

Practical Case of a Road Tunnel

Part 2: Measures

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 [ANS16a] 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	9
2	Reminder of the context of the case study	11
2.1	Context	11
2.2	Presentation of the company	11
2.3	Physical organisation of the tunnel	12
2.4	Functions implemented in the tunnel	13
2.5	Categorisation of the various functions	14
3	Breakdown of the main measures	15
3.1	Role and responsibility	15
3.2	Risk Analysis	15
3.3	Mapping	16
3.4	Operator Training, Control and Certification	16
3.5	Audits	17
3.6	Monitoring process	18
3.7	Business Resumption Plan and Business Continuity Plan	18
3.8	Emergency Modes	19
3.9	Alert and Crisis Management Process	19
3.10	Network interconnections	20
3.11	Remote Diagnosis, Remote Maintenance and Remote Management	21
3.12	Surveillance and Intrusion Detection Methods	22
3.13	Intervention Management	23
3.14	Architecture diagrams	24
4	Breakdown of the detailed measures of the organisational type	27



4.1	Knowledge of the ICS	28
4.1.1	Roles and responsibilities	28
4.1.2	Mapping	29
4.1.3	Risk Analysis	29
4.1.4	Back-up Management	30
4.1.5	Documentation Management	30
4.2	User Control	31
4.2.1	User Management	31
4.2.2	Awareness and training	32
4.2.3	Intervention Management	32
4.3	Integration of cybersecurity in the ICS life cycle	33
4.3.1	Requirements in contracts and specifications	33
4.3.2	Integration of cybersecurity in the specifications phases	34
4.3.3	Integration of cybersecurity in the design phases	34
4.3.4	Audits and cybersecurity tests	35
4.3.5	Operational transfer	35
4.3.6	Management of modifications and changes	36
4.3.7	Monitoring process	37
4.3.8	Obsolescence Management	38
4.4	Physical security and access control for premises	38
4.4.1	Access to the premises	38
4.4.2	Access to devices and cabling	39
4.5	Incident response	40
4.5.1	Business Resumption Plan or Business Continuity Plan	40
4.5.2	Degraded modes	40
4.5.3	Crisis Management	41

5	Breakdown of the detailed measures at the technical level	43
5.1	User authentication: logical access control	43
5.1.1	Account Management	43
5.1.2	Authentication management	44
5.2	Securing the ICS architecture	45
5.2.1	Partitioning ICSs	45
5.2.2	Interconnection with the MIS	45
5.2.3	Internet access and interconnections between remote sites	46
5.2.4	Remote Access	46
5.2.5	Distributed ICSs	47
5.2.6	Wireless communication	47
5.2.7	Protocol security	48
5.3	Securing devices	48
5.3.1	Configuration hardening	48
5.3.2	Vulnerability management	50
5.3.3	Connection interfaces	51
5.3.4	Mobile devices	52
5.3.5	Security for programming consoles, engineering stations and administrative workstations	53
5.3.6	Secure development	54
5.4	ICS Monitoring	54
5.4.1	Event logs	54
5.4.2	Detection Methods	55
A	Description of the components	57
A.1	Operating recess	57
A.2	Control center	57



A.3 Programmable logic controller	58
A.4 Fire Detection Unit	59
A.5 Man-machine interface	59
A.6 workstation	60
A.7 Maintenance station	60
A.8 Firewall	61
A.9 Diode	61
B Architectures for alternative groupings	63
B.1 "All C3" configuration	63
B.2 "C1 , C2 , C3" configuration	64
B.3 "C1+C2, C3" configuration	66
Bibliography	69

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 preliminary work carried out has allowed for the publication in January 2014 of two guides [ANS14a, ANS14b].

This document is the second part of this case study. It describes a possible breakdown of the protective measures present in the two guides, by applying it to the framework of securing a road tunnel. It is largely based on the elements of the first part [ANS16a] in order to justify certain choices.

The study was conducted by ANSSI in cooperation with key actors in the field, in the continuity of the initial working group. It presents various protective measures that can be considered according to jointly validated hypotheses. The securing scenario proposed is based on organisational as well as technical measures: indeed, it arises that a technical measure can advantageously replace an organisational measure and vice-versa. Good articulation between these two aspects makes it possible to reach an adequate level of protection with an acceptable cost.

Chapter 3 is devoted to exploring the main protective measures viewed as the axes of the securing strategy.

Chapters 4 and 5 form a securing proposal according to detailed measures of the second guide, following respectively the organisational axis and the technical axis.

Finally two appendices supplement this analysis: the first provides additional information on certain elements that constitute the road tunnel and the devices used while the second presents a few examples of other architectures that can respond to the cybersecurity need.

Chapter 2

Reminder of the context of the case study

2.1 Context

As indicated in its first part, 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

2.2 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 service providers¹, which are also fictitious, for certain tasks that it



cannot carry out itself:

- Integro provides the supply, integration and then maintenance of the ICS;
- Audito 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 of which details are provided 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.

2.3 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 and comprises technical premises (also called recesses) every 200m. 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), located in Millau and under the responsibility of Tunnello. It also has a control center on the site, primarily used as a backup and located on the Meyrueis side. In the event circulation 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.

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.



2.4 Functions implemented in the tunnel

As seen in the first part of this study, it is necessary to look more closely at the following functions², set up in the tunnel:

- electrical power supply and distribution;
- indication of emergency exits;
- 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, especially remote measurements;
- 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.

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.

²See the first part of the study for more information on these functions.

³Tunnello retained for ventilation and smoke extraction a transversal strategy with concentrated extraction.

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.

2.5 Categorisation of the various functions

The first part of the study made it possible to determine in a first step the class of the various functions, then to analyse the rationalisation provided by the grouping together of the two highest classes, a configuration also noted as “C1, C2+C3” in the first part.

Figure 2.2 summarises the class of each function as well as the relationships between classes such as they will be developed in the rest of this study.

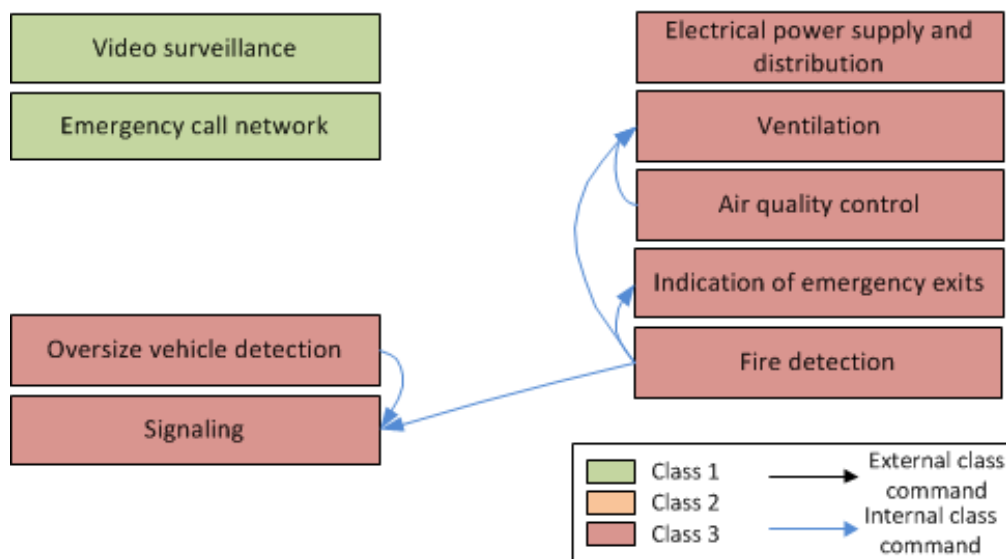


Figure 2.2: Flow chart - “C1, C2+C3”

Chapter 3

Breakdown of the main measures

After a macroscopic use in the first part of the study in order to choose the most suitable grouping, it is now time to decline more fully the main measures presented in the appropriate guide [ANS14a].

This chapter is voluntarily written with a rather “project manager” standpoint, i.e. that of Tunnello, in so much as the measure allows.

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.

3.1 Role and responsibility

The Tunnello company decided to delegate to its chief information security officer (CISO), Mr Charlie, the role of ICS manager of the tunnel. He is assisted in this mission by the operating and maintenance managers.

Mrs. Alice, director of the company, retains the role of Qualified authority for information security accreditation (AQSSI / *autorité qualifiée pour la sécurité des systèmes d'information*).

3.2 Risk Analysis

As a portion of the components are class 3, Tunnello has mandated Audito, as a certified service provider, to assist it in carrying out its risk analysis.

This task will concern all of the ICSs. Tunnello and Audito will rely on Integro, and its knowledge of the architecture and of the devices deployed, in order to best understand the needs in terms of protection for the devices that are essential for the operation of the tunnel without risk for the drivers and the personnel, and to identify the vulnerabilities of the related devices.

The contract in addition calls for an annual review of this risk analysis.



3.3 Mapping

Tunnello decided to have a full inventory taken of the tunnel's ICS and of the devices that have access to it (in particular from the Millau station). This inventory covers the physical and logical standpoints. Tunnello has mandated Integro, in charge of maintenance for the system, to conduct this inventory and to keep it up to date. The latter, which is normally done at every modification, is reinforced with a review of all the class 3 devices (and therefore also class 2) at least once a year.

The mapping of the ICS is launched as far upstream as possible. It covers all the networks and makes it possible to ensure the completeness of the results. It is the source of diagram 2.5.

The documentation is available on paper in a dedicated premises, next to the Millau control room and in the Meyrueis PCC. It is also stored on two encrypted hard drives. Non-encrypted storage is tolerated for documents that show only class 1 devices.

3.4 Operator Training, Control and Certification

Training and certification


In the framework of its prospective management of employment and skills, Tunnello ensures that the operators have a level of training that is suitable for their position. In this framework, the company has decided to include a module on information system security awareness in the internal training cycle for new users.

This initial training is supplemented by certification for all the people that need to intervene on class 2 or 3 systems. This certification incorporates more in-depth awareness. The certifications are delivered for five years, and the training is reiterated during renewals. These certifications are carried out by a certified external organisation when they concern class 3 devices (and therefore also those of class 2).

Moreover, during the establishment of contracts for the maintenance portion, Tunnello verified with Integro that the training of operators for the latter, monitored as a qualified service provider in Integration and Specialised Maintenance in Cybersecurity, was not in disagreement with the training of its own personnel. A reminder on cybersecurity remains ensured by Tunnello during the welcoming of operators.

Control

In order to ensure a good level of monitoring for the operators, Tunnello has integrated the required information (identity, certifications where applicable, devices on



which the user can intervene) into its human resources information system (HRIS). The latter is supplemented with a branch dedicated to managing external operators: entries are created according to the declarations of the service providers, with a revalidation/extension of the accounts per quarter.

Tunnello transcribes the information coming from HRIS (identity, accounts, certification where applicable, devices on which Tunnello is authorised to intervene) into technical directories, one for class 1 and one for classes 2 and 3. Due the small number of people involved, Tunnello feels that manual management of the updates to the directories is acceptable, as the complexity of an automatic synchronisation mechanism is not justified.

Tunnello has asked Integro that, as much as possible, the devices refer to the technical directory of the same level for the management of the authorisations and of the accesses via the supervision mechanisms.

For class 3 devices (and therefore also for those of class 2) that cannot refer to the technical directory or that cannot log the accesses, Tunnello uses organisational measures in order to ensure control and traceability (see section 3.13).

3.5 Audits

The management of Tunnello decided to entrust Audito, certified audit supplier, with an annual audit contract for 5 years, on devices of class 2 and 3 of the industrial IS. These audits are carried out on coverage adapted to each class. As Audito is not specialised in industrial systems, it works with a certified service provider in this field, which is competent for the devices in place and independent of Integro in order to ensure objectivity for the audit.

The contract provides for the establishment of a formal action plan by the service provider in collaboration with the production teams. This action plan is then sent to the management of Tunnello for validation and integration into the company's strategic plan.

In order to limit the perimeter of the service described hereinabove, Integro has given responsibility, after validation from Tunnello, to an internal team dedicated to this type of activity, to ensure the audit of all or a portion of the class 1 devices during the changes in the architecture or the replacing of hardware.



3.6 Monitoring process

The technological monitoring must apply to the hardware as well as to the software present in the ICS. On a regular basis, a report must be remitted to the CISO (cf. measure 1) for information on the security level of the components.

As it does not have the resources or skills internally, the management of Tunnello has given Integro the responsibility of ensuring this monitoring in the framework of the maintenance contract for the system. To do this, Integro has taken out a subscription to the security bulletins of the manufacturers of each of the devices of the site, as well as to the security bulletins of its local CERT, CERT-FR¹.

For every 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.). Integro is also in charge of providing the CISO and the AQSSI with a table of the situation for information on the level of security of the components.

The contract provides for classes C2 and C3 maximum periods for updating in case of a vulnerability deemed to be critical (one week for stations and devices of the PCCs, one month for field devices), and these periods can be adjusted by the CISO.

Integro undertakes to make suggestions on changes that should be considered at the level of the ICS in order to be protected from new threats concerning all or a portion of the class 2 or 3 devices.

3.7 Business Resumption Plan and Business Continuity Plan

Through its nature, dependability imposes redundancy, wherever possible, of all of the devices required for the security of the users. This redundancy makes it possible to ensure a certain level of availability for the system, forming in fact the first bricks of the BRP and BCP.

For the approval of a road tunnel, it is as such requested that the operator provide a full security dossier, describing the management of various incident scenarios and the level of resilience of the components implemented.

In the present case, Tunnello, with the assistance of its service provider Integro, has set up redundancy of the PLCs in order to ensure operating continuity. The presence

¹Cf. www.cert.ssi.gouv.fr.



of a local control station, allowing for complete remote control of supervision, is also to be integrated into these plans.

Finally, the need for a BRP beyond the management of incidents is limited by the presence of a road that allows the tunnel to be bypassed when the latter is unavailable, as indicated in the “Classification” chapter of the first part and more particularly the scale of the impacts in terms of availability.

3.8 Emergency Modes

Physical switches of the “mushroom” type make it possible to trigger the vital functions manually (signalling, indication of the emergency exits, ventilation in smoke extraction mode), without going through the supervision consoles.

Integro has set up an administrator account that allows for local access on the various devices and is reserved for emergency situations. This account is protected by a password with sufficient complexity and is unique per device. These passwords are retained in sealed envelopes kept in vault in the PCCs. These administrator accounts can be used by an operator as well as by an integrator when they have access to the maintenance station and to the passwords in question.

Moreover, manual signalling devices (torches, horns, mobile signalling signs) can be accessed on the site and in the vehicles of the operators in order to be able to report a tunnel closing or guide drivers, including when it is not possible to control the ICS remotely.


The operations manager must ensure that what is required is done in case of wear and tear of these elements: replacing consumable items, battery recharges, replacing revealed passwords, etc.

Tunnello takes care of checking at least once a year for the presence and the good condition of these elements and the associated procedures.

3.9 Alert and Crisis Management Process

In the framework of the contract that binds it with its service provider Integro, Tunnello has set up the following processing mechanisms for the security incidents concerning the ICSs:

- Setting up of an organisation at several levels, with the Tunnello operators providing level 1 (qualification of the incident and the most accurate description



possible of the environment) and simple resolutions (replacing a bulb, resetting), the operators of Integro ensure levels 2 (updating, configuration) and 3 (engineering, problem management).

- Setting up of a ticket management tool allowing for monitoring of incidents and problems. The interventions coming from the monitoring process, carried out in accordance with section 3.6, are also logged here.
- Setting up of a “crisis unit” that can quickly bring together the competent people involved in case of need. The related procedures are logged on paper in the two control stations and at Integro. They are also made available to the authorities who may need to follow the roll ups from various sources.

In the framework of its security dossier, Tunnello must describe these crisis management processes. Likewise, an up-to-date list of the significant events that have occurred in the tunnel as well as the analysis of them must be updated. Tunnello is therefore part of this process as regards cybersecurity incidents.

Moreover, note that a major scale crisis will be managed by the intermediary of a public or administrative emergency plan (such as the Orsec System in France). This type of crisis however concerns the repercussions of a hardware and human incident, not just the aspects of cybersecurity of the ICS.

3.10 Network interconnections

Management information system

The network implemented by Integro does not have a connection with a management information system.

Public network

The network implemented by Integro does not have a connection with a public network, with the connection between the main control station and the site of the tunnel carried out via encrypted and authenticated tunnels. The latter is accomplished using a pair of qualified IPsec VPN gateways dedicated to the class under consideration. The flows transiting therein are moreover protected by qualified firewalls, which are also dedicated to each class, positioned on either side of the VPN tunnel.

These different VPNs are then transported over a dedicated line (segmentation via MPLS).



ICSs network

The control centers, on the one hand, and the field system, on the other hand, are considered as two separate systems within the same architecture. Qualified firewalls, redundant and separate, are therefore set up on either side of the connection in order to partition the two systems for each one of the classes (with C2 and C3 merged).

3.11 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 commands. In these terms, Supervision from the PCC at Millau forms a remote management mechanism.


However, this Supervision was integrated right at the start of the analysis, whether in the risk analysis or in the defining of classes. In addition, the connection between the PCC and the site of the tunnel is carried out through an encrypted and authenticated tunnel over a dedicated line (segmentation via MPLS), as indicated hereinabove in this chapter (cf. 3.10).

Integrating the security issues of ICSs right from the design phase, the architecture set up by Integro and Tunnello does not involve an administration network². Indeed, Tunnello deemed, after a preliminary study conducted during the project phase, that the costs and risks linked to this type of functionality was not justified due to the low frequency of the maintenance actions and the usual failure rate for these devices. The models of the various pieces of hardware consequently chosen in order to make it possible to limit the physical ports that authorise administrative or programming actions.

It is therefore in fact not possible to carry out remote maintenance or remote diagnostics beyond the information rolled up from the supervision and logging systems. Any maintenance has to be done by means of a **connection to a dedicated port** of the device from a mobile station which is also dedicated to maintenance and on which the dedicated tools are installed.

The geographical separation of these two functions (with Supervision being carried out from the PCC and maintenance from the tunnel) in fact imposes a physical separation

²Modifications to firmware, programs or the configuration are considered as administration tasks. In the absence of an administration network, these actions are therefore carried out as a direct connection with the devices.



between the stations that allow these two tasks to be carried out.

Remote management is provided from the stations located in the Milliau control station, with a supervision station (or several according to need) being dedicated to class 1 and a second dedicated to class 3 (and therefore also to class 2).

3.12 Surveillance and Intrusion Detection Methods

Logging

In order to meet the requirements of logging in the specifications supplied by Tunnello, Integro chose an infrastructure of the syslog type in order to ensure the centralisation of the logs for the security devices (firewalls and VPN gateways), the stations as well as for the devices that participate in the supervision function.

Through the architecture implemented, Integro provides a log server per class or class group (therefore one for C1 and one for C2+C3). The latter generate an overview report intended for the operations department, on a daily basis for class 3 (and therefore also for class 2 devices) and weekly for class 1.

At least once a month, an operator travels on site to conduct a systematic collection of the logs over all the devices that are not connected to the network.

Detection sensors


Tunnello decided to reinforce the protection of the most sensitive devices by setting up detection sensors.

The risk analysis (see section 3.2) indicates that the most sensitive point concerns the interconnection between the “control centers” and “field system” sets, particularly when the devices are of class 3. Indeed, the devices and the terms for management implemented for these two sets are relatively different.

Moreover, as the communication protocols on the “field system” portion cannot all be secured despite a careful choice of the devices, Tunnello feels that, in light of the risk analysis, an increased monitoring of these exchanges is necessary.

Because of this, a sensor is set up to monitor the exchanges between the two sets of class 3 (in the wide sense, i.e. also covering C2 in this case) by the intermediary of port mirroring downstream of the firewall, set up as described hereinabove (cf. 3.10).

A second sensor for detection is set up for controlling the exchanges that allow for the interconnection of the PLCs and fire detection on the field network.



The alarms generated by the supervision system are transmitted in real time to the operations team, with the particulars for taking this into account described in the framework of incident management (cf. 3.9).

Likewise, the alerts generated by the dedicated unit, and which correspond to the intrusions in the premises or cabinets under control, roll up via an appropriate differentiated mechanism. The particulars for taking them into account are also provided in the framework of incident management (cf. 3.9).

3.13 Intervention Management

Main principles

The management of certifications and the control principles were covered hereinabove in this chapter (cf. 3.4).

In order to ensure the operational aspects, Integro and Tunnello have set up a certain number of procedures.


It is first enacted that any intervention generates the creating of a ticket in the appropriate manager regardless of the devices concerned and the intervention. Tunnello considers that this ticket manager acts as a logbook. The ticket is filled in with the date and time, name of the user, purpose of the intervention, number of the seals removed and reinstalled where applicable (see further on). The ticket can be filled in beforehand when the intervention is planned (scheduled maintenance).

Access to the premises

When the user goes on site, he must report by telephone to the central control station at the beginning and at the end of the intervention in order to deactivate / reactivate the alarms³. If necessary, he must also recover the diagnostic and maintenance tools mentioned hereinbelow, which are kept at the secondary control station, and put them back at the end of the intervention.

As the ticket management tool has access to the information on the certifications and authorisations present in the technical directory, the operator present at the central control station has the possibility to refuse access (and not deactivate the alarms) to the user where applicable.

³The alarms are rolled up in real time and tracked in the two PCCs. Likewise, the video surveillance images are recorded and can be accessed for viewing at the level of the PCCs.



Tunnello has furthermore decided to use single-use numbered collars as seals when this is necessary.

In order to provide physical protections for class 3 devices (or class 2), Tunnello has provided, during the specification/design phase, and as agreed with Integro, 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 (or class 2) 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. In fact, the procedure also applies to class 1 devices when they are housed in the same premises or cabinets as a class 2 or 3 device.

The obligation to call the main control station is considered by Tunnello as a traceability mechanism that is sufficient for cabinets that concern video surveillance (class 1) when these 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, the keys for the dedicated cabinets are entrusted to the users in charge of these functions.

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 cover all possible cases, without any particular tolerance including for the tools for which the usage remains exceptional.

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.

3.14 Architecture diagrams

The list of complementary components, stemming as hereinabove from the main measures, is provided in the following table.

Class	Additional components
Class 1	<ul style="list-style-type: none"> - maintenance station for technical administration; - import secure data exchange (optional, not necessarily connected to the network); - centralised logging server (optional).
Class 3 (C2+C3)	<ul style="list-style-type: none"> - maintenance station for technical administration (portable, separate from the supervision station); - import secure data exchange (not necessarily connected to the network); - diagnostic and intervention tools dedicated to the site; - centralised logging server; - technical directory; - firewall; - VPN between sites; - SIEM solution (optional); - intrusion detection solution.

The technical architecture diagram of figure 3.1 represents a field network of class C2+C3 separate from the field network of class C1. Each network is independent and the networks are sealed between them.

The decontamination station is materialised by a PC and a secure USB key per class. This station is not connected to any supervision network. Each site independently has its own decontamination station.

In the case of updates, the decontamination station and the secure USB key are used in the following way:

- on the decontamination station, the operator files the software components into a dedicated directory referred to as “unsecured” (*input secure data exchange*);
- he then makes out a copy of the unsecured directory to a secure directory (*output secure data exchange*) by applying the means of decontamination, including the execution of an antivirus;
- from the output secure data exchange, the updates are then copied to the secure key (cf. the means for securing a USB key);
- the operator can apply the updates to each device using the secure key.

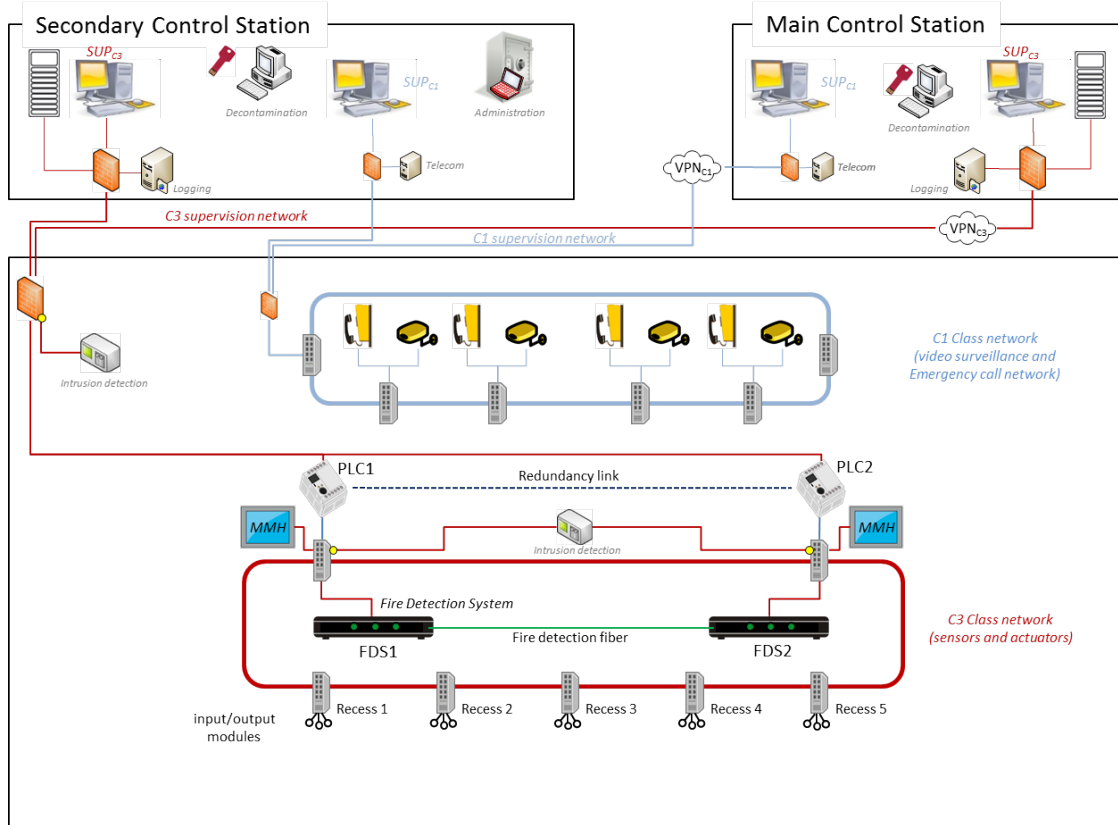


Figure 3.1: ICS - Secure technical architecture "C1, C2+C3"

Chapter 4

Breakdown of the detailed measures of the organisational type

As seen in the preceding chapters, the classification method allows to divide the ICS in three classes in terms of needs in cybersecurity.

Following the analysis of the main measures on the various segmentations considered, Tunnello decided to retain the solution based on the grouping of two of the three classes, namely C2 and C3 on one side and C1 on the other side.

The diagram in figure 4.1 shows the various logical components (including the application modules) that contribute to the securing of the ICS.

Refer to figure 3.1 in section 3.14 for the technical view of the architecture.

The purpose of this chapter is to decline the applicable set of the detailed directives, as well as the recommendations that Tunnello and Integro felt justified to apply. In order to facilitate the reading, the organisation of this chapter is similar to that of the ANSSI guide, dedicated to the detailed measures [ANS14b]. Moreover, it covers¹, in the spirit of completeness, the set of main measures described in the preceding chapter, in order to supplement them. The inclusion of certain parts of chapter 3 is therefore desired, with the objective of a complete summary concerning the retained configuration (i.e. “C1, C2+C3”).

Contrary to chapter 3, this chapter is voluntarily written with a point of view that is rather “project manager”, i.e. primarily the integrator Integro in this case, when the measure so allow.

¹This includes for example the taking into account of cybersecurity in the study phases or the justification of technical elements already present in figure 3.1.

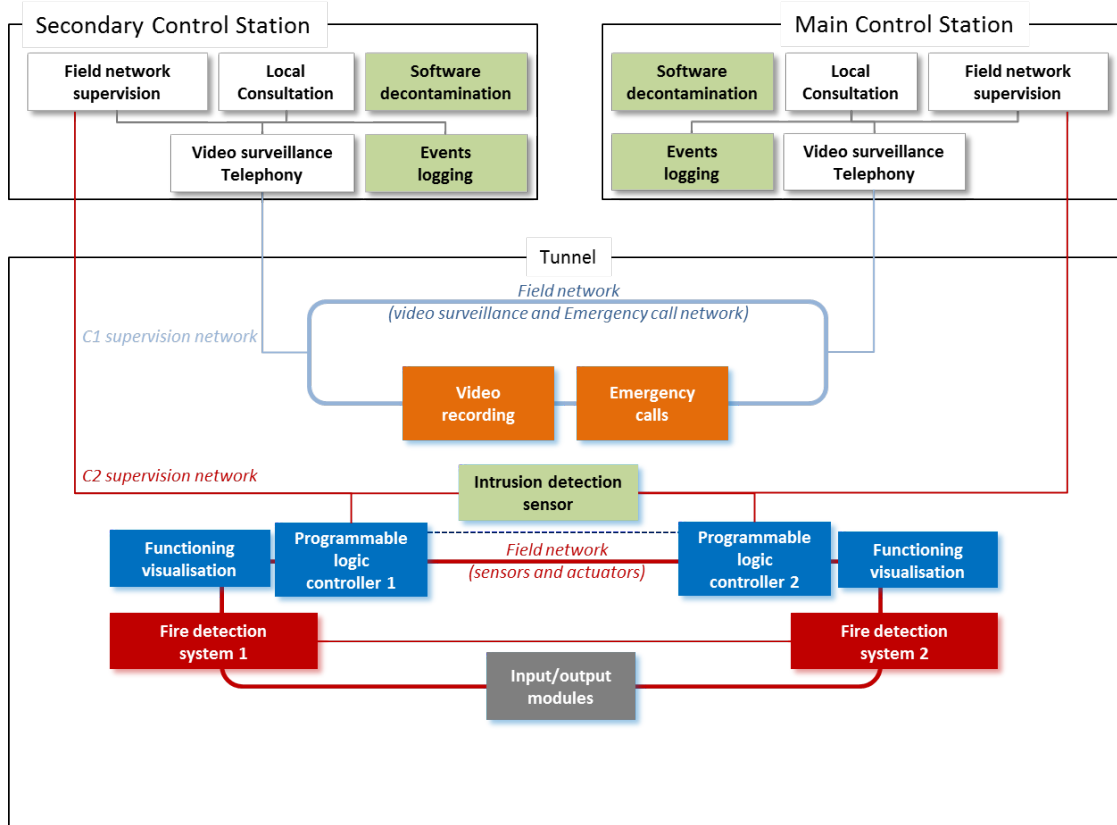


Figure 4.1: ICS - Logical architecture after conducting of the method

4.1 Knowledge of the ICS


4.1.1 Roles and responsibilities

Summary of the detailed measures

A chain of responsibility for cybersecurity shall be implemented, covering all ICSs.

The Tunnello company decided to delegate to its chief information security officer (CISO), Mr Charlie, the role of ICS manager of the tunnel. He is assisted in this mission by the operating and maintenance managers.

Mrs. Alice, director of the company, retains the role of Qualified authority for information security accreditation (AQSSSI / *autorité qualifiée pour la sécurité des systèmes*



d'information).

4.1.2 Mapping

Summary of the detailed measures

A complete inventory of the ICS must be produced.

Tunnello decided to have a full inventory taken of the tunnel's ICS and of the devices that have access to it (in particular from the Millau station). This inventory covers various points of view, including physical and logical architectures, the inventory of the roles and responsibilities and the flow matrix. Integro is mandated by Tunnello to take this inventory and to keep it up to date according to the particularities described hereinbelow.

The mapping of the ICS is launched upstream of this analysis and covers all networks. It must make it possible to ensure the completeness of the results. It is the source of the diagrams of figures 4.1 and 3.1.

It is requested that Integro update the inventory and the map at each modification, in liaison with the data of the CMMS (computerised maintenance management system). Integro shall also conduct a review of all of the devices once a year.


The documentation is available on paper in a dedicated premises, next to the Millau control room and in the Meyrueis control room. It is also stored on two encrypted hard drives.

4.1.3 Risk Analysis

Summary of the detailed measures

ICSs shall be subject to a detailed risk analysis using a method chosen by the responsible entity.

As at least one component is of class 3 regardless of the configuration retained, Tunnello has mandated Audito, as a qualified service provider, to assist it in carrying out its risk analysis. During this task, that will cover all of the ICSs, Tunnello and Audito will rely on Integro, and its knowledge of the deployed devices, to best understand the



objectives of the main assets and their operation, and to identify the vulnerabilities of the support assets.

The contract in addition calls for an annual review of this risk analysis.

4.1.4 Back-up Management

Summary of the detailed measures

A backup policy must be set up in order to ensure protection for important data and configurations. This policy must also comprise regular restoration tests and must not call the partitioning between the classes into question. The backup must in addition be based on a suitable infrastructure.

Integro has set up a backup infrastructure dedicated to the tunnel for the backing up of the log servers and the various stations. These undergo a full backup every week and a differential backup every day.

For the devices of the ICS, the procedures stipulate that any modification to the configuration or update must be followed by a manual backup. The backup policy specifies that the backups retained must cover the last five modifications and the last three months.


4.1.5 Documentation Management

Summary of the detailed measures

A classification of the documentation must be done in a coherent manner for each class. The storage and access to the documentation must be done in a suitable manner, in such a way that the users can have access to it in accordance with their need to know it. A review process must be provided in a global manner.

All of the documents are grouped together on an office station that is disconnected from the rest of the IS and made available to the users. Each user can consult only the documents that concern the devices on which he is authorised to intervene.

In addition, a hard copy of the most critical (and required including in the case of service shutdown of the documentation station) documents is retained in a safe in the secondary control station. This concerns for example the documentation required for



restarting the IS after a service shutdown, whether voluntary or not, possibly useful information coming from the support contracts, etc.

This documentation station is included in the backup policy: as it is a station that is disconnected from the network, the backup is provided manually and managed according to the same procedures as for network devices.

The operational management also provides in its planning one half-day per year dedicated to checking the documentation and more particularly the proper updating thereof.

4.2 User Control

4.2.1 User Management

Summary of the detailed measures

Class 3 requires the setting up of procedures for managing users, their skills and their hardware, as well as the management of accounts and the associated rights. This procedure can be unique and transversal. Through transitivity, this procedure can easily be extended over class 1, even if this is only optional.

Class 3 also imposes an annual review of the users and their rights.

In order to ensure a good level of follow-up to the users, Tunnello has integrated the required information (identity, level of certification where applicable, devices on which the user can intervene) into its human resources information system (HRIS). The latter is supplemented with a branch dedicated to managing external users: entries are created according to the declarations of the service providers, with a re-validation/extension of the accounts per quarter.

Tunnello transcribes the useful information of the HRIS (identity, accounts, certification where applicable, devices on which the user is authorised to intervene) into technical directories (for the configuration retained, one for classes 2 and 3 and one for class 1).

Due to the small number of people involved, this transcription is carried out by creating the accounts manually.

4.2.2 Awareness and training

Summary of the detailed measures

All users shall be certified and controlled. The cybersecurity training included in the certification must be ensured by service providers that are qualified as Integration and Specialised Maintenance in Cybersecurity or lacking this, service providers that comply with the requirements' reference documents.

In the framework of its prospective management of employment and skills, Tunnello ensures that the operators have a level of training that is suitable for their position. In this framework, the company has decided to include a module on information system security awareness in the internal training cycle for new users.

Moreover, in order to meet the contractual requirements set up by Tunnello, Integro, a qualified service provider, ensures that its users have a good level of training. It also ensures, as a precaution, that this training does not contain any major disagreement with the one received by the Tunnello personnel. A reminder on cybersecurity remains ensured by Tunnello during the security welcoming of users.


The initial training for users gives rise to a certification delivered for 5 years, with the training being reiterated when there is a renewal of personnel. These certifications are carried out by a certified external organisation when they concern class 3 devices (and therefore also those of class 2), and can be managed internally for class 1 devices.

Finally, the Integro employees are prohibited by Tunnello from any intervention on class 3 devices (and class 2) before their certification is effective, with a nominative derogation possible for internal operators in the process of certification when the intervention is supervised by an authorised operator. This prohibition is in fact also valid for the other subcontractors and Tunnello's own operators.

4.2.3 Intervention Management

Summary of the detailed measures

In addition to the setting up of procedures in order to supervise the interventions, class 3 imposes that the company have all of the tools and devices required for the various interventions on the ICS, including the specific diagnostic devices.



Any intervention generates the creating of a ticket in the appropriate manager regardless of the device concerned and the intervention, with Tunnello considering that this manager acts as a logbook. The latter is filled in with the date and time, name of the user, purpose of the intervention, number of the seals removed and reinstalled where applicable (see further on). The ticket can be filled in beforehand when the intervention is the object of scheduled maintenance.

With regards to the hardware means for allowing the intervention on the devices, the specifications issued by Integro with its own partners and suppliers in the framework of this contract 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, without any particular tolerance including for the tools for which the usage remains exceptional.

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.

4.3 Integration of cybersecurity in the ICS life cycle


4.3.1 Requirements in contracts and specifications

Summary of the detailed measures

Class 3 imposes the formalising right from the specifications of a list of expected requirements, preliminary analysis documents and a test plan in the aspects concerning cybersecurity.

The purchasing procedures in effect within Tunnello indicate that any call for tender for studies impacting the ICSs must comprise a section on the cybersecurity of these systems, which in particular includes the directives and recommendations presented in the guide of the detailed measures (without however being limited to this list). Tunnello decided to generalise this section to all of its calls to tender, regardless of the class of the devices concerned, with only the weighting of this criterion varying according to whether it entails a class 1 device or a higher class.

The call for tender concerning the creation of the system equipping the tunnel is therefore provided with such a section, upstream of the design and specification phases.



Moreover, Mr Charlie, as CISO, is designated as the point of contact for cybersecurity. He therefore ensure that the specifications include a confidentiality clause if needed, as well as compliance with the rules of cybersecurity right from the project phase (traceability, security assurance plan, auditability, use of a secure development environment).

4.3.2 Integration of cybersecurity in the specifications phases

Summary of the detailed measures

The operations that are not necessary for conducting must be done on a separate IS. The design in addition integrates protection of the configuration and the management of vulnerabilities. The hardware and service providers must be certified.

The purchasing procedures in effect within Tunnello indicate that any call to tender for studies impacting the ICSs must comprise a section on the cybersecurity of these systems, which in particular includes the directives and recommendations presented in the guide of the detailed measures (without however being limited to this list).

The call for tender concerning the specifications of the system equipping the tunnel was therefore provided with such a section, upstream of the design phase.

4.3.3 Integration of cybersecurity in the design phases

Summary of the detailed measures

The complexity must be reduced as much as possible, and the characteristics in terms of cybersecurity must be taken into account in the choice of the hardware. In particular, the capacity to separate administrators and users must be taken into account as early as the design phase.

The purchasing procedures in effect at Tunnello indicate that any call for tender that impacts the ICSs must comprise a section on cybersecurity of these systems. The call for tender concerning the design of the system equipping the tunnel is therefore provided with such a section.

4.3.4 Audits and cybersecurity tests

Summary of the detailed measures

Regular audits shall be implemented and must be carried out at least once a year. These audits should be carried out by independent, certified service providers.

The management of Tunnello decided to entrust Audito, certified audit supplier, with an annual audit contract for 5 years, on devices of class 2 and 3 of the industrial IS. As Audito is not specialised in industrial systems, it works with a certified service provider for maintenance in the field, which is competent for the devices in place and independent of Integro in order to guarantee objectivity for the audit.

The contract calls for the establishing of a formal action plan by the service provider in collaboration with the production teams. This action plan is then transmitted to the management for validation and integration into the Tunnello's IS change plan.

4.3.5 Operational transfer

Summary of the detailed measures

The systems shall be approved and require authorisation prior to entry into service.

Integro is in charge of setting up the approval file, in accordance with the procedure described in the appropriate ANSSI guide [ANS14]. The file includes the risk analysis and inventory, as well as a list of threats and an analysis of the protective measures provided for this purpose. It also includes the initial report on the audit conducted by Audito, carried out such as described in the preceding section and used by Integro for its improvement plan.

The file is presented at the ICS approval commission. In particular, the AQSSI takes the responsibility of accepting the residual risks detected before any putting into service.

4.3.6 Management of modifications and changes

Summary of the detailed measures

Updates must be tracked.

During an update, it is possible to compare the current version and the version to be installed in order to be sure that all the changes are necessary. Moreover, an integrity check on the programs and configuration files must be carried out during the execution. Finally, the tests are carried out in a dedicated environment.

In the specifications, Tunnello requested that the problems concerning integrity and authenticity be taken into account, ideally via a binary signature by the device supplier or the integrator when the latter has intervened in order to customise them.

Although it does not in the end have the infrastructure making it possible to sign all the binaries, Integro was nevertheless considered as sufficiently trustworthy when the contract was awarded, because of its status as a qualified service provider.

Tunnello and Integro have therefore agreed to a procedure that favours a hash calculation of all the files delivered when passing through the secure data exchange of the decontamination station (cf. 3.14), with a visual check of the hashes provided through a different means of distribution of the binaries (fax, hard copy, and signed email are acceptable means).

Integro must ensure the integrity of all the files provided by the manufacturer. If this procedure is systematically implemented for modifications concerning class 2 and 3 devices, class 1 devices can be managed in “best effort” mode.

Moreover, the integrator supplies a differential between the versions for the code for which he has control and for the modifications made to the configurations. He contractually undertakes to supply a version note that fully covers (but prioritised whenever possible) all of the modifications made to the files.

4.3.7 Monitoring process

Summary of the detailed measures

A monitoring process must be set up in order to keep informed:

- of the change in the threat and attack techniques;
- of vulnerabilities identified in the products and technologies used on the ICSs;
- of developments in protection mechanisms.

The technological monitoring must apply to the hardware as well as to the software present in the ICS. On a regular basis, a report must be remitted to the AQSSI (cf. measure 1) for information on the security level of the components.

As it does not have the resources or skills internally, the management of Tunnello has given Integro the responsibility of ensuring this monitoring in the framework of the maintenance contract for the devices. To do this, Integro has taken out a subscription to the security bulletins of the manufacturers of each of the devices, as well as to the security bulletins of CERT-FR².

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.).

Finally, Integro is in charge of providing the AQSSI and the CISO with a table of the situation for information on the level of security of the components.

Integro furthermore undertakes to make suggestions on changes that should be considered at the level of the IS in order to be protected from new threats concerning all or a portion of the devices.

²Cf. the site www.cert.ssi.gouv.fr.

4.3.8 Obsolescence Management

Summary of the detailed measures

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

Tunnello has required right from the specifications the contractual obligation to be informed of the end of the service life of the devices deployed as soon as the end-of-sale is known and at least three years before the actual end-of-life.

Moreover, it is the responsibility of Integro to ensure that it has sufficient access with the support services of the various manufacturers in order to ensure the maintenance of devices deployed until the actual stoppage of the support.

4.4 Physical security and access control for premises

4.4.1 Access to the premises


Summary of the detailed measures

An access policy must be set up, making it possible to ensure that only those people who have keys and access codes need them and are internal users (except if it is possible to track the access of external users). This therefore implies that a service provider must not intervene alone, except if their access can be tracked.

Accesses must be tracked, able to be audited and protected by an alarm and video surveillance.

When the user goes on site, he must report by telephone to the central control station at the beginning and at the end of the intervention in order to deactivate / reactivate the alarms. If necessary, he must also recover the diagnostic and maintenance tools (see "Intervention management" in the section), which are kept at the secondary PCC, and put them back at the end of the intervention.

As the ticket management tool has access to the information on the certifications and authorisations present in the technical directory, the operator present at the central



control station has the possibility to refuse access (and not deactivate the alarms) to the user where applicable.

In order to provide physical protections for class 3 devices (and therefore also class 2), Integro and Tunnello have provided during the specification/design phase, to set up access control to the premises via an individual badge, an alarm for the main and secondary control stations. These measures are furthermore supplemented by the video surveillance present in the tunnel. The security policy reserves the delivery of these badges only to internal users.

4.4.2 Access to devices and cabling

Summary of the detailed measures

Servers must be placed in protected premises as described hereinabove. Sensitive devices of the industrial IS must be placed under key and no network sockets must be accessible in the public areas.

The opening of cabinets containing sensitive devices of the industrial IS must be tracked (at least with alarms and seals).

In addition to the points concerning access to the premises, Tunnello has decided to use single-use numbered collars as seals when this is necessary.

The premises and cabinets that are not protected by access control but which house class 2 or 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. In fact, the procedure also applies to class 1 devices when they are housed in the same premises or cabinets as a class 3 (or class 2) device.

The obligation to call the main control station is considered by Tunnello as a traceability mechanism that is sufficient for cabinets that concern class 1 devices 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.

The video surveillance cameras are moreover installed in anti-vandalism caissons with seals.

4.5 Incident response

4.5.1 Business Resumption Plan or Business Continuity Plan

Summary of the detailed measures

Business Resumption Plans or Business Continuity Plans must be implemented and tested at least once a year.

Through its nature, dependability imposes redundancy, wherever possible, of all of the devices required for the safety of the users. This redundancy makes it possible to ensure a certain level of availability for the system, forming in fact the first bricks of the BRP and BCP.

Before the commissioning of a road tunnel, it is as such requested that the operator provide a full security dossier, describing the management of various incident scenarios and the level of resilience of the components implemented. In the present case, Integro has set up redundancy for PLCs in order to ensure operating continuity, in accordance with the requirements of Tunnello.

The presence of a local control station that allows for full remote control of supervision, is also to be integrated into these plans, as well as the existence of a data backup that is checked on a regular basis (see “Back-up management” in section 4.1.4).


Finally, the need for a BRP beyond the management of incidents is limited by the presence of a road that allows the tunnel to be bypassed when the latter is unavailable, as indicated in the chapter that describes the impacts in terms of availability.

4.5.2 Degraded modes

Summary of the detailed measures

Emergency intervention and degraded mode operation procedures must be provided. These procedures must maintain traceability of the actions.

Physical switches of the “mushroom” type make it possible to trigger the vital functions manually (signalling, indication of the emergency exits, ventilation in smoke extraction mode), without going through the supervision consoles.



Integro has set up a technical administrator account that allows for local access on the various devices. This account is protected by a password with sufficient complexity and is unique per device. These passwords are retained in a sealed envelope placed in the safe of each one of the control stations.

Moreover, manual signalling devices (torches, horns, mobile signalling signs) can be accessed on the site and in the vehicles of the users in order to be able to report a tunnel closing or guide drivers, including when it is not possible to control the ICS remotely.

The operations manager must ensure that what is required is done in case of wear and tear of these elements: replacing consumable items, battery recharges, replacing revealed passwords, etc.

Tunnello takes care of checking at least once a year for the presence and the good condition of these elements.


4.5.3 Crisis Management

Summary of the detailed measures

Crisis management procedures must be set up in accordance with directives D.118 to D.120 of [ANS14b]. These procedures must be tested every year.

In the framework of the contract that binds it with its service provider Integro, Tunnello has set up the following processing mechanisms for the security incidents concerning the ICSs:

- Setting up of an organisation at several levels, with the Tunnello operators providing level 1 (qualification of the incident, including the most accurate description possible of the environment and simple resolutions such as replacing a bulb, resetting, etc.), the operators of Integro levels 2 (updating, configuration) and 3 (engineering, problem management).
- Setting up of a ticket management tool allowing for monitoring of incidents and problems. The interventions coming from roll ups in the monitoring process are also logged here.
- Setting up of a “crisis unit” that can quickly bring together the competent people involved in case of need. The related procedures are logged on paper in the



two control stations and at Integro. They are also made available to the *direction départementale de l'équipement* (french public road administrative agency) who may need to follow the roll ups from various sources.

These processes of operational management for incidents and the names of the people to be contacted in case of emergency are forwarded to the cybersecurity authority.

Moreover, note that a major scale crisis will be managed by the intermediary of a public or administrative emergency plan (such as the ORSEC System in France). This type of crisis however concerns the repercussions of a hardware incident, not just the aspects of security of the ICS.

Chapter 5

Breakdown of the detailed measures at the technical level

Following on from the preceding elements, this chapter describes a set of possible choices as well as their implementation.

5.1 User authentication: logical access control

5.1.1 Account Management

Summary of the detailed measures


Users must use individual accounts, which are deleted when they leave, with generic accounts being prohibited except in a significant constraint. Administrative accounts or those with privileges must be protected with authentication that is separate from that of standard accounts. Roles will be set up in order to ensure that the rights correspond strictly to the needs. A local or centralised review of the accounts and associated rights must be organised every year.

Integro configures the components that are in the control stations so that they refer for authorisation management to the technical directory of their level. Access logging is also set up.

For the class 3 devices of the control stations that cannot connect to the technical directory or that cannot log the accesses, Tunnello uses organisational measures in order to ensure control and traceability (see “Access to the premises” and “Access to devices”).

Outside of the control stations, individual accounts are set up for ICS devices when this is possible, with the generic accounts being deleted by default, or deactivated when it is not possible to delete them.

As the tunnel is of a relatively small size, Tunnello has made the decision to manage these accounts manually over all the devices. Intervention on site is therefore to



be planned within the framework of the arrival/departing circuits of personnel who provide intervention on the site.

5.1.2 Authentication management

Summary of the detailed measures

The devices cannot be accessed until after an authentication process following a mechanism that protects the password. Strong authentication (with multiple factors) is to be favoured for the most exposed devices.

By default, compensatory measures, for example perimeter or organisational measures, must be implemented in order to make it possible to achieve an equivalent level of protection.

The connection between the two control stations is based on an encrypted tunnel over an MPLS connection, as detailed hereinafter in section 5.2, paragraph “Internet access and interconnections between remote sites”. This tunnel is authenticated via a certificate, which Tunnello and Integro consider to be a sufficient level of protection for this connection.

For the ICS, the technical administrative stations and the supervision stations, the individual accounts use strong authentication (chip card and certificates) by connecting to the technical directory as a reference base. The certificates in question are managed by means of a PKI built according to the regulations.

Finally, regarding the PLCs that cannot rely on the technical directory, the generic administrative account is used with a sufficiently robust password (in accordance with the ANSSI guide [ANS12]), with an updating of the password by an internal user at the end of each maintenance intervention.

5.2 Securing the ICS architecture

5.2.1 Partitioning ICSs

Summary of the detailed measures

The industrial IS has to be broken down into coherent zones that are physically partitioned, with filtering between zones. The administration must in addition be carried out through the intermediary of a dedicated network that is not connected to Internet. The unidirectionality of the flows between C3 and the lower classes is provided by a hardware data diode¹

The control centers, on the one hand, and the field system, on the other hand, are considered as two separate subsystems within the same architecture. Qualified firewalls, redundant and separate, are therefore set up in order to partition them for each one of the classes (with C2 and C3 merged).

The C1 system and the C2+C3 system are not interconnected in the retained architecture.

5.2.2 Interconnection with the MIS

Summary of the detailed measures

The interconnection has to be protected by a firewall and the authorised flows have to be reduced to a minimum. A hardware data diode has to protect the unidirectional flow from C3 to the management IS.

The network implemented by Integro does not have a connection with a management information system (MIS).

¹Reference can be made to appendix A.9 for more precision.

5.2.3 Internet access and interconnections between remote sites

Summary of the detailed measures

Protection for the exchanges between remote ICSs must be guaranteed. Each site is in addition protected by a firewall. Direct exchanges with a public network are prohibited.

The management of the ICS, i.e. the ability for example to modify the set parameters, is part of the supervision process, which, for recall, covers the capacities for viewing, logging and operation. Because of this, there is a remote management process in the very definition of the needs in that the ICS has to be supervised from the main control station, located in Millau.

In order to ensure the security of this remote management, the connection between the main control station and the site of the tunnel is done through an encrypted tunnel of the IPsec type authenticated by certificate², with the whole transiting over a dedicated line (segmentation via MPLS).

Moreover, the architecture implemented by Integro does not have a connection to Internet or any other public network, with the connection between the main control station and the site of the tunnel carried out via encrypted tunnel over a dedicated line (segmentation via MPLS).


5.2.4 Remote Access

Summary of the detailed measures

Remote maintenance is prohibited from the outside of C3. When it cannot be avoided, it can then only be implemented by integrating it into C3 and by applying the rules with respect to distributed ICSs (therefore not from a public network, partitioned and dedicated administration station, etc.).

After a preliminary study conducted during the project phase, Tunnello feels that the low frequency of the maintenance actions and the normal failure rate for these devices does not justify the costs and risks linked to this type of functionality: as such, the

²Concerning the setting up of an IPsec tunnel, reference can be made to technical note [ANS15].



architecture set up by Integro does not include an administration network. The models of the various pieces of hardware were consequently chosen in order to make it possible to limit the physical ports that authorise administrative or programming actions.

It is therefore in fact not possible to carry out remote maintenance or remote diagnostics beyond the information rolled up from the supervision and logging systems. Any maintenance has to be done by means of a local connection to the device with a mobile station dedicated to maintenance on which the dedicated tools are installed.

A station is dedicated to class 1 and another to classes 2 and 3.

5.2.5 Distributed ICSs

Summary of the detailed measures

VPN gateways and firewalls must be installed at the ends of the connections. Dedicated connections are systematically used.

Tunnello and Integro have decided to manage the remote main control center, in the form of a remote management point rather than as a distributed ICS.

5.2.6 Wireless communication

Summary of the detailed measures

A detection sensor must be implemented at the interconnection with the wired network and its centralised roll ups are monitored in real time. This type of communication is prohibited in case of a significant constraint in terms of availability.

The network implemented by Integro does not possess any wireless communication equipment.

5.2.7 Protocol security

Summary of the detailed measures

The unsecured protocols must be deactivated.

Integro has selected devices that make it possible to deactivate the unsecured protocols for supervision and administration, other than direct connection to the device.

5.3 Securing devices

5.3.1 Configuration hardening

Disabling unnecessary accounts

Summary of the detailed measures

On the devices, the default accounts, unused ports and services that are not indispensable are deactivated.

On the user stations, the debugging and test tools and unused ports and services that are not indispensable are deactivated.


For the applications of the ICS, the comments and mnemonics are not loaded on the devices.

As indicated in the section concerning their management, individual accounts are set up for ICS devices when this is possible, with the generic accounts being deleted by default, or deactivated when it is not possible to delete them. Where applicable, an intervention on site to delete the account that has become obsolete is also provided for in the framework of the departing circuit for personnel.

Strengthening protection

Summary of the detailed measures

Applications should run with only the privileges that are absolutely necessary. For in-depth defence, the devices must protect access to their hardware resources and only authorised applications can be executed.



During the writing of its specifications, Tunnello explicitly requested that the devices respect the following criteria:

- there is a procedure for execution via a white list on the ICS;
- the services present on the servers have to be executed with a dedicated account, not as an administrator.

Compliance with these requirements was taken into account when choosing the devices deployed.

The specifications also call for the hardening of the various user stations. It is in particular provided for the maintenance station to have a logical access control (no “AutoLogin”) and full encryption for the hard drive. Moreover, its updates and available software changes follow the same rules as those for devices (cf. the following section).

Integrity and authenticity


Summary of the detailed measures

The procurement process must be controlled as much as possible and in particular includes an integrity control of the critical elements. This control must be based on a signature process of the elements and a comparison of the software versions delivered and put into the history.

In the specifications, Tunnello requested that the problems concerning integrity and authenticity be taken into account, ideally via a binary signature by the device supplier or the integrator when the latter has intervened in order to customise them.

Although it does not in the end have the infrastructure making it possible to sign all the binaries, Integro was nevertheless considered as sufficiently trustworthy when the contract was awarded, because of its status as a qualified service provider.

Tunnello and Integro have therefore agreed to a procedure that favours a hash calculation of all the files delivered when passing through the import secure data exchange (cf. 3.14), with a visual check of the hashes provided through a different means of distribution of the binaries (fax, hard copy, and signed email are acceptable means). Integro must ensure the integrity of all the files provided by the manufacturer (cf. the section “Management of modifications and changes”).



In addition, the comparison between the versions of the software delivered by Integro and the version put into the history by Tunnello, makes it possible to ensure the integrity of the scripts and the binaries deployed on the components of the tunnel. The previous versions are put either into history on the supervision server, or on the decontamination station, or on a PC in a secure cabinet inside the PCC.

Concretely, the import secure data exchange is a machine, connected to the Internet, of which the only functions are the downloading of updates and the verification of their signatures, before placing the latter on a USB key. The secure data exchange is shared on the main PCC, but a movable media is dedicated for each field network.

To do this, this machine uses an operating system of the “liveCD” type, which as such prevents persistent attacks (rebooting the station is sufficient to resume with a “clean” system, as the antivirus database is updated as soon as the station boots up). Integro supplies, in the framework of the maintenance contract, regular updates for the “liveCD” distribution.

5.3.2 Vulnerability management

Summary of the detailed measures

Known vulnerabilities that are not corrected (or residual vulnerabilities) must be documented, as well as the remedial measures implemented in order to limit the exposure or impact.

A management plan for the vulnerabilities and patches must be implemented, establishing in particular the priorities and a follow-up indicator for the actual deployment of the patches.

As it does not have the resources or skills internally, the management of Tunnello has given Integro the responsibility of ensuring this monitoring in the framework of the maintenance contract for the devices.

Integro in particular undertakes to provide advice on changes that should be considered at the level of the IS in order to be protected from new threats, as well as on the updates and remedial means. (cf. “Monitoring process”).

5.3.3 Connection interfaces

Removable media

Summary of the detailed measures

A management policy for removable media must be implemented, including a decontamination station and the making available of media dedicated to the industrial IS.

The ports that are not necessary for removable media are deactivated. The decontamination station is replaced via a secure data exchange in a controlled zone.

The ICS security policy of Tunnello imposes that the only removable media accepted are dedicated USB keys that can be used in the road tunnel or in the control stations. In addition each piece of media is dedicated to a given class in order to prevent the spreading of any contamination. The media involved is identified in such a way as to prevent any error.

In order to allow for an updating of devices, Integro has set up a “hardened” station, i.e. for which the security is reinforced. The role of the latter is to ensure the innocuousness of the documents that are copied or imported from another media before they are placed on the USB keys. This station is the only device to which all the dedicated USB keys of the tunnel can connect, independently of the class. It is however entirely disconnected from the networks used by the control stations or in the tunnel.


Network access points

Summary of the detailed measures

Management for the network access points must be set up (identification, deactivation if necessary) and a management of alerts must be set upon an event.

The network access points can be accessed only in the controlled premises and in the sealed cabinets.

During the installation of the devices of the tunnel, Integro documented the use of the ports of the various switches, in the framework of the inventory of the system.



The latter is regularly updated (see hereinabove the section that is devoted to it) and Integro is required to deactivate ports that are not documented.

In addition, in order to ensure good identification of the various classes, Integro has implemented a differentiation in the colours of the Ethernet cables (red for connecting class C3 devices – and therefore also C2 –, green for those of class C1).

In the absence of a dedicated administration network (the network devices are managed by means of a local connection), the roll up for alerts is based on arming the cabinets with an alarm, in accordance with what is described in the sections that address the monitoring of the interventions and the protection of the premises.

5.3.4 Mobile devices

Summary of the detailed measures

A management of the mobile devices must be set up and the use of personal mobile terminals is prohibited. When the mobile contains sensitive data, it must be encrypted.

The mobile devices used must be dedicated to the industrial IS and to the site, including those of the service providers.

Two laptop computers dedicated to the tunnel are made available in order to connect to the devices and to ensure the maintenance thereof, as indicated in the section devoted to remote access hereinabove in this chapter, as well as in section 3.11. They are retained indefinitely on the site. One is dedicated to class 1 and another to classes 2 and 3.

Outside of these maintenance stations, Tunnello nor its subcontractors use mobile devices (smartphones, tablets, etc.) in order to connect to the various networks present in the tunnel or in the control stations. Portable telephones are reserved for voice/SMS use (“data” connections are still tolerated for related uses but must not in any circumstances allow access to the IS of Tunnello or Integro).

5.3.5 Security for programming consoles, engineering stations and administrative workstations

Summary of the detailed measures

Management of the administration stations, engineering stations and programming console must be set up. Administrative workstations must not be used for monitoring ICSs.

Through the organisation set up, only the supervision stations are implemented in the PCCs.

As the site does not have a technical administration network, this latter task cannot be carried out from the PCC by the supervision stations. It is possible only thanks to the mobile maintenance stations described hereinabove, which are required in order to obtain administrator access locally for a device. Technical administration is therefore in fact separate from the supervision activity and complies with the segmentation of the system (class 1 on one side, classes 2 and 3 on the other). Finally, as the engineering phase is carried out in the premises of Integro, there is also a separation.

The security of these various stations also depends on updating them on a regular basis. However, this action can be challenged by the need to retain a given version of the operating system for stations for the tools of the ICS, as these two have different life cycles.

The maintenance contract for devices therefore also covers maintenance for the associated tools such as the supervision and engineering software (as indicated in section 4.2.3), which allows Tunnello to have tools that are compatible with an up-to-date operating system.

Integro is therefore in a position to provide updates for workstations and servers on a quarterly basis, with the maintenance stations updated at least once a year (for example during the annual visit for updating the documentation - cf. section 4.1.5).

The recovery of the updates for stations moreover goes through a process similar to firmware updates described in section 5.3.1.

5.3.6 Secure development

Summary of the detailed measures

The development must be carried out in a dedicated environment, following the rules for secure development. The code must be analysed and audited.

Integro undertakes that this development is done in accordance with best practices. A version manager is in particular implemented by Integro in order to ensure the follow-up of the development of patches, the ability to roll back to any delivered version whatsoever and to check the integrity of it. This version manager covers both the sources and the binaries delivered.

Integro has furthermore provided an equivalent commitment from its suppliers.

5.4 ICS Monitoring

5.4.1 Event logs

Summary of the detailed measures

An event management policy must be set up, including a follow-up of parameter modifications and log centralisation. This policy must also include a regular analysis of the data collected.

During the design phase, Integro opted for an infrastructure of the syslog type in order to ensure log centralisation for the security devices (firewall and VPN gateways), the stations and also for devices that support the centralised collection functions for logs in the framework of the supervision function.

At least once a month, a user travels on site to conduct a systematic collection of the logs over all the devices that are not connected to the network or do not allow for the centralisation of logs.

Through the architecture implemented, Integro provides a log server for class 1 and one for the "C2+C3" class. The latter generate an overview report intended for the operations department, on a daily basis for class 3 and weekly for class 1.

5.4.2 Detection Methods

Summary of the detailed measures

Intrusion detection methods shall be implemented on the perimeter of ICSs and at points identified as critical. The detection methods used should be certified.

Integro decided to reinforce the protection of the most sensitive devices by setting up certified detection sensors.

Its risk analysis on this particular point reveals that the most sensitive point concerns the interconnection between the (sub)systems of class 3 “control stations” and “tunnel”. Indeed, the devices and the management methods implemented in these two systems are relatively different, with the “control station” portion being provided for daily use by the users, with stations that can have advanced interfaces and various document inputs (via an import secure data exchange), while the “tunnel” system is based on automated operation, with the only incoming information passing through the interconnection mentioned hereinabove (other than maintenance). Because of this, a sensor is set up to monitor the exchanges between the two sets of class 3 (in the wide sense, i.e. also covering C2 in this case).

The risk analysis also shows that the communication protocols on the “field system” portion cannot all be secured despite a careful choice of the devices, Tunnello feels that an increased monitoring of these exchanges is necessary. A second sensor for detection is therefore set up for monitoring the exchanges that allow for the interconnection of the PLCs and fire detection on the field network.

The sensors are set in place by the intermediary of port mirroring downstream of the firewall set up beforehand (cf. 3.10), as well as on the switches that allow for the interconnection of the PLCs and fire detection on the field network.

The alarms are transmitted in real time to the operations team, with the particulars for taking this into account provided for in the framework of incident management (cf. 3.9).

Appendix A

Description of the components

A.1 Operating recess

A recess is a technical room located inside the tunnel. Recesses are installed about every 200 m.


Each recess contains one or several offset input/output modules that concentrate the connections of devices in the vicinity. The latter are of two types:

- **Actuators**, which are physical elements that, receiving a command from the control portion, triggers a useful physical action. In the case of the tunnel, the actuators are computer-controlled and the commands transit via the field networks.
- **Sensors** are devices that make it possible to measure a physical magnitude and to transform it into a usable magnitude. In the case of the tunnel, the magnitudes are digitised and are transmitted in a computerised manner to the control portion via the field networks.

Each recess includes, in addition to this or these module(s), one or several switches that make it possible to connect the devices to the field network, with each switch being connected to a single network. In the case of the tunnel, the field networks, which connect the various recesses with the local PCC, are of the Ethernet type. 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.

A.2 Control center

The control center, or PCC for “*poste de contrôle-commande*”, concentrates all of the supervision activity for the field networks. All of the information rolls up to the servers of the ICS using one or more networks, with each one corresponding to a



different class (as the number of networks depends on the configuration retained, we shall refer to this during the unfolding of the study for more precision on this point).

Inside each PCC, there is a technical system via a supervision network. Each one of these technical systems is comprised of the following elements:

- a server of the ICS;
- a technical supervision console;;
- peripheral devices.

The link between the first two items is carried out in client/server mode. The following table describes the functions provided within each PCC.


Functions	Description
Indicator display	All of the information measured by the sensors is rolled up and aggregated at the supervision server level. The supervision console makes it possible to display the measurements using dashboards.
Analysis of the situation	The supervision system determines, according to the pre-defined thresholds, the type of alert to be rolled up and its criticality.
Sending of information	The supervision system allows for the sending of information intended for actuators of the various field networks. We can mention for example the increase in the flow rate of air renewal (ventilation) following the exceeding of a threshold on the sensors linked to the control of air quality.

A.3 Programmable logic controller

Programmable Logic Controllers (PLC) provide the automated control portion of the ICS.

To do this, the PLCs, connected to a field network, receive information rolled up by the sensors and deduce from this the commands to be sent to the actuators according to a pre-programmed logic.

The turning on of fans following the detection of smoke in order to ensure smoke extraction is an example of an action controlled by a PLC.



For reasons of dependability, it is frequent for two PLCs to be implemented in a field network in order to provide redundancy, in which case a dedicated link is generally implemented in order to synchronise the PLCs. In the case of the tunnel, these redundant PLCs are located at the two ends of the latter.

Finally, although an LCD screen may be available on the PLCs in order to check the correct execution of the actions of the PLC, they are generally accompanied by a MMI console (see hereinafter) when this follow-up is required by the operator as regular follow-up.

A.4 Fire Detection Unit

As its name indicates, the fire detection unit is a device of which the role is to detect a fire as early as possible. This is a programmable safety controller (APS), i.e. a specialised PLC dedicated to a security function as its operation is guaranteed including in degraded mode, for example thanks to internal redundancy of certain control chains.


Fire detection can receive information from sensors dedicated to fire detection (smoke detectors, deformation detectors, etc.) and of which the actions can be to sound the alarm or trigger reflex actions via the standard PLCs (for example order the stopping of the ventilation).

Fire detection is in particular based on a rather specific component, fibrolaser. The latter uses the physical properties of an optical fibre, running along the length of the tunnel.

In case of a substantial increase in the temperature, the device will be able to detect the dilatation of the fibre in order to roll up the alarm. The location of this point of dilatation, and therefore the generation of heat, is made possible via the variations in conductivity that it induces in the fibre. This location is then used to carry out a concentrated extraction at the assumed location of the fire.

A.5 Man-machine interface

In the field of automation, the term man-machine interface (MMI) most often designates a touch-sensitive screen that makes it possible to centralise the control of a function or of a set of functions, by displaying pertinent indicators and by making available to the operator controls that make it possible to direct their operation, within the limits set by the program of the PLC.



Thanks to this, a MMI can be assimilated with a highly simplified version of the supervision station, deployed as close as possible to the field installations. Just as with the supervision stations, they do not make it possible to modify the programs in the PLCs (contrary to the maintenance station).

A.6 workstation

Connected to a supervision server, the workstation used by Tunnello 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;
- **the administration and maintenance of the supervision solution:** this is the installation, setting and configuration of the software required to supervise the tunnel;
- **the 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.

A.7 Maintenance station

Also called the programming console, its role is to allow for maintenance actions on the field devices (*i.e.* in the tunnel), starting with the PLCs. More particularly, it makes it possible to connect to the devices of the tunnel in order to perform privileged operations such as the modification of the programs within the PLCs or the updating of firmware of all the devices. This station is therefore sensitive in its construction since all of the tools required to dialogue with the devices are installed.

In the particular case of the tunnel concerned by the study, the hypothesis is taken to use one (or several) laptop computers to carry out these actions, in particular in order to be able to connect directly to the various devices, without depending on an administration network. Because of this, this station is sometimes qualified as mobile.

In this initial approach, this maintenance station 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 function and a location, this maintenance station can also be used for other actions, as soon as it is necessary to have extended rights on a device.



Due to its criticality, access to this station and the actions performed with it have to be tracked.

A.8 Firewall

The role of a firewall is to ensure a satisfactory level of protection for the exchanges during the interconnection of the networks for which the level of trust or sensitivity is not necessary equivalent.

The protection provided by this device is directly linked to its ability to detect non-compliant exchanges. Because of this, a generic firewall, adapted to the analysis of the services present in a conventional information system, is not equivalent to a device that can assess the industrial protocols and the associated functional flows.


Through its role, monitoring the alarms rolled up by a firewall is essential. In the framework of the study, each firewall is therefore attached to the technical supervision console and to the logging system set up for the class that it depends on (cf. the contents of the study for more details on this latter point).

A.9 Diode

Several architectures proposed implement one or more data diodes (hardware). The role of a data diode is to ensure the unidirectionality of certain links. Indeed, as indicated in the section “Functional dependencies” in chapter 2 of the first part of the case study [ANS16a], it is possible to have information transit from a network of a given class to a network of a lower class, but it is imperative to block any command from a lower network to a network of a higher class.

In the simplest case, the information can be limited to a simple change of status, such as for example the triggering of a fire alarm. In this case, it is possible to use the basic elements in order to carry out the exchange mechanisms, such as the setting up of an **optocoupler** between a simple output of the PLC of a high class and an input of the contactor type on the PLC of a lower class. This type of device can also be used to transit information that is a little more complex by encoding it (it is possible to find optocouplers that allow for a connection of a few kbps).

According to the protocols implemented for complex information, it is however likely that the use of a hardware data diode alone (i.e. without any other element accompanying it) is not possible, as the protocol is expecting for example acknowledgement feedback. In this case, the hardware data diode should be supplemented with two “windows”, on either side, which ensure compatibility with the respective protocols of



the two networks, while still guaranteeing the transfer through the data diode in an adapted manner (error correction code, flow rate management, etc.).

In the architectures mentioned in this document, these two windows are considered as part of the “data diode” component taken as a whole and are therefore not materialised in the diagrams.

Finally, as for the other security products, priority will be given to data diodes that have been certified by ANSSI as the latter appear on the market.

Appendix B

Architectures for alternative groupings

This appendix groups together proposals for architectures built using other groupings presented in the chapter “Choice of the architecture” of the first part of the case study [ANS16a] for which the main measures have been listed.

B.1 “All C3” configuration

Being limited to the unfolding of the main measures, the latter show the need to set up the following components, in addition to the main functions:

Class	Additional components
Class 3	<ul style="list-style-type: none">- maintenance station for technical administration (separate from the supervision station);- dedicated diagnostic and intervention tools;- import secure data exchange (not necessarily connected to the network);- centralised logging server;- technical directory;- firewall;- VPN between sites;- SIEM solution (optional);- intrusion detection solution.

The architecture diagram in figure B.1 shows the ICS that is the result of the study.

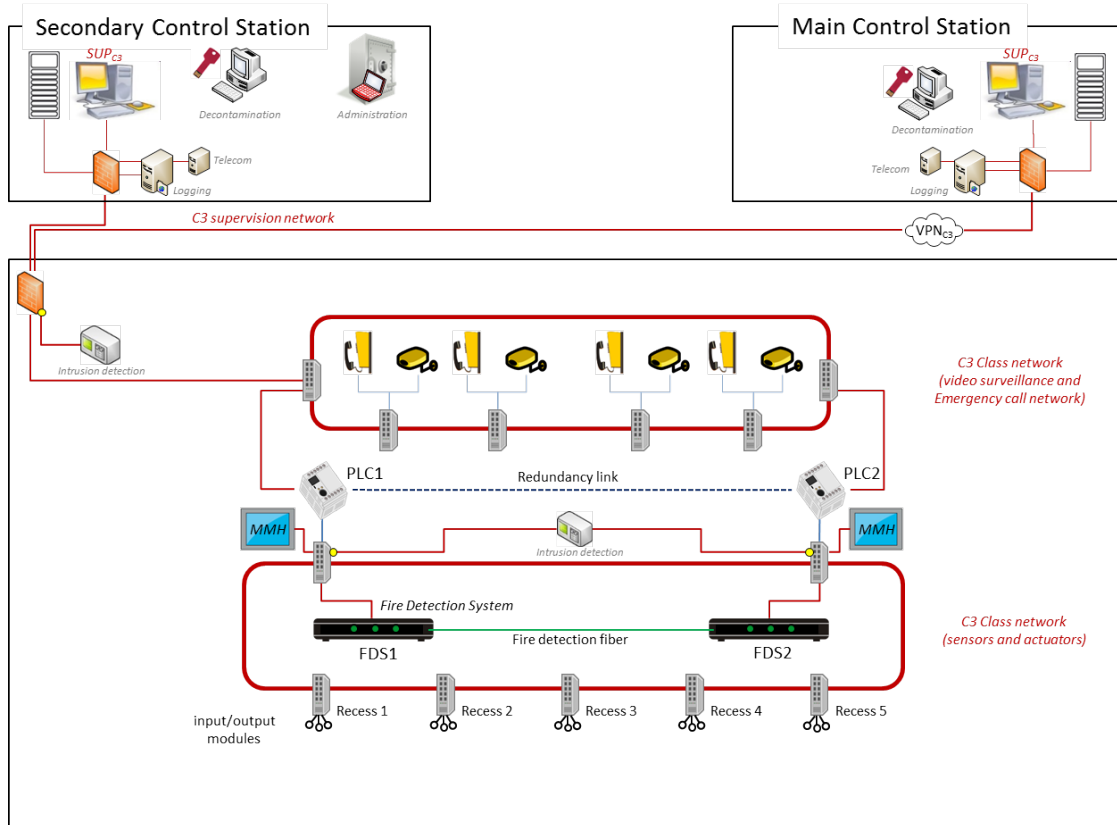


Figure B.1: ICS - Secure technical architecture "All C3"

The field network as well as the supervision network are classified in the highest level of security, C3.

Video surveillance remains on a dedicated network (same principle as mentioned hereinabove).

All of the sensors and actuators are on the same loop.

At the level of the control stations, a single supervision console is sufficient (marked "Sup C3"); it is deployed behind the ICS.

B.2 "C1 , C2 , C3" configuration

Being limited to the unfolding of the main measures, the latter show the need to set up the following components, in addition to those linked to the main functions:

Class	Additional components
Class 1	<ul style="list-style-type: none"> - maintenance station for the technical administration; - import secure data exchange (optional, not necessarily connected to the network); - firewall; - VPN between sites; - centralised logging server (optional).
Class 2	<ul style="list-style-type: none"> - maintenance station for technical administration (portable, separate from the supervision station); - diagnostic and intervention tools dedicated to the site, with a tolerance when their usage remains exceptional; - import secure data exchange (not necessarily connected to the network); - centralised logging server; - firewall; - VPN between sites; - intrusion detection solution (optional).
Class 3	<ul style="list-style-type: none"> - maintenance station for technical administration (portable, separate from the supervision station); - diagnostic and intervention tools dedicated to the site; - import secure data exchange (not necessarily connected to the network); - centralised logging server; - technical directory; - firewall; - VPN between sites; - data diode allowing information to move down to C2; - SIEM solution (optional); - intrusion detection solution.

This configuration diagrammed in B.2 is the most complex to implement as it requires a specific network for each class.

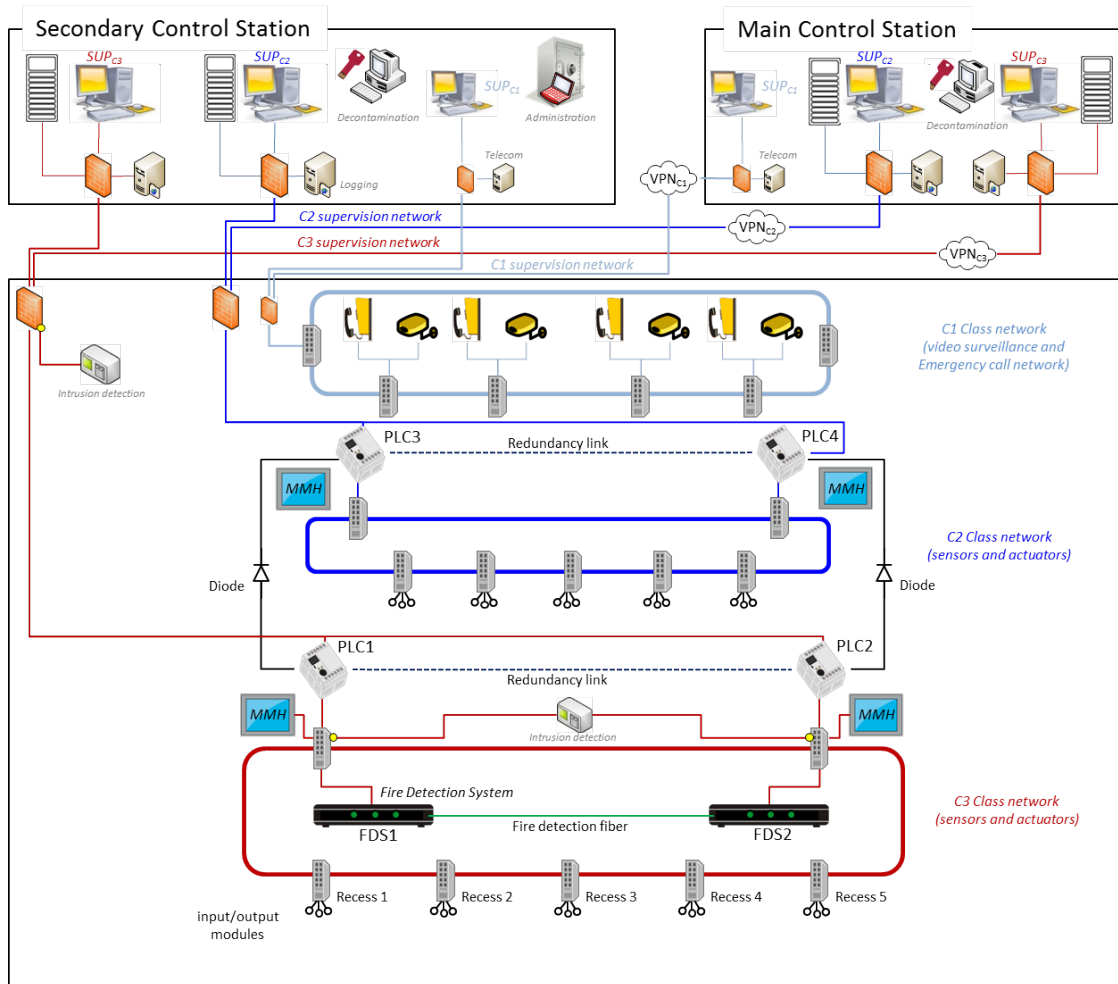


Figure B.2: ICS - Secure technical architecture "C1, C2, C3"

B.3 "C1+C2, C3" configuration

By carrying out the same method as hereinabove, the list of complementary components is provided in the following table.

Class	Additional components
Class 2 (C1 + C2)	<ul style="list-style-type: none"> - maintenance station for technical administration (portable, separate from the supervision station); - diagnostic and intervention tools dedicated to the site, with a tolerance when their usage remains exceptional; - import secure data exchange (not necessarily connected to the network); - centralised logging server; - firewall; - VPN between sites; - intrusion detection solution (optional).
Class 3	<ul style="list-style-type: none"> - maintenance station for technical administration (portable, separate from the supervision station); - diagnostic and intervention tools dedicated to the site; - import secure data exchange (not necessarily connected to the network); - centralised logging server; - Technical directory; - firewall; - VPN between sites; - data diode allowing information to descend to C2; - SIEM solution (optional); - intrusion detection solution.

The communication between networks of different classes results in the implementation of a hardware data diode represented in the physical architecture diagram in figure B.3.

The sites are connected together by the VPNs of each class. Each VPN is secured by a firewall when leaving the tunnel and at the input of each control station. The architecture therefore makes it possible for all of the functions to be executed independently in one control station or the other.

In the case of maximum security, several options are possible:

- installation of servers in cluster mode in the two sites, while still giving attention to data synchronisation between the two sites,
- displacement of the second member of the cluster of each supervision level (SUPcX) in the second site.

Recall: there is no connection between the two supervision networks C2 and C3.

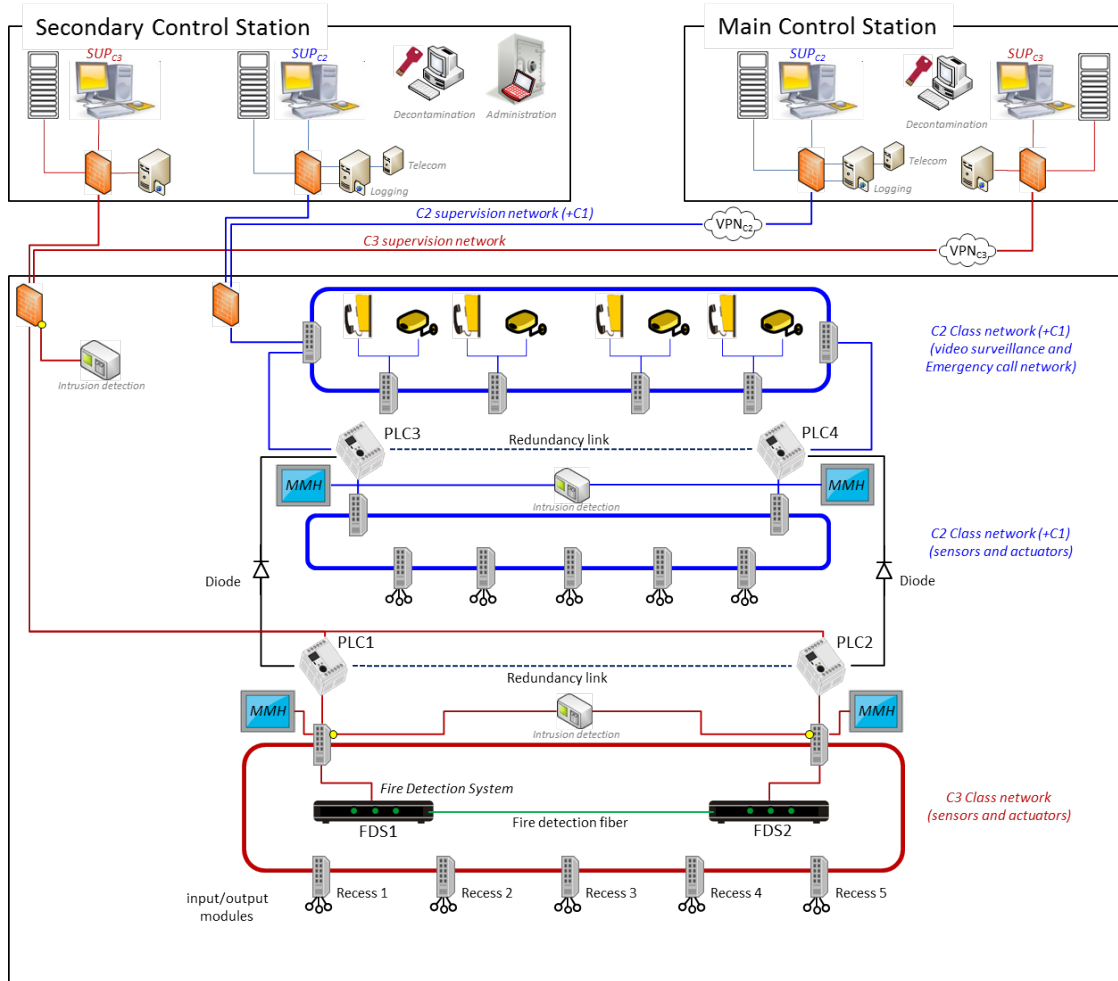


Figure B.3: ICS - Secure technical architecture "C1+C2 and C3"

Bibliography

- [ANS12] *Recommandations de sécurité relatives aux mots de passe.*
Note technique DAT-NT-001/ANSSI/SDE/NP, ANSSI, juin 2012.
<http://www.ssi.gouv.fr/mots-de-passe>.
- [ANS15] *Recommendations for securing networks with IPsec.*
Technical Report DAT-NT-003-EN/ANSSI/SDE/NP, ANSSI, 2015.
<http://www.ssi.gouv.fr/en/ipsec>.
- [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>.
- [ANS14] *L'homologation de sécurité en neuf étapes simples.*
Guide Version 1.0, ANSSI, juin 2014.
<http://www.ssi.gouv.fr/guide-homologation-securite/>.

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](mailto:conseil.technique@ssi.gouv.fr)