be useful, in order to better understand the operating mode of the tunnel, to model the flows between the various classes in the form of a simplified logical architecture diagram, declined from the graph of function dependency (cf. figure 4.10).

Figures 5.1 to 5.4 correspond to these architecture diagrams for the four configurations under consideration. Supervision is not presented for reasons of readability.

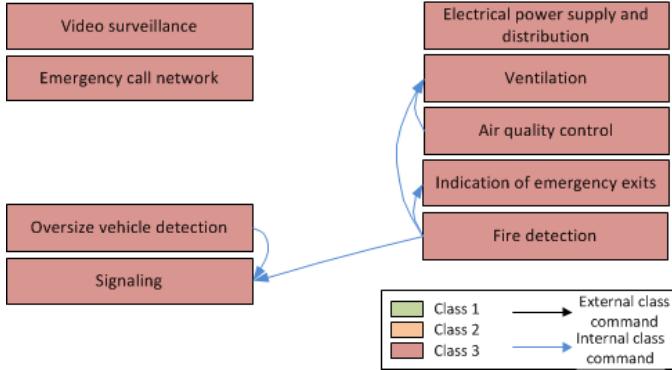


Figure 5.1: Flow diagram - "All C3"

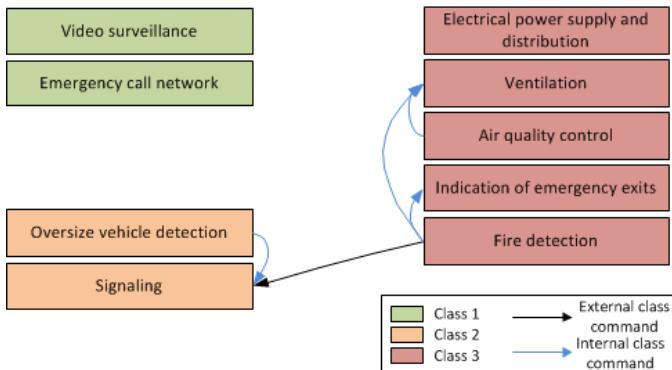


Figure 5.2: Flow diagram - "C1, C2, C3"

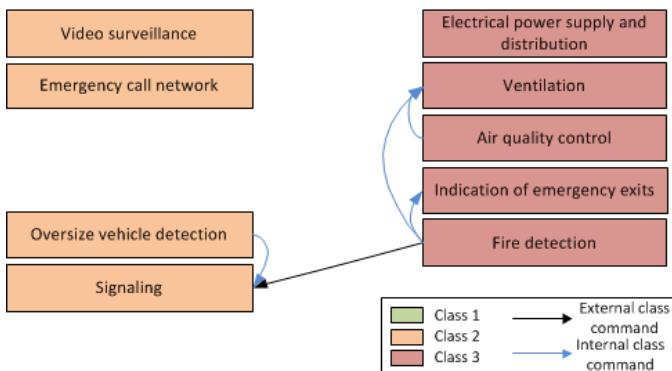


Figure 5.3: Flow diagram - "C1+C2, C3"

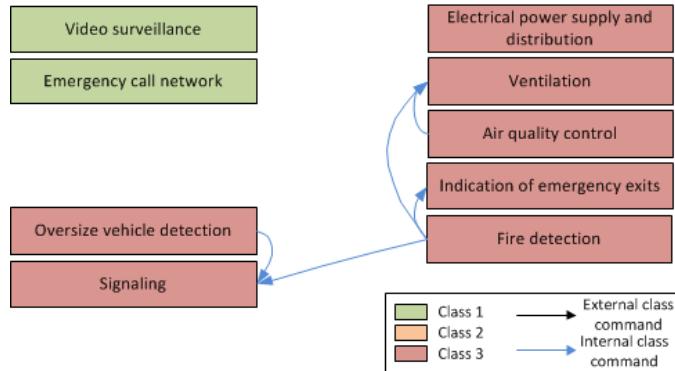


Figure 5.4: Flow diagram - "C1, C2+C3"

5.2 The main differentiating elements

5.2.1 User Training, Control and Certification

Training and authorisation

In the framework of its HR processes, Tunnello ensures that the operators have a level of training that is suitable for their position, which includes a module on cybersecurity awareness. This initial training is supplemented, for all persons concerned, by personnel authorisation conducted internally in order to intervene on the class 2 devices and carried out by a certified external organisation when they concern class 3 devices.

Control

Tunnello transcribes the information coming from HRIS (identity, accounts, certification where applicable, devices on which Tunnello is authorised to intervene) into technical directories, one per class. The latter are used as much as possible by the devices of the corresponding class for the management of authorisations and log the access via the supervision mechanisms.

As such, a grouping of certain classes allows for a sharing of the corresponding directories and therefore a simplification of the entire operation.

5.2.2 Audits

Audits are necessary for the various classes, such as will be specified during the breakdown of the various measures. It can however be noted that the latter are all the more significant the higher the class involved is.

In addition, an internal audit conducted by a team dedicated to this type of activity can be sufficient for class 1 infrastructures, while calling upon a certified service provider is required for class 3 infrastructures.

Maintaining a separation when this is possible therefore does make it possible to limit the financial impacts on the operations, since the constraints of class 3 are not passed on to the lower classes.

5.2.3 Monitoring process

For each new vulnerability, Integro evaluates the exposure of the system and the potential impacts in order to decide with the operating teams and the manager of the security of ICSs the action to be taken (accepting and documenting the risk, updating the devices, setting up work-around resources, etc.).

The constraints, in particular in terms of deadlines, for the carrying out of this evaluation and, where applicable, the application of patches, are linked to the class of the devices. This process will therefore have an impact that is all the more significant given the "high" classes group a large number of devices together.

5.2.4 Network Segmentation and Segregation

The control centers, on the one hand, and the field system, on the other hand, are considered as two separate units within the same architecture. Firewalls, redundant and separate, are therefore set up on either side of the connection in order to partition these two sets within each one of the classes. These firewalls are in addition qualified for the C2 and C3 classes.

Likewise, for each one of the classes, the communications between these two sets are carried out through a pair of IPsec VPN gateways dedicated to the class under consideration.

The grouping together of certain classes would have the effect of reducing these security devices at a network level.

5.2.5 Remote Diagnosis, Remote Maintenance and Remote Management

Supervision makes it possible to modify the operation of the system through the intermediary of the Operation subfunction and its possible action on the set parameters. In these terms, Supervision from the PCC at Millau forms a remote management mechanism.

This mechanism is based in particular on communications between the PCC and the site of the tunnel, communications which are carried out through an encrypted and authenticated tunnel over a dedicated line (segmentation via MPLS), as indicated hereinabove in this chapter (cf. 5.2.4).

Moreover, as will be outlined in the chapters devoted to breaking down the various measures, there is no administration network strictly speaking. This in fact imposes the use of one mobile station per class for maintaining the industrial devices.

Here again, a reduction in the number of infrastructures via the grouping together of certain classes would make it possible to reduce the number of MPLS connections required and the mobile stations dedicated to maintenance.

5.2.6 Surveillance and Intrusion Detection Methods

Through the architecture implemented, Integro provides a log server per class, at least for the devices that allow for an automatic roll up. The latter generate an overview report intended for the operations department, on a daily basis for class 3, biweekly for class 2 and weekly for class 1.

The anomalies and alarms rolled up are moreover taken into account according to the particularities provided for in the framework of incident management, details of which are provided hereinbelow in the appropriate section. This management is, among other things, controlled by the class of the devices concerned.

With regards to logging, it is observed that a reduction in the number of classes simplifies operations by harmonising the corresponding procedures. At the same time, not grouping devices together into a high class when this is not necessary prevents having to apply unnecessary restrictive procedures to it.

5.2.7 Intervention Management

Main principles

It is assumed that any intervention generates the creating of a ticket in the appropriate manager regardless of the devices concerned and the intervention. Tunnello considers therefore that this ticket manager acts as a logbook.

Access to the premises

Due to the presence of class 3 devices, Tunnello has provided to set up access control to the premises via an individual badge, an alarm and video surveillance for the main and secondary control stations. The security policy reserves the delivery of these badges only to internal users.

The other premises and cabinets, which are not protected by access control but which house class 3 devices, are provided with an alarm, seals and locks of which the keys are retained in a key box at the secondary control station. Access to these therefore indirectly requires the use of a badge.

The obligation to call the main control station to raise the alarm is considered by Tunnello as a traceability mechanism that is sufficient for cabinets that contain class 2 devices or that concern video surveillance (class 1) when the cabinets are protected by an alarm. A key and seals are therefore entrusted to the users for these functions. Traceability moreover allows Integro to be able to intervene on these devices without the presence of a Tunnello operator.

For the other cabinets that contain only class 1 devices, they keys for the dedicated cabinets are entrusted to the users in charge of these functions.

This quick analysis shows that by not grouping devices together in a high class when this is not necessary, Tunnello prevents having to apply unnecessary restrictive procedures to it, such as for example the required presence of a Tunnello employee in order to carry out or accompany a simple maintenance operation.

Device maintenance

The specifications stipulate that class 2 and 3 devices must be supplied with all of the hardware and software tools required for diagnostics and for interventions, in order to cover all possible cases, with however a tolerance for the tools for which the usage remains exceptional in the case of class 2 devices.

The maintenance contract for devices must also cover the diagnostic and maintenance tools and the updating of them. These devices are acquired by the Tunnello company and are dedicated to the site.

As in the preceding point, an unnecessary grouping of devices into a high class could have a substantial financial impact.

5.3 Choice of the configuration

The analysis of the differentiating elements hereinabove show that although grouping classes together in order to rationalise the infrastructures can have a few advantages both in the design and in the operating of the whole, this also has disadvantages.

As such, the first reflex which would consist in bringing together all of the devices into a single class 3 infrastructure does indeed make it possible to limit the number of devices but imposes substantial constraints in terms of the operating of the least

sensitive elements: the obligation to devote to the site a complete set of maintenance and diagnostic tools for the emergency call network or the reinforced monitoring of alerts for this function can appear to be oversized. Because of this, Tunnello does not retain the “all C3” configuration.

For similar reasons, Tunnello issues a preference for the “C1, C2+C3” configuration to the “C1+C2, C3” configuration, as it seems to Tunnello that it is a little simpler to factor the procedures in the first case than in the second case.

The analysis of figures 5.1 to 5.4 shows moreover that the “all C3” and “C1, C2+C3” configurations seem, from the flow diagram standpoint, simpler than the two others due to the independence of the various groupings.

On the contrary, the “C1+C2, C3” and “C1, C2, C3” configurations reveal a link between the two field networks C3 and C2 in one direction. Indeed, starting with the data collected on the sensors of the C3 field network C3 (in particular Fire detection and Air quality control), certain pieces of information have to be sent to the actuators of the C2 field network (signalling).

These elements therefore bolster separating the “C1+C2, C3” configuration to the benefit of the “C1, C2+C3” configuration.

Finally, the “C1, C2, C3” configuration, which has a different infrastructure per class effectively prevents the unnecessary restrictions but has a more expensive architecture that is more complex to maintain due to the two field networks.

In the particular case of the tunnel, the separation of C1 on one side and C2+C3 on the other makes it possible to limit the restrictions on the class 2 devices while still reducing the technical and organisational complexity. The additional constraints applied to class 2 devices are relatively limited due to the nature of the class 2 functions and the possibility of sharing the security functions with the class 3 devices.

So Tunnello has decided to implement the “C1, C2+C3” configuration.

Bibliography

- [ANS14a] *Cybersecurity for Industrial Control Systems - Classification Method and Key Measures.*
Guide Version 1.0, ANSSI, janv 2014.
http://www.ssi.gouv.fr/uploads/2014/01/industrial_security_WG_Classification_Method.pdf.
- [ANS14b] *Cybersecurity for Industrial Control Systems - Detailed Measures.*
Guide Version 1.0, ANSSI, janv 2014.
http://www.ssi.gouv.fr/uploads/2014/01/industrial_security_WG_detailed_measures.pdf.
- [ANS16a] *Practical Case of a Road Tunnel - Part 1: Classification.*
Cas pratique Version 1.0, ANSSI, sept 2016.
<http://www.ssi.gouv.fr/systemesindustriels>.
- [ANS16b] *Practical Case of a Road Tunnel - Part 2: Measures.*
Cas pratique Version 1.0, ANSSI, sept 2016.
<http://www.ssi.gouv.fr/systemesindustriels>.
- [CET10] *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.
- [CET03] *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.

This case study on cybersecurity for Industrial Control Systems was produced by the French Network and Security Agency (ANSSI / Agence nationale de la sécurité des systèmes d'information) with the help of the following companies and organisations:

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

About ANSSI

The French Network and Information Security Agency (ANSSI / Agence nationale de la sécurité des systèmes d'information) was created on 7 July 2009 in the form of an agency as an agency with national jurisdiction.

By Decree No. 2009-834 of 7 July 2009 as amended by Decree No. 2011-170 of 11 February 2011, the agency has responsibility at national level concerning the defence and security of information systems. It is attached to the General Secretary of Defence and National Security, under the aegis of the Prime Minister. For more information on ANSSI and its missions, please visit www.ssi.gouv.fr/en/.

Version 1.0 – October 2016 (translation: September 2017)

Licence « information publique librement réutilisable » (LIP V1 2010.04.02)

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