CETU

Guides

TUNNEL EQUIPMENT MANUAL

French guide on automatic incident detection in road tunnels by image analysis

December 2025

Centre for Tunnel Studies

www.cetu.developpement-durable.gouv.fr

MINISTÈRE DES TRANSPORTS

Liberté
Égalité
Fraternité

GUIDES

CETU guides are the result of methodological work conducted by CETU. They are intended to serve as a reference for the design, construction, or operation of underground structures in France. Although relevant at the time of writing, any guide may become obsolete, particularly due to regulatory or technical developments. Each user is responsible for its correct application.
These documents can be downloaded from the CETU website.

TUNNEL EQUIPMENT MANUAL

French guide on automatic incident detection in road tunnels by image analysis

Decembre 2025

Centre for Tunnel Studies
25, avenue François Mitterrand
69500 BRON – France
Tel. 33 (0)1 40 81 30 30

cetu@developpement-durable.gouv.fr
www.cetu.developpement-durable.gouv.fr

TABLE OF CONTENTS

APPENDICES

1 INTRODUCTION

1.1 BACKGROUND

For the past thirty years or so, long or high-traffic road tunnels have been equipped with automatic incident detection systems (AID) based on image analysis. An AID system assists the operator at the Control and Command Centre (CCC) in monitoring the tunnel by alerting them to the occurrence of an incident that could lead to a potentially dangerous situation for road users. The operator can then trigger the most appropriate response scenario as quickly as possible. Image-based AID is not the only means of ensuring incident detection and is not intended to replace operators or all other systems, but it is an essential means of detection in road tunnels under constant surveillance.

Figure 1: Video wall at the Control and Command Centre of the Traffic Management and Safety Centre in Moulin-les-Metz

1.2 KEY ISSUES IN FRANCE

Incident detection based on image analysis plays a very important role in supporting the operation of road tunnels, and a great many tunnels are now equipped with it. This equipment contributes to the functions of "detecting" and "classifying" an incident, as defined in the CETU's Information Note No. 23. Whilst it is not the only means of ensuring the detection function, it remains an important piece of equipment, as it can save time in situations where a rapid response is crucial for user safety.

Feedback indicates that CCTV, combined with an Automatic Incident Detection (AID) system, is the primary means of detecting significant incidents. Statistics show that between 40 and 60 per cent of incidents are detected using this equipment.[2]

Given the importance of this system, it must be carefully designed and properly calibrated to ensure it remains reliable over time and serves as a trusted tool for the operator.

Indeed, a poorly designed or incorrectly calibrated AID system is likely to generate too many false alarms, which is a source of disruption for operators. Conversely, a poorly designed or incorrectly calibrated system may fail to detect a genuine incident, be slow to do so, or misclassify it, which undermines the system's credibility and reduces the confidence operators have in it.

Furthermore, AID tests carried out between 2011 and 2023 by the CETU on more than 40 French tunnels, as part of detailed inspections, revealed a significant discrepancy between observed and expected performance, thereby highlighting the need to pay close attention to this system to ensure it performs to its full potential.

1.3 OBJECTIVES OF THIS GUIDE

This guide sets out recommendations for the design, installation, validation and maintenance of AID systems in road tunnels to help ensure their long-term performance. It supersedes the information document published by the CETU in 2015.

It was drawn up following feedback from tunnel owners, project managers, tunnel operators, equipment manufacturers and system integrators. Changes compared with the 2015 document relate to new sensor technologies (thermal cameras) and analysis systems, network architectures, and cybersecurity. Certain chapters have been significantly expanded, such as those dealing with the design and installation phases or the operational phase of the tunnel. Changes to recommendations have been included, particularly regarding the classification of incidents, which has been expanded and updated with new terminology. Finally, new indicators are proposed to assess the system's overall performance.

Organised into seven chapters, this document first identifies the incidents to be detected, then describes the AID equipment and its modes of operation. It also provides information on expected performance and on general cybersecurity and operational safety principles. The design, installation and performance validation tests of the system are then discussed. Finally, the last section is devoted to the operations to be carried out throughout the tunnel's lifetime, which are essential for maintaining the system's proper functioning and the highest level of confidence in it.

1. Information Note No. 23, *Definition of Safety Functions – Application to degraded operating modes and minimum operating requirements*.
2. Source: CETU breakdown/accident database – Rex 2014-2020.

2 REGULATORY ASPECTS

2.1 CCTV SURVEILLANCE OF PUBLIC SPACES

The use of video surveillance is primarily governed in France by Articles 17 to 25 of Section IV of Act No. 2011-167 of 14th March 2011 on Guidelines and Planning for Internal Security Performance (LOPPSI 2).

This Act does not specify the technology to be used but merely defines the main operating procedures for the systems and sets technical standards (by French decree of 3rd August 2007, updated on 16th March 2011 – technical appendices published in the Official Journal of 25th August 2007) which relate, on the one hand, to cameras and to transmission and storage systems, and, on the other hand, to the interoperability of systems for storing and exporting data to the police and gendarmerie.

The provisions of LOPPSI 2 have been incorporated into the Internal Security Code (ISC). The document issued by the French National Commission for Information Technology and Civil Liberties (CNIL) on 18th November 2024, entitled *Conventional Video Surveillance*, summarises the applicable legislation and sets out the rules to be observed[3].

Video surveillance in road tunnels, for the purposes of risk prevention, personal safety and traffic flow management, is governed by Articles L.223-1 to L.223-9 and R.223-1 to R.223-2 of the ISC. These articles stipulate, in particular, that:

- installation requires authorisation from the prefect following the submission of a technical dossier including, where necessary, a Data Protection Impact Assessment (DPIA);
- the data collected is limited to images useful for detecting incidents (excluding audio and facial recognition), and may be retained for a maximum of one month;
- access to the footage is strictly restricted to authorised staff;
- persons filmed must be informed by means of a notice;
- access rights to the data are regulated, with possible restrictions for the sake of public security.

Public authorities, companies and organisations processing personal data, as well as their service providers and sub-contractors, are now fully responsible for the protection of the data they process.

It is their responsibility to ensure that their processing of personal data complies with the General Data Protection Regulation (GDPR – 25th May 2018) throughout the data's lifecycle and to be able to demonstrate such compliance.

In particular, the CNIL states that "AI models may fall within the scope of the GDPR if they store personal data derived from their training. The CNIL proposes a method for providers to assess whether their models are subject to the GDPR or not"[4]. AI providers must therefore ensure that they comply with these rules.

2.2 AUTOMATIC INCIDENT DETECTION IN ROAD TUNNELS

Where human monitoring is provided, the French Technical Directive (TD) relating to safety provisions in new tunnels on the State-managed road network, set out in Appendix 2 to Circular 2000-63 of 25th August 2000, requires the installation of a video surveillance network and an automatic incident detection system. Indeed, paragraph 3.9 of the Directive specifies that:

"*A CCTV surveillance network covering the entire interior of the tunnel and its immediate surroundings, as well as an automatic incident detection system, are mandatory wherever surveillance – whether permanent or otherwise – is provided (permanent staffing and surveillance levels D3 or D4…). In the event of an alarm that may result from an incident or accident, the CCTV footage showing the area from which the alarm originated must be recorded automatically so as to enable subsequent analysis of the incident or potential accident. This is a minimum requirement: a system that systematically records all footage and retains it for a few minutes under normal circumstances and for an indefinite period in the event of an alarm naturally offers better opportunities for subsequent analysis…*".

3. Source: *"Conventional" video surveillance – Summary of applicable legal references*, 18th November 2024, document from the French Data Protection Authority (CNIL).
4. Source: *AI: analysing the status of an AI model under the GDPR*, 22nd July 2025, document from the French Data Protection Authority (CNIL).

Tunnels which are required by the French Technical Directive to have a system capable of detecting incidents, must therefore also be equipped with a video surveillance system. This incident detection is consequently generally carried out by analysing images from video surveillance cameras.

The French Technical Directive does not specify the type of incident that the incident detection system must detect.

Similar French requirements are laid down in the Order of 9th November 2007 amending the Order of 8th November 2006 and setting out the minimum safety requirements applicable to tunnels over 500 metres long within the trans-European network.

Tunnels meeting this criterion must comply with the minimum safety requirements set out in paragraph (m) of Article 2, which states:

"*Video surveillance systems and a system capable of automatically detecting traffic incidents or fires shall be installed in all tunnels equipped with a control and command centre.*
Automatic fire detection systems shall be installed in all tunnels without a control and command centre, where the operation of mechanical ventilation for smoke control differs from the automatic operation of ventilation for pollutant control."

2.3 CYBERSECURITY

CCTV and AID systems are among the information systems that are particularly vulnerable to cybersecurity risks.

The regulatory framework governing information security comprises European Directives and national laws and decrees enacted over several decades. In France, these include, in particular, the French Data Protection Act (LIL)[5], the Military Programming Acts (MPA) for 2014-2019 and 2024-2030, the Network and Information Security (NIS) Directive, and the European General Data Protection Regulation (GDPR) EU 2016/679.

Furthermore, the ISO 27000 series of standards, in particular the NF EN ISO/IEC 27001:2023 standard[6], sets out the requirements for the certification of an Information Security Management System (ISMS).

In accordance with these texts, the Chief Information Security Officer (CISO) and the organisation's IT department draw up an Information Systems Security Policy (ISSP) comprising a section specifically tailored to operational occupation-specific systems. The Operations and Security Procedure (OSP) must be drawn up for the AID system in accordance with the ISSP.

5. French law No. 78-17 of 6th January 1978 on data processing, data files and civil liberties.
6. NF EN ISO/IEC 27001:2023 Information security, cybersecurity and privacy – Information security management systems – Requirements.

3

INCIDENTS TO BE DETECTED

3.1 DEFINITION OF AN INCIDENT

The term **"incident"** refers to an abnormal and unforeseen event that has an adverse effect on the operation and safety of a tunnel[7].

It is essential for an operator to detect abnormal situations as early as possible so that they can respond very quickly.

Some incidents that occur in a tunnel, such as accidents or fires, may pose high direct risks, whilst others may be precursors to more serious events. This second category includes, for example, slow-moving traffic, stopped vehicles on the carriageway, or the presence of pedestrians in tunnels where they are not permitted.

Incident detection can be either direct or indirect. In the former case, the incident itself is detected. In the latter case, it is the impact of the incident on traffic that is detected.

3.2 CLASSIFICATION AND SELECTION OF INCIDENTS TO BE DETECTED

Amongst the wide variety of incidents that may occur in tunnels, the regulations do not specify which ones should be detected.

This chapter therefore provides a list of the types of incidents to be detected.

Naturally, every operator wishes to be able to detect as many incidents as possible. However, athough the detection capabilities of incident detection systems are constantly improving, the greater the number of incidents to be detected, the more difficult the system is to configure and the more likely it is that its performance may be compromised. In some cases, often linked to insufficient preventive maintenance, the degradation is such that it can lead to operators being overwhelmed by false alarms, with the risk of the AID system being discredited. It is therefore important to carefully select the types of incidents to be detected.

To this end, a list of the most common incidents has been drawn up. It is **categorised into three levels**: from Level 1 (considered a priority) to Level 3 (detection is of interest but not essential). Naturally, these different levels can be adjusted according to the characteristics of the tunnel and its surroundings, its mode of operation and the expected service.

Incidents can be prioritised based on:

- their severity and frequency;
- the system's ability to detect them;
- whether or not there are measures in place to respond to their occurrence.

Table 1 below sets out this hierarchy of the most common incidents (a detailed description of these is provided in Appendix A). In light of the specific risks associated with each tunnel, this table may be supplemented by other types of incidents to be defined on a case-by-case basis.

Incident level	Incident
1	Stopped vehicle
	Fire[8]
2	Traffic congestion[9]
	Stopped vehicle during traffic congestion
	Vehicle travelling in the wrong direction
	Pedestrians
3	Object
	Slow-moving vehicle

7. Definition provided by the World Road Association (PIARC).
8. The system can detect either a loss of visibility (smoke) or the presence of a flame.
9. Congestion: a phenomenon that occurs when demand exceeds the capacity of the infrastructure (source: *Understanding Road Traffic – Methods and Calculations*, 2010, Centre for Studies on Networks, Transport, Urban Planning and Public Works, (CERTU).

A stopped vehicle and a fire[10] are the two incidents that must be systematically detected throughout the entire tunnel.

For other incidents, an analysis should be carried out to determine whether they need to be detected and, if so, in which areas of the tunnel they should be detected.

The following factors may be used to guide this analysis:

- smoke and object detection using cameras located at the tunnel entrance should be avoided as far as possible, as this may in some cases lead to a deterioration in the system's performance;
- detection of vehicles travelling in the wrong direction may be relevant for tunnels longer than 1 km or located on routes equipped with emergency response facilities;
- in the event of pedestrian detection, it may be appropriate, in addition to detection at the tunnel entrance, to extend this detection into the tunnel itself for pedestrians coming from unauthorised "quick-drop-off" points or intrusions via various access points (exits, slip roads, etc.);
- object detection within tunnels is only relevant where traffic volumes are low. Indeed, in high-traffic tunnels, it is highly likely that the object would have caused another incident– one that is itself detectable – or would have been moved by a vehicle before any action could be taken by the Control and Command Centre (CCC). Finally, feedback from tunnel operators shows that this type of detection can lead to recurring false alarms. It is therefore advisable to implement it only in very specific cases and following a detailed analysis of the intended objectives;
- the detection of slow-moving vehicles is less commonly required. It may, for example, prove useful in tunnels where the minimum speed of vehicles is a particular concern (such as in the case of major cross-border tunnels…).

Thus, depending on the type of tunnel and its context, it is possible to select one or more types of incident from each level.

10. The former term "Smoke detection", which appeared in the 2015 information document, has been replaced by "Fire", which can be detected either through a loss of visibility or via flame detection capabilities now offered by thermal imaging cameras.

4

AID EQUIPMENT

The image-based AID function relies on a scene capture system, typically derived from the tunnel's CCTV cameras, which requires specific characteristics. The video feed generated is analysed by dedicated software that utilises several types of algorithms. When an incident is identified by this system, an alarm is generated and transmitted to the operator.

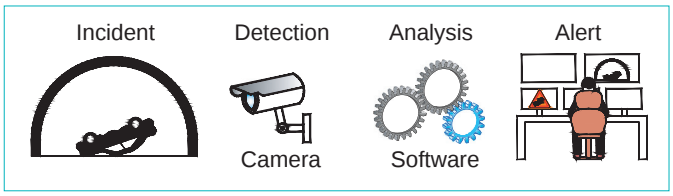


Figure 2: AID sequence

4.1 CAMERAS

An AID system based on image analysis uses images captured by a camera, which usually has a permanent fixture.

The term "camera" refers to the assembly comprising the sensor, the lens, the housing and its mounting system.

The image obtained depends on the characteristics of the camera's sensor.

Two types of camera are used: **conventional cameras**, which are sensitive to visible light, and **thermal cameras**, which are sensitive to infrared radiation (see box opposite). Each technology has its advantages and disadvantages.

A few systems using analogue cameras still exist, but they are reaching the end of their life due to a lack of spare parts and are gradually being replaced by digital technologies – "IP (Internet Protocol) cameras".

Sensor characteristics

Electromagnetic spectrum

Depending on the type of camera, the operating range may cover different wavelengths within the electromagnetic spectrum. The electromagnetic spectrum is defined as the classification of electromagnetic radiation by wavelength (from zero to infinity) in a vacuum. It is divided into several bands, within which the radiation is studied using specific methods. A representation of this spectrum is shown in Figure 3.

Resolution

The sensor's resolution corresponds to the total number of pixels.

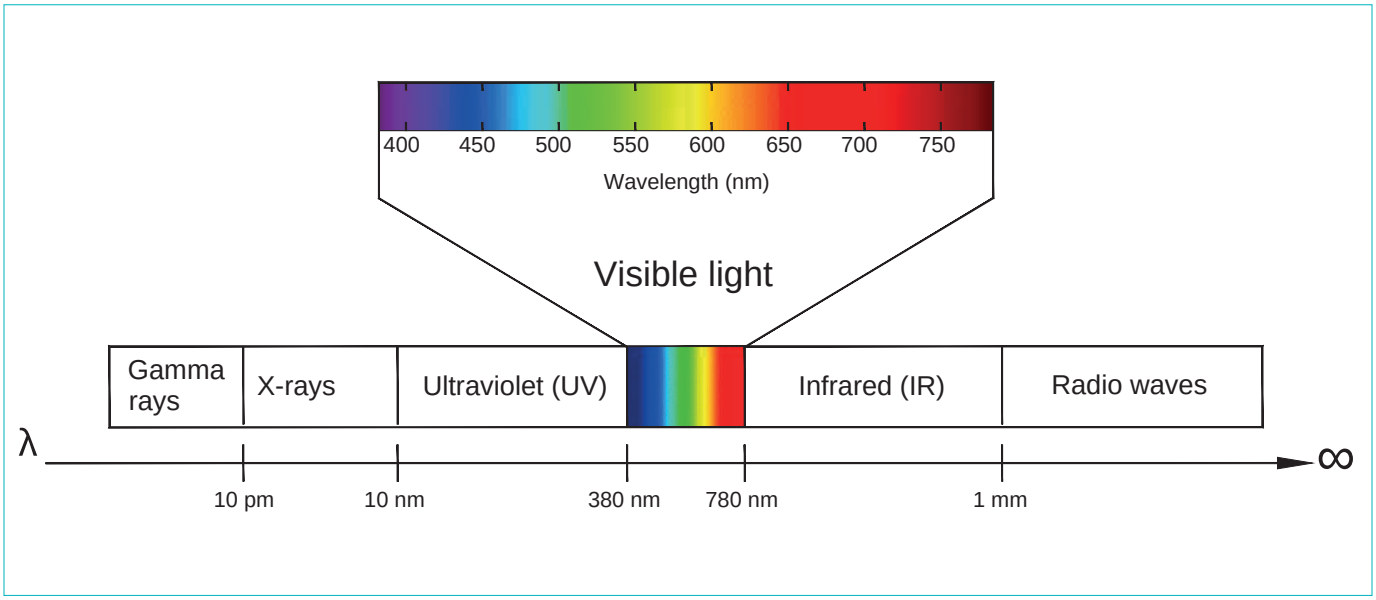


Figure 3: Representation of the electromagnetic spectrum (© Cerema DTecITM)

4.1.1 Conventional cameras

Conventional cameras use a photosensitive electronic sensor (utilising photodiodes and Complementary Metal-Oxide-Semi-conductor (CMOS) technology that operates on the principle of reflection. This enables the conversion of electromagnetic radiation into an electrical signal.

Depending on its application, this sensor can operate in the following wavelength ranges:

- ultraviolet (10–380 nm), which is of no interest for AID;
- visible (380-780 nm);
- near-infrared (700–1,500 nm), NIR in Figure 4.

Cameras operating in the visible wavelength range are widely used in tunnels.

The advantages of this technology are as follows:

- immediate visual feedback of the incident in true colour (operator comfort);
- sensor resolution of up to 4K, which is very useful for assessing the incident;
- smoke detection is possible;
- lower cost than a system using thermal technology.

The disadvantages of cameras operating in the visible wavelength range are as follows:

- sensitivity to weather conditions such as rain or fog;
- sensitivity to changes in light levels and visibility conditions, such as glare at the tunnel portal; cannot be used in the dark (except for day/night cameras) or in a smoke-filled tunnel;
- sensitivity to shadows;
- sensitivity to intrinsic and extrinsic camera faults (such as reflections on the lens, for example).

Cameras operating in the near-infrared spectrum are not currently used for AID in tunnels.

Their characteristics and potential applications are described in Appendix B.

4.1.2 Thermal cameras

Thermal cameras, generally deployed in tunnels, use a microbolometer-type sensor sensitive to infrared radiation in the 7.5-14 µm range.

This sensor produces an image that corresponds to the thermal gradients present in the observed scene. It operates within the LWIR wavelength range (7-15 µm).

These cameras can produce images either in false colour or in black and white.

Infrared spectral bands;

- NIR, *near infrared*;
- SWIR, *short wave infrared* ;
- MWIR, *medium wave infrared*;
- (V)LWIR, *(very) long wave infrared*.

These bands are shown in Figure 4.

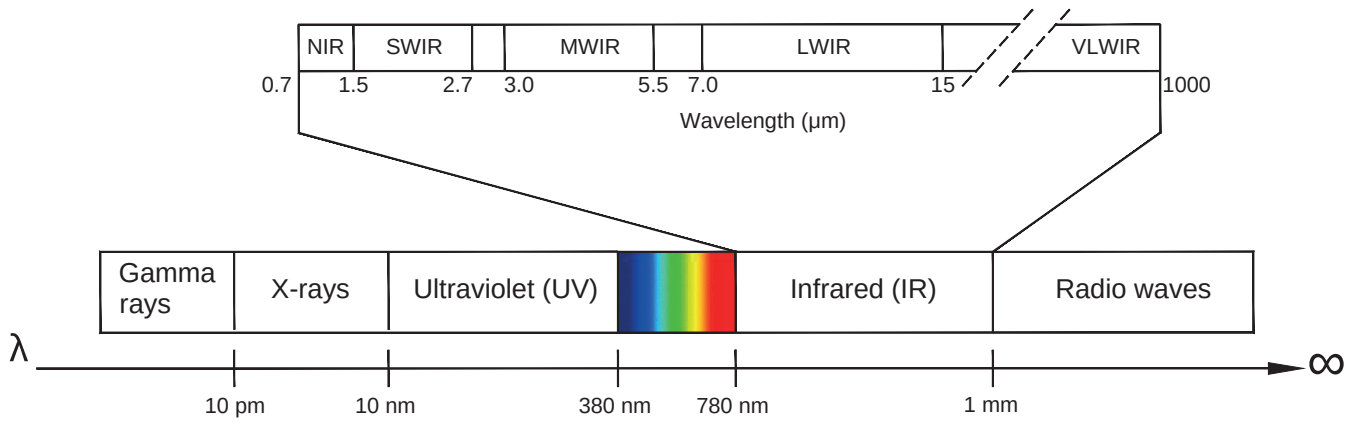


Figure 4: The different frequency bands in the infrared spectrum (© Cerema DTecITM)

As this technology is relatively insensitive to variations in brightness and visibility conditions, its main advantages are as follows:

- low sensitivity to weather conditions such as fog;
- insensitivity to headlamp glare and light reflections on wet road surfaces;
- the ability to detect objects through smoke (depending on the camera's sensitivity);
- low sensitivity to shadows (particularly in tunnels);
- potential for flame detection (depending on the wavelengths used by the camera).

The disadvantages associated with this type of technology are as follows:

- not suitable for traffic monitoring or visual inspection of incidents by the operator[11];
- not suitable for detecting objects with radiation levels similar to those of the tunnel's surroundings, such as cold smoke or objects that do not emit heat;
- the sensor's resolution is currently lower than that of sensors used in conventional technology;
- higher cost than conventional cameras.

Image transformation

In an image-based early warning system, the incidents to be detected are analysed not in three-dimensional space but on a projection surface.

The image transformation consists of a perspective projection that transforms a three-dimensional point in space into a point in a two-dimensional image.

This projection is highly dependent on the parameters of the optical system (camera positioned and oriented within its environment), which fall into two categories:

- parameters relating to the camera's specific characteristics (sensor size, sensor resolution, lens focal length, optical distortion, etc.);
- parameters dependent on the camera's position and orientation within the tunnel (location, tilt and azimuth), which are directly linked to the tunnel's geometry (number of lanes, bends, clearance).

These various parameters affect **the image resolution**, i.e. the ratio of pixels per metre (the smallest unit of a digitised image).

4.1.3 Coverage and layout

The optical system parameters (see the "Image Transformation" box opposite) must be taken into account in order to achieve the desired AID coverage within the tunnel.

Indeed, depending on its position, its angle of inclination and the focal length used (usually 8 mm or 16 mm), a camera can cover a greater or lesser distance in a straight line within the tunnel (ranging from 60 to 100 metres); however, the further the area under observation is from the camera, the lower the pixels-per-metre ratio.

The image captured by the camera is generally divided into three parts vertically (see Figure 5 below):

- the first half of the image, with the highest resolution, represents the near field of view;
- two-thirds of the second half, of medium resolution, represent the middle of the field of view;
- the remaining third of the second half, with low resolution, represents the end of the field of view.

As the image quality of objects in the end of the field of view is poorer, the detection performance of the AID system may be compromised.

Overlap between cameras is necessary to enable the system to detect the required incidents at any point on the carriageway. This also applies to hard shoulders, emergency lay-bys and walkways, where they exist.

A **preliminary camera layout study** is essential to ensure the desired coverage (see paragraph 8.1 – Design studies). It should be noted that the development of an AID system often leads to an increase in the number of cameras compared with that required for video surveillance alone. Naturally, the more complex the geometry of the tunnel (bends, gradients, etc.), the more complex the positioning of the cameras becomes and the greater the number required.

The layout study must also take into account the effects of the various disturbances described in paragraph 4.3 – Specific provisions.

Where the tunnel clearance permits, cameras should preferably be positioned along the tunnel's central axis to avoid obstruction by heavy goods vehicles.

11. This type of camera can effectively complement a surveillance system but is unlikely to replace it. Indeed, conventional cameras are generally necessary to enable the operator to view and analyse events.

4.2 THE AID ANALYSER

The AID analyser is the tool that processes the images captured in the tunnel. It can be integrated into the camera, or located remotely and shared amongst several cameras. Its analyses are based on algorithms.

4.2.1 Image analysis algorithms

An AID system based on image analysis aims to replicate the visual monitoring that an operator would carry out to identify an incident in the tunnel.

To achieve this, manufacturers combine several types of algorithms. The earliest algorithms – referred to as "historical" algorithms in the rest of this document, which have been used and are still in use today – are "background extraction" (also known as "foreground/background algorithms"), "tripwire" and "tracking" algorithms. These algorithms make it possible to characterise movements within the tunnel and to detect abnormal situations indicative of incidents (stopped vehicles, vehicles travelling in the wrong direction, etc.).

The ***"background extraction"*** method involves storing the static part of the scene ('background') as a reference and analysing changes in the image that could be interpreted as an incident.

The ***"tripwire"*** method involves defining specific zones within the image, each zone being defined by transverse and longitudinal lines. The rate of change in brightness along these lines is then interpreted as a vehicle passing. This measurement enables the calculation of an average speed and the determination of the direction of travel.

The ***"tracking"*** method is based on shape recognition and object tracking. By analysing the object's size, direction of movement and speed, it is possible to distinguish between different elements in the image.

More recently, with the development of intelligent transport systems (ITS), new methods for extracting images of people or objects from video sequences have been developed. These are based on artificial intelligence[12](AI) and, more specifically, on the use of deep learning.

The ***"deep learning"*** method utilises artificial neural network techniques. In order to function effectively, these networks must learn to recognise a large number of objects present in the scenes under study. The power of these algorithms depends heavily on the number of neurons per layer, the number of layers of artificial neurons used, and the size and quality of the database[13].

It is possible to combine these different methods to improve the system's robustness.

Complementary algorithms are also implemented to address the disturbances described in paragraph 4.3 – Specific provisions.

4.2.2 The "mask" concept

Regardless of the operating principle adopted, the image from a camera is broken down into several analysis zones known as masks.

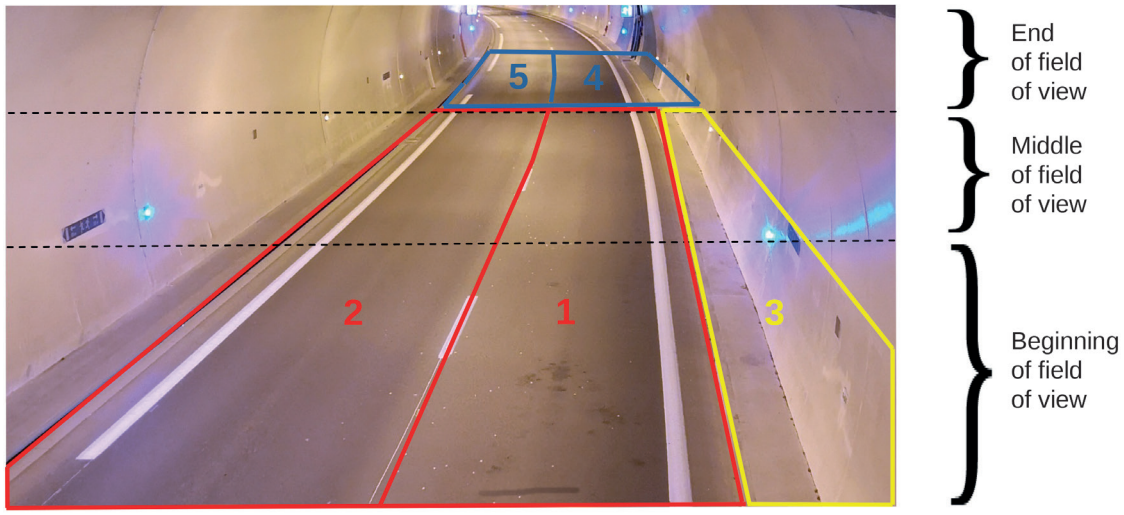


Figure 5: Example of a representation of masks and the various fields of view

12. AI is a field of research that encompasses all the techniques and methods aimed at understanding and replicating the functioning of the human brain. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13th June 2024 establishes harmonised rules concerning artificial intelligence.
13. The system's performance is directly linked to the consistency of the dataset used, which must be tailored to the incidents to be detected in the tunnel.

The main purpose of the mask is to link the detected incident to the various traffic zones within the tunnel (lanes, direction of travel, walkway, hard shoulder, lay-by, etc.). It also enables zones of interest to be defined according to the types of incidents that may occur there, with their own specific detection rules.

Figure 5 shows an example of an image divided into masks. Masks 1 and 2 correspond to the carriageway. There can be as many masks as there are lanes: mask 1 corresponds to the slow lane, including the hard shoulder, and mask 2 to the fast lane. In these areas, the aim is to detect incidents relating to vehicle traffic and, where applicable, pedestrians, or the presence of objects.

Mask 3 corresponds to the walkway, where the aim is generally to detect the presence of pedestrians and, where applicable, objects.

Masks 4 and 5 correspond to the area furthest from the camera, where the pixels-per-metre ratio is low, as explained in section 4.1.3 – Coverage and layout. It is therefore preferable to detect incidents occurring in this area using the next camera, for which they will be at the start of the field of view.

Finally, whilst it may be tempting to increase the number of masks to assign specific functions to each one, it is important to note that as this number increases, the analysis system becomes more complex and may result in either a deterioration in detection quality or an increase in the number of false alarms.

It should be noted that the use of masks has evolved since the early algorithms. Indeed, algorithms now based on "deep learning" detect incidents across the entire image and use the concept of a mask simply to characterise the location of the detected incident.

4.3 SPECIFIC PROVISIONS

In road tunnels, the components of AID systems are subject to constraints specific to this particular environment. These constraints may cause damage to the equipment or a deterioration in the quality of the footage. Specific provisions must therefore be made accordingly.

4.3.1 Protection of equipment

Cameras are subject to numerous stresses (humidity, pollution, vibration, dirt, temperature fluctuations, etc.).

This is why they are generally enclosed in a heated, glazed, watertight and corrosion-resistant housing, which is itself mounted on an adjustable support. This system must be sufficiently robust over time to ensure the stability and proper functioning of the cameras.

Depending on the environment (proximity to fans, for example), it may also be worth considering an image stabilisation system.

4.3.2 Adaptation to external disturbances

Optical sensors are subject to several types of interference, which can cause false alarms or failure to detect vehicles. The main types of interference in tunnels are as follows:

- optical occlusion: this phenomenon occurs when one vehicle partially or completely obscures another. Incorrect camera positioning can exacerbate this phenomenon (for example, cameras installed on the tunnel walls in a two-way tunnel). This problem can be avoided through a rigorous site survey;
- adverse weather conditions: rainwater runoff or fog can enter the tunnel and disrupt the analysis functions;
- light levels: rapid changes in light levels can, depending on the sensor's sensitivity, distort the analysis, particularly:
  - when sunlight enters the tunnel's entrance areas,
  - when there are changes in the lighting regime (threshold zone lighting or interior zone lighting),
  - where lighting is non-uniform, creating alternating dark and light areas,
  - in cases of insufficient lighting, i.e. where there is not enough contrast between an object to be detected and its surroundings.

New generations of cameras make it possible to effectively overcome some of these disturbances (see the advantages and disadvantages of the various technologies in section 4.1 – Cameras).

Detection must be guaranteed regardless of lighting conditions. Information regarding changes in lighting conditions must therefore be transmitted to the AID system by the SCADA system, so that it can adapt in real time to the new conditions without any deterioration in its performance.

4.4 ARCHITECTURES

A video surveillance system has three functions:

- acquisition,
- management,
- visualisation.

The AID system complements these functions with image analysis and alerts to the control room operator. The diagram below shows the hardware associated with each function. In practice, several functions may be combined within a single piece of hardware. In particular, thanks to virtualisation technology, several virtual servers can be hosted on a single physical server.

Video surveillance systems are now equipped with digital cameras, which have replaced analogue ones (see 4.1 – Cameras).

They are connected to the tunnel's backbone network[14]. For this purpose, this network is generally organised into virtual local area networks (VLANs)[15].

The wide range of hardware present in a video surveillance-based AID system, combined with the variety of functions offered, opens up the possibility of numerous architectures for this system. Their evolution towards ever more powerful and miniaturised technologies further increases the possibilities.

However, the overall architecture remains heavily dependent on the architecture of the tunnel's video surveillance system.

The choice of architecture for the AID system must take into account various criteria, namely:

- the number of cameras;
- the video bit rate, which depends on the chosen image quality;
- the capacity of the communication networks;
- the number of plant rooms and their locations;
- the space available in the plant room(s) and at the control centre(s);
- the level of operational reliability and cybersecurity to be achieved, depending on the project's requirements.

Depending on the chosen architecture, the positioning of the equipment varies.

In all cases, data is acquired inside the tunnel – via cameras – and displayed at the control room – on the video wall, on the SCADA system[16] or on the AID client[17].

Various solutions are available for managing and analysing video streams: ranging from analysis carried out as close as possible to the point of capture – with image analysis integrated into the camera – to remote, centralised analysis at varying distances from the tunnel.

Typical AID architectures for tunnels are presented below. These are merely examples. Architectures combining the ones presented are also possible.

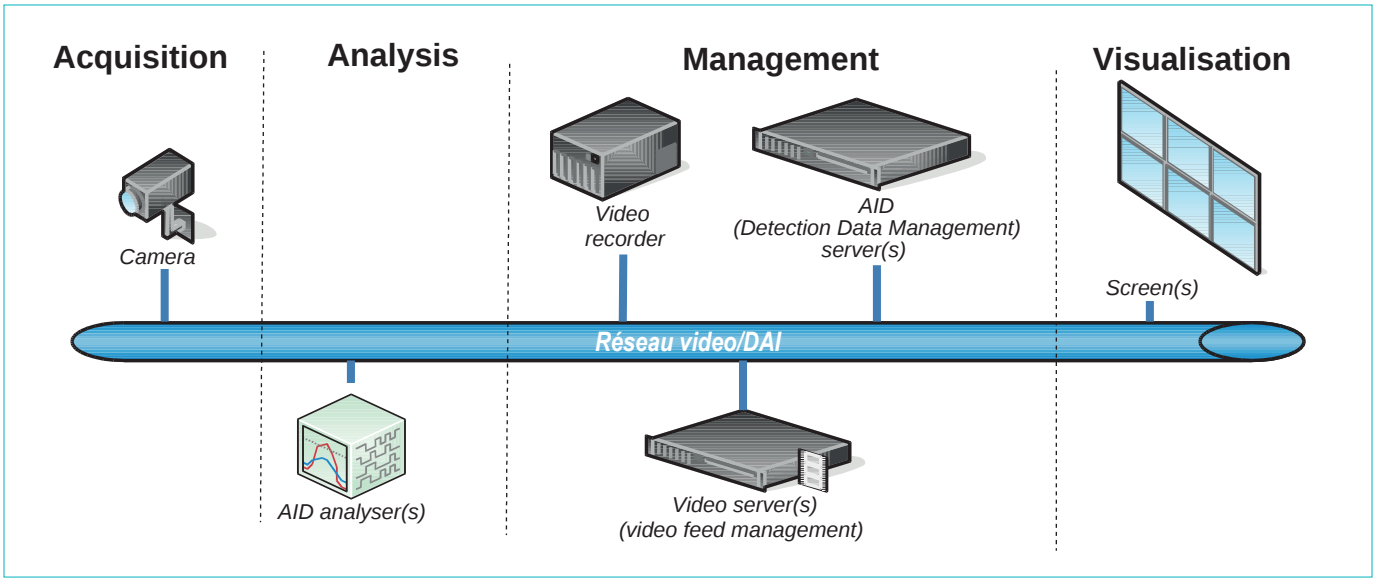


Figure 6: Typical diagram of an AID system

14. The backbone network is the network through which data is exchanged between tunnel systems (SCADA, CCTV, AID, Emergency Call Network, signage oustside the tunnel, etc.).
15. A local computer network grouping together a set of machines logically rather than physically.
16. Human-machine interface enabling the tunnel operator to monitor and control the tunnel's equipment.
17. Management and supervision software developed by the manufacturer of the AID system.

Architecture example no. 1: analysers in the tunnel plant room

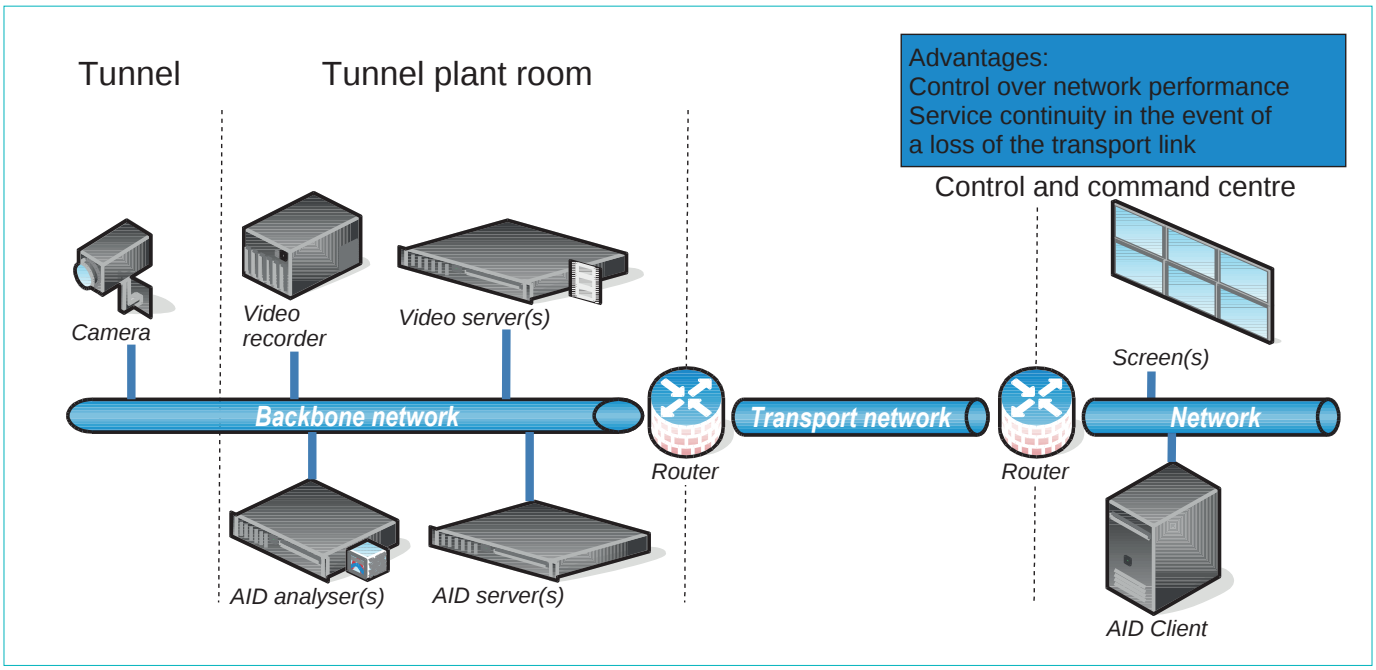


Figure 7: Diagram of an AID system with analysers in the tunnel plant room

This architecture is commonly found in tunnels: all servers and analysers are installed in a plant room within the tunnel. The data acquisition and analysis phases rely solely on the backbone network, which is managed by the tunnel operator (reliability and data throughput). This configuration also allows the system to be used in local mode independently of the link to the control and command centre. This configuration also offers the advantage of ensuring service continuity from the backup control and command centre(s) in the event of a failure of the main centre.

Architecture example no. 2: analysis integrated into the camera

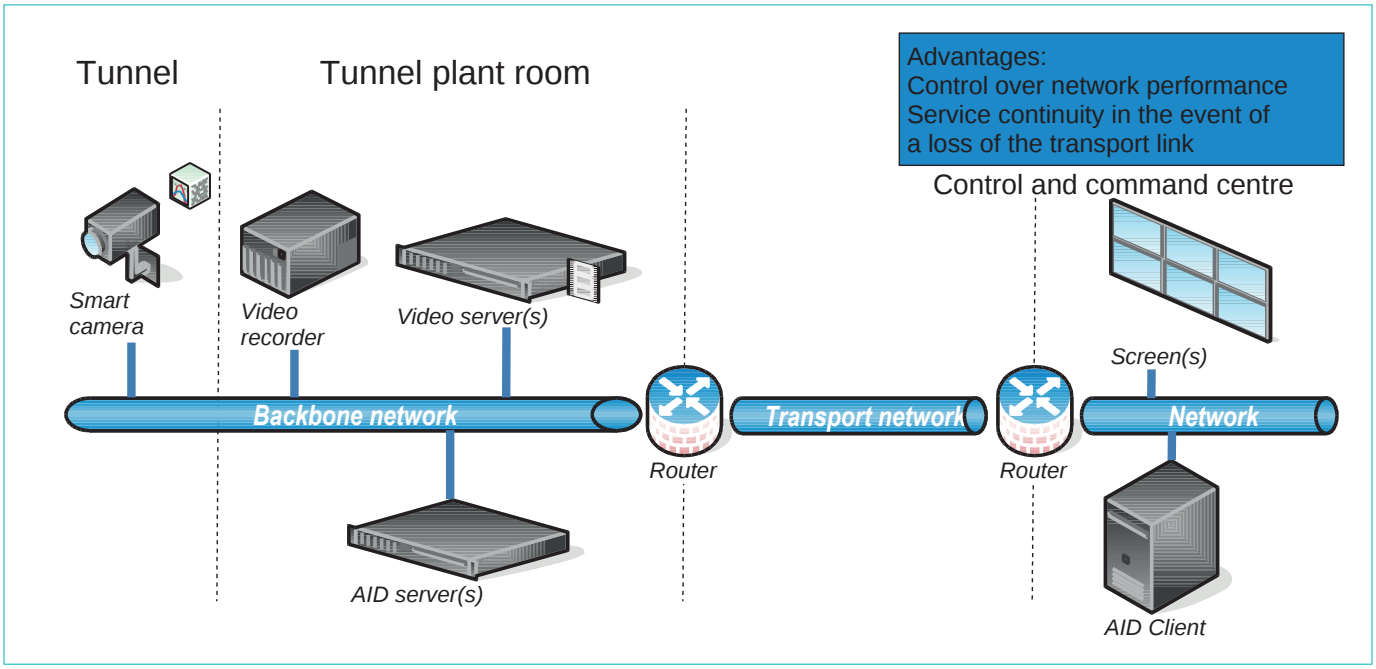


Figure 8: Diagram of an AID system with analysis integrated into the camera

In this architecture, the analysis function is integrated into the camera. The advantages are similar to those of solution 1.

Architecture example no. 3: servers and analysers located at the control and command centre (CCC)

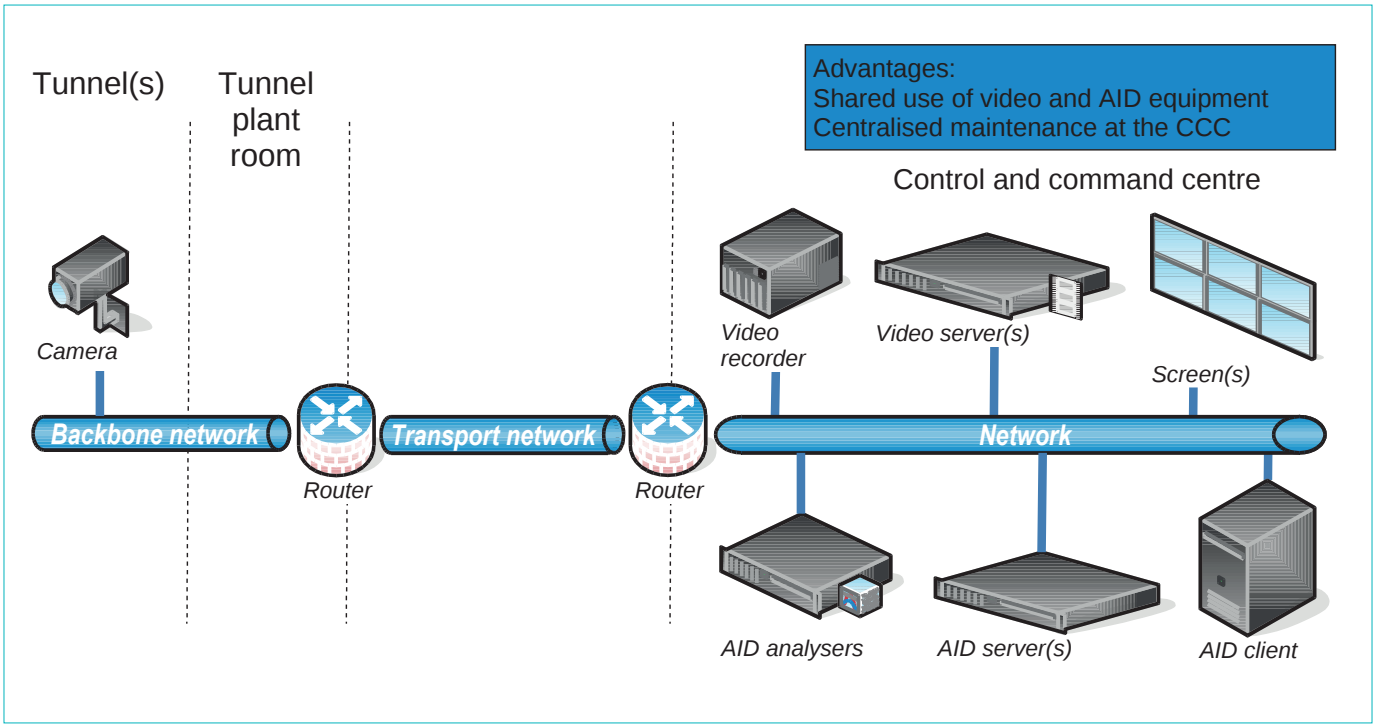


Figure 9: Diagram of an AID system with servers at the CCC

This latter architecture brings together all management and analysis components at the CCC.

Although at first glance this solution appears to offer numerous financial and maintenance benefits, in-depth studies of the system as a whole must be carried out prior to its deployment, taking into account the capacity of transport networks and their reliability (see Chapter 7 – Cybersecurity and System Dependability).

For architectures 1 and 3, it is also possible to pool certain resources (spare analysers[18] between tunnels, server virtualisation, etc.) to improve the system's overall analytical resilience. Architecture 2 limits the loss of the AID function to a small area of the tunnel in the event of a fault in one of the analysers (camera).

Regardless of the architecture chosen by the tunnel owner, resilience must be assessed in light of the tunnel's safety requirements (see Chapter 7 – Cybersecurity and System Dependability).
It is also important to take full account of the constraints relating to upkeep and maintenance.

18. Spare hardware that enables rapid recovery.

5 AID SYSTEM FUNCTIONS

The role of an AID system is to detect abnormal situations occurring in a tunnel. This is its primary function, which must be maintained at all times in an operational tunnel, to assist the operators responsible for monitoring the tunnel. It is also a mandatory function under regulations (see Chapter 2 – Regulatory Aspects).

However, AID systems are equipped with other features, designed in particular to facilitate their use and maintenance.

These various features are outlined in this chapter.

5.1 STANDARD TUNNEL OPERATIONS FUNCTIONS

At the Control and Command Centre (CCC), in the absence of an incident, the screens allocated to the AID may be either in standby mode or in display mode. If in operation, the AID client is active.

As a general rule, as soon as an incident occurs, the sequences detailed below are triggered in succession. This sequence may vary from one system to another. Furthermore, certain sequences may be carried out in parallel.

These sequences are as follows:

- the AID analyser detects the incident, time-stamps it and informs the AID server of the camera, zone/lane and type of incident;
- the AID server may filter the incident according to predefined rules (section 5.2) and applies prioritisation rules;
- the incident is displayed on the AID client along with all the relevant information;
- the video server automatically displays the images from the camera that detected the incident on the screen dedicated to the AID;
- the AID server extracts the sequence corresponding to the incident from the digital video recording (a configurable duration which generally begins 30 seconds before and ends 2 minutes after the incident);
- the AID server may forward any alarms relating to the incident to the SCADA system. The corresponding operational view is activated on the monitoring screen. The incident is pinpointed on the synoptic diagram;
- an audible and visual alarm is triggered at the Control and Command Centre;
- the video footage of the incident can be reviewed to analyse the situation;
- either the incident is confirmed and the operator triggers the appropriate operational scenario (tunnel closure, fire, etc.), or it is a false alarm;
- the operator classifies and acknowledges the alarm.

5.2 OPTIONAL TUNNEL OPERATIONS SUPPORT FUNCTIONS

Several optional functions are available to facilitate operations.

If simultaneous or successive incidents are detected, a "stack" is created. This can be viewed on the AID client, where incidents can be selected individually for display on the screens dedicated to the AID.

Filtering mechanisms over a configurable time period are incorporated into the algorithms to prevent the same incident from triggering a succession of detections, whether on the same camera or on successive cameras. The concept of neighbouring cameras includes up to two cameras upstream and two downstream of the camera in question. It may also apply to cameras that are close by but not in the same line of sight.

These features help to limit alarms that are of no interest to the operator (for example, successive vehicle stops in a traffic jam that has already been detected).

The AID server allows each type of detection to be disabled per camera, per lane and per tunnel tube. These disablements can be applied individually or by group or zone. This function is very useful when the tunnel is not operating normally (e.g due to roadworks) and can be preconfigured as a scenario.

The display durations for detection alarms and for the reappearance of an unacknowledged incident can also be configured by the operator via the AID server.

5.3 MAINTENANCE SUPPORT FUNCTIONS

Maintenance support functions enable the operator to be alerted in the event of a system fault. An AID system can perform self-diagnostics by consulting the technical and operational status of the installation's components.

The AID system can therefore trigger the following alarms:

- **camera movement:** the system triggers an alarm to the control and command centre when it detects camera movement that could impair detection performance. However, this alarm should not be triggered in the event of minor vibrations caused, for example, by vehicles passing near the camera, provided that these do not affect the analysis parameters;
- **deterioration in image quality:** the system triggers an alarm to the SCADA system when the image is no longer of sufficient quality to ensure incident detection and meet the required performance standards. This includes detecting dirt on the window of the housing or a loose lens, for example;
- **loss or degradation of the video feed:** the system notifies the control and command centre of the absence or degradation of the incoming stream;
- **technical and functional faults:** software and hardware faults trigger a technical alarm. These are generally technical faults (such as excessively high processor temperature or any fault leading to a loss of functional availability), or functional faults such as the malfunction of an analysis function, the suppression function, etc.).

The aim of these maintenance support functions is to trigger an intervention to rectify the fault.

Depending on the scope of the intervention carried out, non-regression tests[19] of the system may be necessary.

5.4 ADMINISTRATION FUNCTIONS

The AID server allows the operator to access certain administration functions. Depending on the systems and their administrator functions, the operator can:

- define or reconfigure the areas to be monitored;
- define or modify filtering rules;
- enable or disable detections by incident type, by traffic lane and/or by tunnel tube;
- define and manage system users;
- archive data;
- view and edit the event log;
- reload the saved default settings, which may be useful following a software update;
- display the operational status of AID devices (cameras, servers, etc.).

19. Tests to ensure that functionality and performance are at least maintained at the same level as before the modification.

6 DETECTION PERFORMANCE

The performance level of an AI system – namely its ability to detect incidents and classify them correctly – is assessed using several indicators.

Achieving a high-performing AID system involves finding the best balance between detection rates, false alarms and detection times, which are interdependent parameters.

6.1 ALARM CATEGORIES

The performance of an AID system is assessed according to the alarm categories defined below:

- **genuine alarm (GA):** the system triggers an alarm for the operator, and the human observer, after reviewing the video footage, confirms that the detected incident did in fact occur and corresponds to the alarm. For example, a stopped vehicle is correctly detected as a "stopped vehicle" alarm;
- **false alarm (FA):** the system triggers an alarm for the operator, but the human observer, after reviewing the video footage, finds no incident, or the phenomenon observed is not one that should be detected. For example, a shadow in a tunnel is identified as a "stopped vehicle". This type of alarm is classified as a false alarm;
- **misclassified alarm (MA):** the system triggers an alarm for the operator, but the human observer, after reviewing the video footage, finds that the type of incident does not correspond to the alarm triggered, whilst nevertheless being one of the incidents to be detected. For example, a pedestrian is identified as a slow-moving vehicle. As the alert function has been fulfilled, this misclassified alarm may be counted as a genuine alarm or considered to be a false alarm, depending on the operator's requirements for their system;
- **non-detection (ND):** the system does not trigger any alarm even though an incident, which is included in the list of those to be detected, has occurred.

The incidents detectable by the system correspond to the sum of **GA**, **ND** and, where applicable, **MA**, that is to say, the set of incidents that the AID system must be capable of detecting, if it has been perfectly programmed and is operating at 100 per cent of its capacity.

Under this definition, not every incident is a "detectable incident". For example, the operator may wish for the AID system's algorithm to suppress any detection of an incident occurring on the same camera within 2 minutes of an initial detection. It is therefore normal for this incident not to be detected.

The classification of detections as genuine alarms, false alarms or misclassified alarms must be assessed by a human, namely the project manager or contractor during the testing phase and the tunnel operator during the operational phase. This classification, applied to a representative statistical sample of incidents, enables the system's key performance indicators to be assessed.

6.2 INDICATORS

The indicators defined below are calculated on the basis of the number of genuine alarms, false alarms, misclassified alarms and non-detections.

6.2.1 Definitions

There are six indicators used to define the performance of an AID system:

- **the overall detection rate (ODR)**, which measures the system's sensitivity across all types of incident. It is equal to:

$$ODR = \frac{GA+MA}{GA+MA+ND} \times 100$$

- **the overall false alarm rate (OFR)**, which, for all types of incident, measures the probability that an alarm is false. This rate depends on the total number of alarms reported and requires a sufficiently large sample to be representative. It is equal to:

$$OFAR = \frac{FA}{FA+MA+GA} \times 100$$

- **the detection rate (DR)**[20] which measures the system's sensitivity by incident type. It is equal to:

$$DR = \frac{GA}{GA+ND} \times 100$$

20. For this formula, the MAs must be incorporated into the FAs or GAs, depending on the operator's choice.

- **the false alarm rate (FAR)**, which measures the probability that an alarm of a given incident type is false. This rate depends on the total number of alarms reported and requires a sufficiently large sample to be representative. It is equal to:

$$FAR = \frac{FA}{FA + GA} \times 100$$

- **the false alarm frequency (FAF)**, which represents the number of false alarms per incident type relative to the duration of the sample in days and per camera. This rate, relative to the number of cameras in the tunnel, is representative of the disruption caused to the operator by false alarms.
  Furthermore, a **general false alarm frequency (GFAF)** can be defined, corresponding to the sum of the various FAF values for the types of incidents to be detected;
- **the average detection time (ADT)**, which is defined as the average of the time intervals elapsing between the occurrence of incidents and their detection by the AID system. It is equal to:

$$ADT = \frac{\sum_{i=1}^{N_{det}} (t_d - t_i)}{N_{det}}$$

where:

– N_{det}: is the number of incidents detected,

– t_d: is the time t at which the incident was detected,

– t_i: is the time t at which the incident occurred.

It is important to note that the time at which the incident was detected may vary significantly depending on whether it is observed in very close vicinity to the tunnel (AID client in the plant room) or at the operator's level (alarm raised on the SCADA system). Depending on the objective (acceptance of the AID installation, inspection during the tunnel's service life), one or the other will therefore be prioritised.

6.2.2 Relationship between detection rate and false alarm rate

The indicators – detection rate (DR), average detection time (ADT) and false alarm rate (FAR) – are not independent of one another. Prioritising the detection rate or rapid detection leads to a higher frequency of false alarms, and vice versa. Calibrating the AID system is therefore a crucial step aimed at finding the best balance between minimising missed detections, minimising false alarms and ensuring an appropriate detection time. This adjustment must be carried out with great care.

In terms of configuration, a balance must therefore be struck between settings that detect virtually all incidents but generate a large number of false alarms, and settings that do not detect all desired incidents but limit the number of false alarms.

For a given detection time, the false alarm rate (FAR) increases as the detection rate (DR) increases. A similar relationship exists between the overall detection rate (ODR) and the overall false alarm rate (OFAR).

6.3 FACTORS AFFECTING PERFORMANCE

Numerous factors can influence the performance of an AID system:

- site characteristics (tunnel geometry, type and volume of traffic, location of the portals, natural light penetration, lighting conditions, quality of the transmission network between the tunnel and the Control and Command Centre, etc.);
- the design of the AID system in terms of hardware and software (technologies used, camera layout, design and configuration of algorithms). This design must be adapted to the specific characteristics of the site (see Chapter 4 – AID Equipment);
- the number of AID cameras, as the number of FA events increases with the number of cameras, which in turn depends on the length of the tunnel and the number of tunnels monitored by the CCC;
- the choice of incident types to be detected, as each type of incident to be detected is associated with a specific FAF; increasing the number of incidents to be detected leads to an increase in the occurrence of false alarms and thus undermines the system's credibility;
- the number of features offered, which is likely to increase as technology evolves, but which must nevertheless be kept under control and restricted to what is essential to ensure user safety;
- the software's user-friendliness and how well operators are able to use it;
- the lack of preventive and corrective maintenance (see paragraph 9.3 – Maintenance and inspection measures).

For AID systems connecting with the SCADA system, it should be noted that the characteristics of the network and the SCADA system influence the overall performance of the "detection" safety function. Indeed, any delays in the transmission of information via the network and in the processing of alarms by the SCADA system, may affect the perceived performance of the system, particularly the detection time.

7 CYBERSECURITY AND SYSTEM DEPENDABILITY

In the event of an incident or accident, AID systems are part of the essential safety equipement enabling users to reach a place of safety and emergency services to intervene. For this reason, such systems are powered by an uninterruptible backup power supply to ensure that they continue to operate even in the event of a failure in the external power supply (see 3.1.1 of the French Technical Directive on road tunnel safety in France, dated 2000).

AID systems are also sensitive systems that may be subject to failures or cyber-attacks, jeopardising their integrity.

As they are therefore extensive and critical information systems, AID systems must be resilient in terms of dependability and protected against cyber threats.

This chapter sets out the general principles of cybersecurity and dependability to be applied to AID systems.

The applicable regulatory texts are set out in paragraph 2.3 – Cybersecurity. Further information is provided in Appendix F.

7.1 SECURING TRANSMISSION NETWORKS

To secure AID architectures as described in paragraph 4.4, (Architectures), dependability principles combined with cyber-security principles must be implemented in order to secure all transmission networks used by the system.

7.1.1 Common principles

To prevent a failure from resulting in an operational loss of the AID system, and ultimately a breach of the Minimum Operating Conditions (MOC), the availability of the transmission system (network, switch, router, etc.) must be enhanced.

The architecture must therefore be designed with **redundancies**, without any *single point of failure* (SPOF). In particular, transmission networks must be designed with "path" redundancies at Layer 2 (data link layer – Ethernet) and "route" redundancies at Layer 3 (network layer – IP) of the OSI model[21].

Furthermore, firewalls connecting different networks or used to establish secure connections must be configured with high availability (HA) redundancy, i.e. designed to minimise service interruptions.

Depending on the nature of the tunnel, AID servers may be grouped into a cluster[22] or as virtual machines on a clustered host system.

7.1.2 Securing the backbone network

As all the equipment in the backbone network is deployed in the field, protection and monitoring of physical access to this equipment (plant rooms, switchboards, etc.) are essential.

For local transmission, loop-based architectures are generally used; these enable the network to withstand the loss of a piece of equipment. At the field level, Layer 2 redundancy is used; standardised protocols (such as *Rapid Spanning Tree Protocol* – RSTP) or proprietary protocols (*Hyperring, Turbochain*, etc.) are available for this purpose, enabling the network to be reconfigured in the event of a link failure.

7.1.3 Securing the transport network

Protecting physical access points is more challenging for the transport network than for the backbone network. To ensure the integrity and confidentiality of data transiting through the transport network, **software-based protections** such as *Virtual Private Network* (VPN) tunnels using the *Internet Protocol Security* (IPSec[23]) protocol are therefore employed, established from secure endpoints.

21. The OSI (*Open Systems Interconnection*) model defined by ISO/IEC 7498-1-1994:1994.
22. Group of devices. Notably to ensure high availability. If one device is unavailable, the other can take over operations in a manner that is completely transparent to users. This also enables load balancing.
23. A protocol for securing IP data, used in particular to ensure data encryption within a VPN tunnel.

The method of securing this network varies, depending on the architecture of the overall network into which it is integrated. Security can be achieved by means of Layer 2 redundancy (of the same type as for the backbone network) and Layer 3 redundancy (*Open Shortest Path First* – OSPF and *Virtual Router Redundancy Protocol* – VRRP). A redundant link may be managed by the operator or by a telecommunications provider supplying internet access or via that provider.

An example of a transmission architecture is shown in Figure 10 below.

7.1.4 Coordination of protection

Simple path redundancies (level 2) and route redundancies (level 3) do not necessarily interact in a coordinated manner and may lead to conflicts. Care must therefore be taken to ensure that the protection measures in place are properly coordinated (see Appendix F).

7.1.5 Access arrangements for maintenance operations

Remote access to equipment and servers may be required, both for the installer during the commissioning and configuration phase of the system, and for maintenance technicians (whether from the operator or a third party).

Such access, whether permanent (tunnel operator) or occasional (third party), must be granted with the utmost caution, in accordance with the Information Systems Security Policy (ISSP).

It is essential to set up a remote access portal, accessible for example via an encrypted VPN (IPSec or *Transport Layer Security* – TLS[24]) with mutual authentication of the machines involved in the connection. Strong, multi-factor authentication on the portal must be required of the user, who is granted access to the various machines based on their identity.

It should be noted that equipment and servers should never be directly accessible from the internet. Outgoing encrypted web connections to the remote server – which are generally permitted by firewalls – are undesirable, firstly because they do not comply with the multi-step and multifactor authentication criteria recommended by ANSSI (French national agency for information system security), and secondly because they do not meet the standards expected of an external firewall.

In a highly secure configuration – which is recommended – the remote user is not permitted to upload or download files directly: they must route them via a dedicated machine on the technical network, with the operator at the CCC intervening to relay them to or from the Internet.

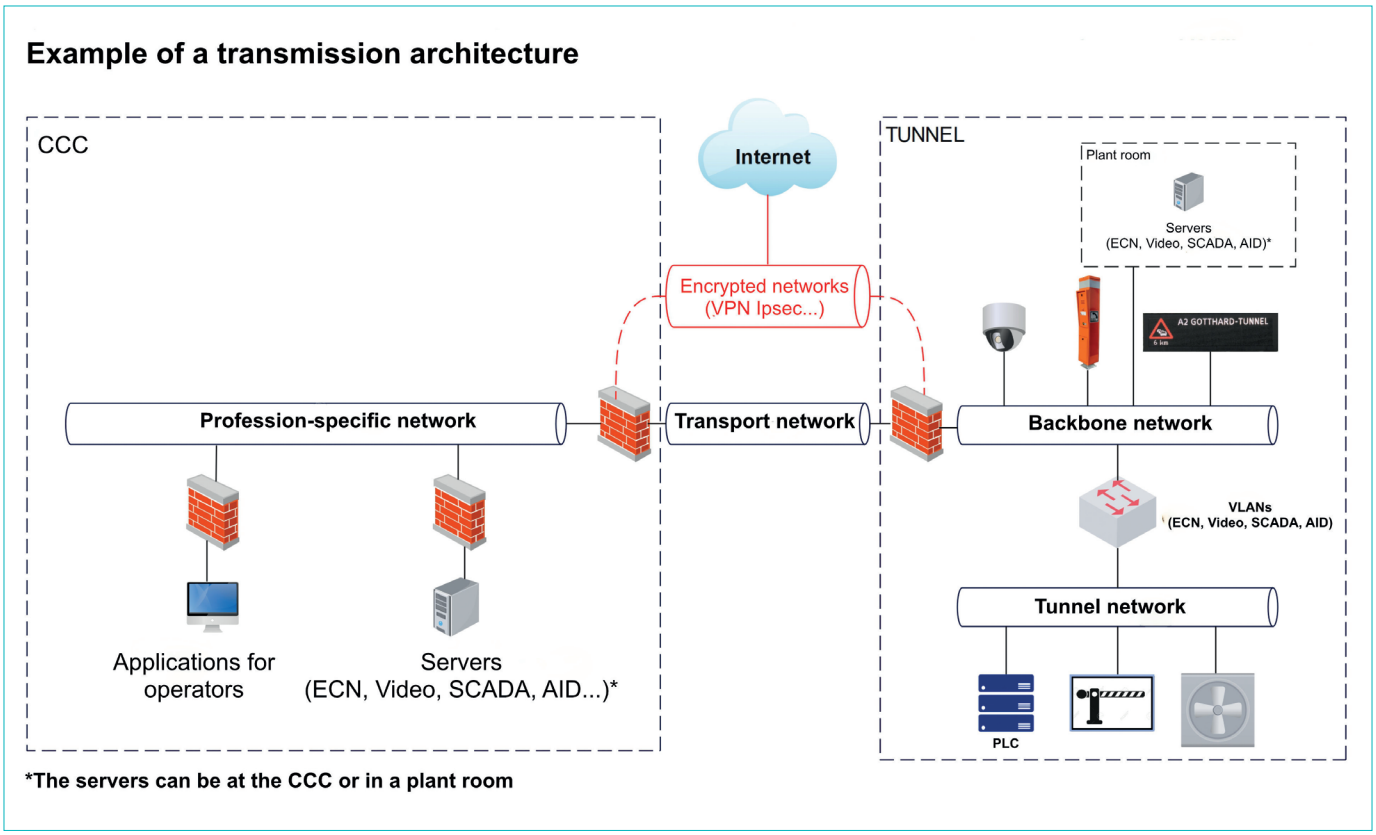


Figure 10: Example of a transmission architecture (© Cerema Sud-Ouest)

24. A protocol for secure communication between a client and a server to ensure the confidentiality (encryption) and integrity of data.

7.1.6 Operation without Internet access

To reduce the risk of intrusion via cyber-attacks, all field equipment and servers must operate in nominal mode without needing to access services or servers on the Internet ("on premises" operation).

In this context, certain devices are still necessary for the system to function, notably time and name servers. Time servers (*Network Time Protocol* – NTP[25]) and name servers (*Domain Name Server* – DNS[26]) are fundamental local or relay devices that are commonly used. When configuring these servers, it is important to ensure their settings allow them to operate without an internet connection.

7.2 SYSTEM UPDATES

AID software is potentially vulnerable, which means it must be updated regularly and patches published by the software vendors must be applied rigorously. It is unwise to leave the system unpatched.

Where possible, the compatibility of updates should be tested on a partial replica of the system operating outside actual operation, using dedicated machines, whether physical or virtual.

When part of the system is obsolete and no longer receives security updates, the operator must implement additional security measures (disconnection, adding proxy servers in *the Demilitarised Zone* – DMZ[27]…) to mitigate the risk of exposure, whilst awaiting the system's replacement.

It is also important to note that, in cybersecurity, there is no such thing as zero risk, particularly due to "*zero-day*" vulnerabilities – that is, flaws in software or a system that are discovered by an attacker and for which there is as yet no known patch. A vulnerability of this type cannot be ruled out in an AID system.

Business continuity plans (BCPs) and disaster recovery plans (DRPs) must therefore be drawn up in line with the Information System Security Policy (ISSP) and tested during exercises.

25. A protocol enabling time synchronisation between multiple machines.
26. An IT service that maps internet domain names (web addresses) to their respective IP addresses.
27. A network location generally situated between two firewalls to secure a local network from internet traffic. This zone hosts machines required to provide direct communication with the internet.

8 FROM DESIGN TO ACCEPTANCE: THE DEVELOPMENT STAGES OF AN AID SYSTEM

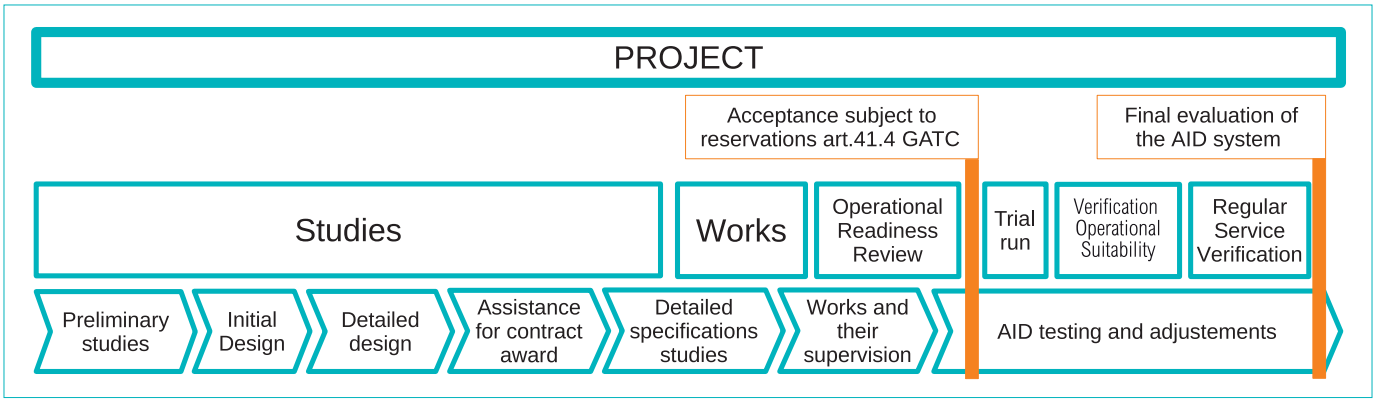


Figure 11: Diagram of the different phases of a project

The performance of an AID system depends first and foremost on the care taken in its design, which must be integrated and carefully thought out, taking into account interactions with the tunnel's other safety systems.

The testing phase, which begins once the works phase is complete, is another crucial phase, as it validates the system's proper functioning. This validation comprises three stages:

1. **Operational Readiness Review (ORR)**, which involves verifying technical and software functionality, as well as incident detection. In the case of tunnels already in operation, this is generally carried out during a tunnel closure. Once the works are deemed to comply with the contract, acceptance is granted subject to the validation of detection performance, resulting in the transfer of ownership of the system to the tunnel owner[28].
2. **The Regular Service Verification (RSV)**, during which the contractor that carried out the works adjusts the system under real traffic conditions, in collaboration with the manufacturer, in particular to reduce false alarms.
3. **The validation of detection performance**, which consists of simulating incidents whilst the tunnel is closed to verify the performance achieved at the end of the RSV period, and is ultimately intended to lift any reservations.

Strict adherence to these stages is essential to ensure compliance with the contract specifications and the system's effectiveness prior to its final validation (see the CETU guide, *Equipement for road tunnels and urban guided transport systems : Tests, acceptance and guarantees* (2019) - available in French).

8.1 DESIGN STUDIES

Design studies comprise, in sequence, preliminary studies, initial design studies and detailed design studies. Once the tunnel operator is identified, it is necessary to involve them in these various stages.

By the end of the design studies, at least the following elements must have been defined:

- **site constraints** (geometry of the tunnel, critical points, structural characteristics, etc.);
- **operational constraints** (permitted road gauge, procedures for maintenance work inside the tunnel, other operational constraints). For safety and durability reasons, no camera must encroach upon the headroom or the lateral protective clearances of the tunnel;
- **the traffic study** (type and volume of vehicles using the tunnel);
- **operating procedures for the video surveillance system** (in particular, if the service providers or installation timelines differ between the AID system and video surveillance systems, a detailed description of the video surveillance system – camera locations, technical specifications – must be provided);

28. Article 41.4 of the General Administrative Terms and Conditions (French public procurement contracts): "*In cases where, in accordance with the provisions of the Specific Administrative Terms and Conditions, certain tests must be carried out after a specified period of service of the infrastructure or at certain times of the year, acceptance may only be granted subject to the successful completion of these tests.*"

- **the rules for managing faults** (list of technical and functional anomalies that must trigger an alarm to facilitate maintenance – see paragraph 5.3);
- **the procedures for integration into the SCADA system** (information required for integration, including communication protocols and alarms associated with technical and operational incidents);
- **detection specifications** (list of incidents to be detected – see Chapter 3 – with precise requirements regarding detection rates, false alarm frequency and detection time – see paragraph 6.2. The following table may serve as an example for drawing up this list.

Target values must be set according to the specific tunnel characteristics (geometry, traffic, etc.).

The detection rate to be achieved is generally between 80 and 98 per cent. The closer one aims to get to a detection rate of 100 per cent for a particular type of incident, the greater the risk of worsening the false alarm rate.

The maximum permissible **false alarm rate** is generally between 0.025 and 0.150 per camera, per day and per incident type. This parameter must be adjusted according to the CCC's configuration (number of AID cameras feeding into the CCC, across all tunnels and incident types to be detected, number of operators on duty, etc.) so that the total number of false alarms (the cumulative total of false alarms at the CCC over a single day) remains acceptable to the operator(s).

Finally, the maximum expected **detection time** may range from 2 to 20 seconds.

Incident	Minimum detection rate (%) to be achieved (GDR or DR)	Maximum permissible false alarm frequency (FA/camera/day)	Maximum expected detection time (in seconds)
Stopped vehicle			
Fire			
...			

Figure 12: Table of performance requirements to be met

8.2 PROCUREMENT DOCUMENTATION

The technical specifications of the AID system, including the table of minimum performance requirements defined during the design phase, are included in the procurement documentation. These elements are supplemented by a list of documents that the company must provide in support of their tender. In particular, these include:

- **justification of the video and AID coverage**, which must include a camera layout plan and associated cross sections; it must take into account important safety areas (emergency call stations, emergency exits, lay-bys, etc.) to ensure optimal visibility of these areas, by positioning them at the start or in the middle of the field of view (paragraph 4.1.3 – Coverage and Layout);
- **the Security Assurance Plan (SAP)**, a contractual document describing the measures the tenderer plans to implement in order to meet cybersecurity requirements. Each relevant cocontractor or subcontractor must draw up a SAP that complies with the client's Information Security Policy (chapter 7 – Cybersecurity and System Dependability). Once the service provider has been selected, the SAP is appended to the contract and supersedes any generic clauses;
- **the general functional specifications** of the video surveillance and AID system;
- **a description of the human and material resources deployed** by the contractor to carry out the various tests, in particular performance tests.

8.3 DETAILED SPECIFICATIONS STUDIES

Once the contract has been signed, the contractor carries out the detailed specifications studies. From the works preparation phase onwards, the contractor must provide:

- **a detailed coverage study with on-site photographs** (paragraph 4.1.3 – Coverage and Layout), which takes into account the equipment installed or planned for installation in the tunnel in order to minimise visual obstruction effects;
- **the camera positioning study**, which must prioritise the installation of cameras on the tunnel ceiling, taking into account the headroom and the lateral clearance margins to minimise visual obstruction caused by heavy goods vehicles;
- **the detailed functional specifications**, which describe the precise functionalities of the video surveillance, AID and recording systems;
- **the Technical Specifications for Equipment (TSE)**, which cover all planned equipment;
- **the interface specifications**, which define the connections to the backbone network, the transport network and the SCADA system;
- **the architecture diagrams**, which illustrate the integration of video surveillance and AID, both in terms of equipment within the tunnel and systems installed in plant rooms;
- **the integration and layout plan**, which details the layout of the equipment in the tunnel, ancillary rooms and the Command and Control Centre, as well as the cable routes.

It is strongly advised not to commence work on installing the cameras until the camera positioning study and the detailed functional specifications have been approved. An assessment procedure must be explicitly included in the contract to ensure this prior to approval.

8.4 WORKS

During the works phase, it is essential to verify that the works carried out comply with the previously approved contractual and technical documents.

This verification covers the following points in particular:

- **camera layout** (verification of their positioning, ensuring they are compatible with the tunnel's vertical and lateral clearance);
- **fields of view and any obstructions** (validation of viewing angles to ensure optimal coverage and identify any areas of visual obstruction);
- **cable routing** (inspection of the routes taken by the cables, in accordance with the installation plans and applicable standards);
- **mounting of the housings** (verification of the strength and stability of the fixings, as well as corrosion resistance, to ensure the durability and safety of the installations).

8.5 SPECIFIC AID SYSTEM TESTS

The overall video surveillance/AID system must undergo rigorous testing to validate the proper functioning of the AID system.

These tests are carried out in the presence of the project manager, the contractor, the manufacturer of the AID system and, where possible, the tunnel operator.

To ensure rigorous monitoring, test specifications documents are validated in advance by the project manager and completed as and when required:

- factory test acceptance specifications;
- simulator test acceptance specifications;
- equipment installation logs;
- final AID evaluation test logs.

AID system tests take place at various locations (factory, simulator or site) and follow a sequence: static tests, followed by partial acceptance tests (PAT), system acceptance tests (SAT) and finally global acceptance tests (GAT), which enable the verification of all equipment and maintenance support and detection functions, first whilst the tunnel is closed, then whilst traffic is flowing during the RSV.

Following the global acceptance tests, the checks prior to the Operational Readiness Review (ORR) are conducted by the project manager. They aim to determine whether or not the AID system can be handed to the tunnel owner.

If the checks prior to the ORR are inconclusive, acceptance is not granted and the contractor must carry out corrective work until the system can be accepted.

This acceptance is granted subject to the completion of the RSV, during which the contractor carries out system adjustments under real-life traffic conditions.

It is only at the end of the RSV, once all reservations have been resolved, that final validation of the AID system can be granted.

8.5.1 Tests prior to the ORR

Functional tests

The checks begin with functional tests, the purpose of which is to verify the operation of the equipment and support functions defined below.

Examples of tests are provided in Appendix C. The tests described constitute a framework to be adapted to the specific characteristics of each installation, given the variability of AID systems.

Some of the tests may be carried out at the factory or on a test platform to validate the interfaces and the proper functioning of the system prior to its deployment at the tunnel site.

Each piece of equipment comprising the AID system must be tested individually. The checks involve ensuring that the cameras, analysers, servers, AID client, and transport and communication networks are all properly powered and operational.

The basic support functions that the system must provide must also be verified, including in particular:

- internal communication between the system's equipment;
- communication between the AID system and related systems (SCADA, video wall, etc.);
- AID administration and configuration functions;
- maintenance support functions for AID equipment (camera movement, etc.);
- the recording, management, viewing and archiving of digital video footage;
- the operation of redundancy systems (servers, analysers, etc.);
- the transmission of technical alarms from the system.

These checks should be carried out via the AID client both locally and remotely (maintenance centre, operations CCC, backup CCC, etc.).

Performance tests

Once the functional tests have been validated, a detection performance test phase must be carried out to ensure that the AID installation complies with the performance levels defined in the contract.

In the case of a new tunnel or existing tunnel where the refurbishment includes the CCTV and the AID systems, these tests may only commence once testing of the CCTV system and the tunnel's communication networks has been completed (Partial Acceptance Tests, System Acceptance Tests). This is because video coverage, image quality and the quality of the backbone network are prerequisites for AID testing.

Performance tests are essential and the time required for them must not be underestimated. This phase may require significant resources in terms of personnel and equipment: light vehicles, pedestrians, drivers, a smoke generator and its power supply, etc. It also takes time, as the tests must be carried out for each type of incident, on each camera and for each lane. Furthermore, to calculate detection rates, the same tests must be carried out several times.

Alarm signals are verified via the AID client terminal to assess intrinsic performance, and then via the SCADA system to verify the integrity of transmissions.

Appendix D sets out proposals for testing incident detection functions, in accordance with the classification set out in paragraph 3.2.

Furthermore, it must be verified that the operation of other systems and equipment installed in the tunnel (changes to lighting modes, dynamic sign display, etc.) does not trigger false alarms.

No changes to settings – with the exception of the disabling of detection functions and filtering rules – must be made during this phase. When testing a given function, all other detection functions must be disabled.

For each incident to be detected, performance is calculated by taking the average of the results obtained from all cameras. These are then compared with the requirements set out in the contract.

A minimum number of tests must be carried out. This is determined according to the tunnel's characteristics: number of lanes, tunnel geometry, number of cameras, selected functions, etc.

Some tests may involve several cameras simultaneously. For example, in the case of the test for the function "Stopped vehicle" at the start of camera *n*'s field of view; the stopped vehicle can also be detected at the end of camera *n*–1's field of view.

Along the tunnel's interior zone, tests can be carried out during the day or at night. The tunnel's lighting regime may be set to the lowest level.

At the tunnel entrances and exits, it may be advisable to prioritise daytime tests to cover as many adverse operating conditions as possible. This is because image analysis can be influenced by weather conditions outside the tunnel: strong sunlight, a wet road surface at the tunnel entrance, etc.

It should be noted that if the AID system is equipped with a video recording analysis function, it is advisable to save the test footage. These reference videos may be used at a later date to ensure that there is no deterioration in system performance during maintenance operations (see paragraph 9.3.6 – Software maintenance).

By way of illustration, Appendix E presents an example of a performance test sheet for stopped vehicle detection and a summary sheet of the observed performance.

The results obtained from all incidents enable the detection rates for each type of incident to be calculated. A summary by camera is a means of identifying any malfunctions. If performance meets the procurement specifications, acceptance may be granted subject to validation of performance following the RSV. Otherwise, corrective measures must be taken and the tests repeated. Any modification to a camera requires a full repeat of the corresponding tests.

8.5.2 System adjustments during the RSV period

Once acceptance has been granted, subject to the conditions outlined above, the general trial run of the tunnel's safety equipment begins (in the case of new tunnels), culminating in the Verification of Operational Suitability (VOS), following which the AID system is put into service (see the CETU guide *Road Tunnels and Urban Guided Transport Systems – Testing, Acceptance and Guarantees*, 2019).

The Regular Service Verification (RSV) then begins, for both new and refurbished installations. Its aim is to verify that the services provided by the system can function under the normal (regular) operating conditions specified in the contract.

The duration of the RSV, which depends on the complexity of the AID system, is generally three months. If problems are encountered during this phase, it may be extended, for example, to up to six months.

During this period, operational data from the AID system is collected and, following analysis, provides an indication of the system's actual performance. These field observations make it possible to verify with certainty which alarms are genuine, which are false and which are misclassified, and consequently to determine the rate and frequency of false alarms. Any system faults are thus precisely identified and steps can be taken to rectify them.

Identifying missed detections is particularly complex, as these do not trigger any sequence or alarm from the system. They can, however, be detected by operators or through systems complementary to the AID system, such as an opacimeter signalling the presence of smoke.

Another method involves the visual analysis of video recordings made continuously over a given period (one or more weeks). These recordings make it possible to identify incidents that could potentially have been detected by the AID system during that period. The list of incidents thus compiled is then compared with the detections actually reported by the AID system.

Ideally, this approach requires each recording of sufficient duration to be viewed carefully by an observer, in order to ensure a reliable assessment. However, due to the significant resources it requires, this method is rarely feasible.

To streamline this process, it is possible to ask the AID system manufacturer to carry out a performance audit in conjunction with the tunnel operator. This involves a monitoring period of several weeks, during which the operator records all observed anomalies – including non-detections and false alarms – in a dedicated document, broken down by camera. Each incident generates a sequence in the form of a video file comprising images taken before and after the incident. These sequences are often sufficient to understand anomalies such as false alarms. Based on the results of this audit, any unsuitable configurations of the AID system are amended. In the event of substantial changes, a new phase of performance testing must be carried out (see paragraph 8.5.1 – Checks prior to the Operational Readiness Review (ORR).

Throughout this RSV period, changes may be made either locally or remotely via an encrypted virtual private network (VPN) compliant with ANSSI recommendations (see paragraph 7.1.5 – Access arrangements for maintenance operations), using the system's administration functions.

8.5.3 Validation of system performance

Once all the tests carried out in accordance with the method described in this chapter have proved successful, the system may be declared validated by the lifting of any reservations raised at the time of acceptance.

Figure 13 opposite summarises the AID system validation process.

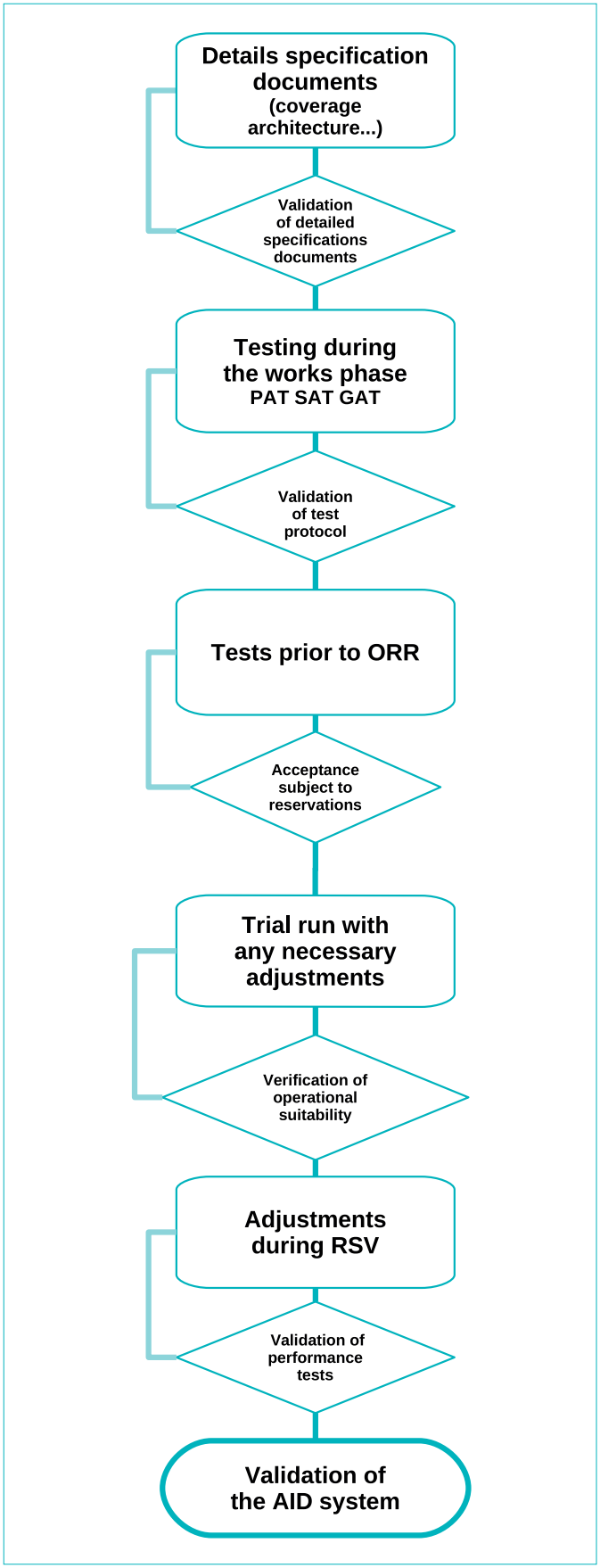


Figure 13: AID system validation process

9 ACTIONS TO BE TAKEN DURING THE OPERATIONAL PHASE

9.1 GENERAL REMARKS

Maintaining the condition and performance of AID systems throughout their service life is a major challenge for tunnel operators.

For certain tunnels, a failure of this equipment, which contributes to several safety functions, may result in a situation below the minimum operating conditions and therefore lead to the closure of the tunnel.

A failure, or even a simple decline in the performance of the AID system, can also lead to situations that are critical to personal safety, if an event that should in principle be detectable by the AID system is not detected.

A total loss of the AID system is usually easily identifiable during routine operation.

Feedback from tests carried out since 2010 by the CETU, particularly during Periodic Detailed Inspections (PDIs), has shown that a significant deterioration in the system's performance may, however, remain undetected by the tunnel operator for a very long time. This situation increases the risk that an incident may escape the operator's attention, delaying the rapid action required in such circumstances.

To ensure that users retain confidence in this system over time, it is important to regularly check, throughout its service life, that it remains capable of fulfilling its functions in the event of an incident.

The verification procedures to be carried out, as shown in the figure below, are detailed in sections 9.3 – Maintenance and inspection measures and 9.4 – Detailed inspections.

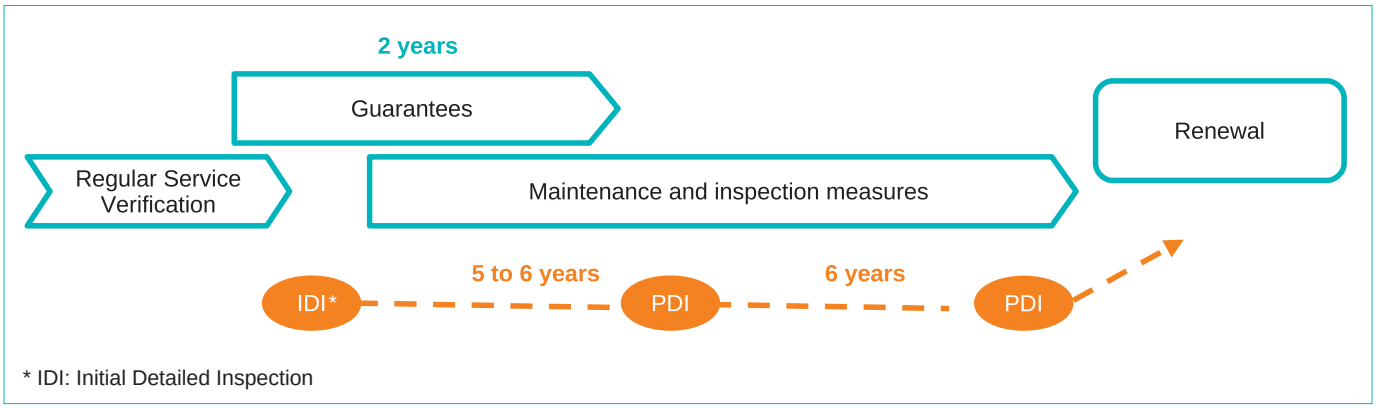


Figure 14: Overview of actions during the operation of the installation

9.2 GUARANTEES

Chapter 5 of the document "*Equipment for Road Tunnels and Urban Guided Transport Systems: Testing, Acceptance and Guarantees*", published in June 2019, sets out recommendations regarding the contractual guarantees for works contracts. The guarantee period begins upon acceptance of the installation.

A distinction is made between the regulatory guarantees defined in the General Conditions of Works Contracts, such as the guarantee of perfect completion, and specific guarantees which may be provided for in the works contract in question. In this regard, provision may be made to extend the guarantees for AID equipment: cameras and their housing, analysers, servers, software, etc. In the absence of specific provisions, this equipment is covered by the regulatory guarantee of conformity applicable to digital equipment and products. These provisions also cover the software component.

9.3 MAINTENANCE AND INSPECTION MEASURES

9.3.1 Maintaining performance

The main objective of maintenance is to ensure the system's long-term reliability by preventing a decline in performance over time.

Maintaining performance relies on the proper functioning of each system component (cameras, analysers, AID software, etc.) as well as that of the "support" equipment (power supply, networks and monitoring systems). It is therefore important to check the condition and proper functioning of this equipment.

As discussed previously, the performance of an AID system is a trade-off between detections (detection time and rate, missed detections) and false alarms. To maintain a good level of system performance, care must be taken to ensure that the performance levels of these interdependent parameters do not deteriorate over time.

An increase in the frequency of false alarms is generally easy to detect due to the disruption caused to the tunnel operator during the day-to-day operation of a tunnel. However, only by comparing the system's performance with actual events on site can a deterioration in the system's ability to detect incidents be identified. Failures to detect incidents can be identified during day-to-day operations by cross-referencing data from other systems such as the emergency call network, SCADA system reports (opening of emergency call station and emergency exit doors, pollution sensors, etc.), or the "logbook", or even a report from a control room operator following the visual observation of an undetected incident.

As not all undetected incidents can be identified in this way, it is nevertheless necessary to simulate incidents by carrying out specific interventions within the tunnel. Simulating incidents in tunnels is an operation which, in addition to human and material resources, requires the closure of the tunnel, which can prove difficult to implement. In this context, utilising "incidents" generated during routine operational tasks, construction works or maintenance may offer a useful partial alternative. For example, a patrol vehicle stopping for a one-off operation, or the setting up or removal of traffic cones, can be used as an "incident" to ensure that the system correctly detects a stopped vehicle or a vehicle travelling in the wrong direction.

To optimise the use of this data, a system must be put in place to trace these incidents as and when they occur, including routine operational incidents (such as a patrol vehicle stops). Whilst minimising disruption to tunnel operation, this traceability system allows the recording of as many genuine "incidents" as possible relating to user traffic, as well as to maintenance work or construction projects within the tunnel, and enables the creation of an "incident" database. To ensure that it remains acceptable, credible and sustainable, the implementation of this traceability system must not be overly burdensome. Its level of detail and the time allocated must be tailored to the context (for example the number of tunnels operated by the CCC), but also to the results of the analyses.

9.3.2 Principles of corrective and preventative maintenance

Two main types of maintenance can be distinguished for a video surveillance/AID system: corrective maintenance and preventive maintenance.

Corrective maintenance is carried out when equipment unexpectedly fails. In order to be able to quickly resolve the problem of the system being wholly or partially unavailable, a stock of spare parts suited to the system's architecture must be provided (see Appendix G1 – Spare Stock).

Preventive maintenance consists of scheduled routine servicing, checks, tests, replacement of hardware components and "support" equipment, as well as software updates. An example of a preventative maintenance programme is given in Appendix G2. It should be noted that preventative maintenance is to be prioritised as it allows for the planning of interventions and ensures that equipment remains in good working order throughout its service life[29].

Furthermore, 'light' but frequent checks (daily, weekly, monthly) should be prioritised over extensive maintenance campaigns carried out at long intervals (every few years), which may result in system malfunctions being detected too late.

For the simpler tasks, some of these maintenance operations on the video/AID system can be carried out in-house, whilst the more complex ones can be contracted out to specialist service providers. It should be noted that granting remote access for these operations requires a prior assessment of cybersecurity risks (see paragraph 7.1.5 – Access arrangements for maintenance operations).

29. Appendix C of Booklet 40, "*Tables of Preventive Maintenance Tasks*", details the various preventive maintenance tasks and the intervals at which they should be carried out on tunnel systems.

9.3.3 Routine maintenance and continuous monitoring

Routine maintenance, the first level of preventative maintenance, involves the cleaning and periodic inspection of the condition of the imaging equipment (level of dirt on the windows of camera housings, immobility of housings, etc.) and the video/AID network (level of dust accumulation on servers, adequate ventilation of server racks, etc.).

Continuous operational monitoring can be carried out primarily using maintenance support functions, which enable the technical condition of equipment contributing to the AID system to be continuously checked and tested (see section 5.3 – Maintenance support functions). Technical alarms can also be displayed on the Human-Machine Interface (HMI) of the tunnel's SCADA system. Furthermore, visual checks to ensure proper operation must be carried out using the available front-end terminals (checking for the presence of video streams and image quality, verifying the consistency of detection masks within the image, etc.). Regular connections to the equipment enable monitoring of processor loads, memory usage, remaining disk space, etc., and the identification of early warning signs of malfunctions.

Figure 15: Dirt on the housing window of an AID camera

9.3.4 Performance audit

A performance audit of the video surveillance/AID system, similar to that carried out during the RSV, enables the number of false alarms – and therefore the frequency of false alarms – to be objectively assessed, and any issues relating to non-detection to be identified.

Analysing the AID alarm log enables a record to be compiled of genuine and false alarms. By reviewing the footage relating to the alarms, their classification (genuine, misclassified or false) and the accuracy of their count can be verified. Implementing comparative monitoring over time also helps to identify analysis anomalies for certain cameras.

Comparing the AID alarm records with incident data derived from external sources (incident log book, SCADA system data, etc.) helps to flag up issues relating to missed detections.

However, this audit does not provide sufficient data to assess overall performance across all cameras and detection types. Specific tests still need to be scheduled.

Figure 16: Poor image quality from a camera with a dirty housing window

Figure 17: Video feed from a camera that has moved (misalignment of the masks)

9.3.5 Scheduled tests

Scheduled tests must be carried out to supplement the other checks.

Firstly, in order to regularly check the detection capability for one of the highest-priority incident levels, "stopped vehicle" tests may be carried out in specific areas of the tunnel (near emergency exits or emergency call stations, for example). It may be appropriate to combine this test with other maintenance operations carried out periodically within the tunnel. For example, parking a vehicle at a location where a recurring maintenance task is to be carried out can constitute an "incident" that allows the detection function to be checked regularly. The alarm activation can be checked at a later time.

Furthermore, all detection functions must be checked during more extensive detection test campaigns. The aim is to simulate all types of incident on site, including those that occur infrequently (fire, wrong-way driving), and to verify detection on a representative sample of cameras, without, however, being as comprehensive as during the initial acceptance phase. The "stopped vehicle" detection function, for example, is tested once on each camera.

These performance checks on the AID system must take into account the entire chain, which includes the interface used by the operator, and must not be limited to an examination of the AID client alone. Indeed, during maintenance phases, it is common to find that the performance of the overall system is lower than that of the AID system on its own.

9.3.6 Software maintenance

Software maintenance involves carrying out:

- data purging operations and software version updates (security updates for operating systems, firmware, drivers, etc.). These actions may be carried out in-house or by a third-party contractor;
- fine-tuning of algorithms following the detection of performance deviations. These adjustments are implemented in the form of patches. It is recommended that a maintenance contract be established to cover this aspect of maintenance. This contract should commence immediately upon the expiry of the guarantee period. It is generally concluded with the AID system supplier.

Where the results of preventive maintenance operations (functional checks, performance audits, scheduled tests) reveal malfunctions or a decline in performance, the data collected should be forwarded to the maintenance contractor so that they can carry out adjustments and propose software updates.

These software updates, particularly on the analysers, require non-regression testing. These tests involve simulating a number of incidents on-site to ensure that alarms are correctly triggered and that they are consistently transmitted to the operator level. If the hardware configuration has not changed (no optical modifications, no reorientation of cameras, etc.), and if the system enables it, replaying incident images on the analysers can be used to verify nonregression.

Maintenance task	"Assessable" parameter	Sources	Sample concerned
Performance audit	Frequency of false alarms Non-detection	"Incidents" identified during the operational phase, or during works: AID alarm log, external sources (Emergency Call Network, SCADA, etc.)	A few cameras and only common types of incidents (stopped vehicles)
Scheduled tests	Detection time and rate Non-detection	Simulated "incidents": alarm log	All cameras and all types of detection

Figure 18: Parameters assessed during maintenance and inspection operations

9.4 DETAILED INSPECTIONS

In accordance with the recommendations of Booklet 40[30], Initial Detailed Inspections (IDI) and Periodic Detailed Inspections (PDI) of the equipment must be carried out by a body external to the operator throughout the tunnel's service life.

These inspections are in addition to the continuous monitoring carried out by the tunnel operator.

The IDI involves establishing a baseline for the condition and performance of the equipment. It applies to new installations or those that have undergone substantial refurbishment. This inspection does not replace the monitoring operations carried out under the works contract (see paragraph 8.3 – Detailed specifications studies). Experience has shown that it is preferable for it to take place a few months after equipment becomes fully operational, so that the system's operation has stabilised and the final reservations have been lifted.

30. *ITSEOA Application Guide, Booklet 40: Tunnels – Structural Elements and Equipment (available in French).*

The IDI comprises a documentary analysis of the As-Built Documentation, supplemented by a site visit to the tunnel, during which an inspection of the condition of the equipment, functional tests and performance measurements are carried out, similar to those performed during an PDI.

The PDI, carried out every six years, includes a site visit to the tunnel to provide a one-off assessment of the condition and performance of the equipment. The following operations are carried out by the inspectors on the video and AID systems:

- a visual inspection of the condition of the equipment (cameras within the tunnel, analysers and servers in the plant rooms, video wall in the control centre, etc.) using appropriate access methods;
- a check on the system's operation (alarm triggering upon detection, automatic display of images on monitors, storage and viewing of AID footage, etc.);
- performance tests (detection times and rates) on a few incidents that are easy to simulate.

When carrying out performance tests, several principles must be taken into account:

- there must be no concurrent activity – at least in the areas where the tests are being carried out – so as not to distort the results with "incident interference";
- performance must be assessed by considering the alarm chain as a whole, taking into account the actual operating conditions of the AID system. Consequently, alarm notifications must be verified on the interface used by operators on a day-to-day basis, using the current operational configuration, including any filters applied (the analysis of the results must take these into account). An inspector must therefore be present at the control and command centre;
- with regard to sampling (type of detection and location), priority should be given to verifying Level 1 detection functions (stopped vehicle, fire). This involves carrying out, on at least one camera, a test for each of these functions and for each traffic lane.

For the "stopped vehicle" function, it may be appropriate to carry out the tests in the vicinity of user facilities (emergency exits, emergency call stations).

Furthermore, it may be useful to simulate stopped vehicles at the edge of a camera's field of view, before the vehicle enters the field of view of the next camera.

The Level 2 and 3 incident detection functions that are easiest to simulate must also be verified in a few areas of particular concern.

The assessment of tunnel equipment forms an integral part of the detailed inspection report and is presented to the tunnel operator in the form of a score by equipment category. In accordance with the recommendations of Booklet 40, two scores are assigned: a "C" score for the assessment of condition, and a "P" score for the assessment of operation and performance.

Two additional symbols are used to highlight issues relating to the maintainability of the system – the "M" symbol – or where safety is directly compromised – the "S" symbol.

Maintenance issues (marked 'M') commonly observed in the field are linked, amongst other things, to equipment deterioration (for example, a camera housing orientation adjustment system jammed by corrosion) or the unavailability of spare parts on the market (for example, the unavailability of spare parts for analogue video networks).

Safety (marked "S") may be compromised either by faults relating to the condition or to the operation of a system. These include, in particular, the risk of components falling as a result of impacts or damage caused by corrosion of fixings (for example, pitting corrosion of bolts and fixtures) or performance that is wholly inadequate for a Level 1 detection function.

The results of detailed inspections enable the operator to improve their maintenance programme and assist in their decision-making when planning the renewal of the installation.

For further information on detailed equipment inspections, the reader may refer to the following documents:

- "Appendix A – Checks and tests to be carried out during an initial detailed inspection of equipment (excluding design checks)" in Booklet 40 (in French);
- "Appendix D1 – Checks and tests to be carried out during a periodic detailed inspection of equipment" in Booklet 40;
- "Appendix D2 – Guidelines for the assessment of equipment" in Booklet 40.

9.5 RENEWAL AND REFURBISHMENT

Renewal involves a complete overhaul of the installation, whereas refurbishment involves replacing only part of the system (retaining the mounting brackets, housings, cables, cameras, etc.).

The renewal or refurbishment of hardware or software may be prompted by various factors:

- when the system has reached the end of its service life or has become obsolete;
- when data from the PDIs and maintenance activities show that the system's condition and performance have deteriorated too significantly.

One way to optimise budgets and reduce environmental impacts may be to opt for partial refurbishments rather than systematic replacements.

It should be noted that, before any work is carried out on the installation, consideration should be given to the need for subsequent system performance verifications through on-site detection tests. These tests are mandatory when cameras or analysers are being replaced.

Booklet 40 sets out typical service lives for the main components of an automatic incident detection system. These data should be viewed in the light of recent experience. For cameras, for example, the observed service life is close to 10 years. Software, on the other hand, may become obsolete after 4 to 5 years, with cybersecurity issues potentially accelerating the need for replacement.

Equipment	Typical lifespans
Cameras	10 years
Screens	10 years
Cables	30 years
Software	10 years – may become obsolete after 4 to 5 years

Figure 19: Typical service lives of AID equipment

10 CONCLUSION

Automatic incident detection via image analysis is the primary means of detecting significant incidents in monitored road tunnels. To ensure their safe operation, it is therefore essential to have a reliable, high-performance and sustainable AID system.

To help achieve all these objectives, this document contains information and recommendations covering all phases of the system's life cycle: design, implementation, acceptance and maintenance.

In the light of experience gained, certain points are fundamental and deserve to be emphasised.

The choice of incident types to be detected must be made according to the specific safety requirements of the tunnel in question, whilst seeking to limit the number of such incidents. Similarly, the performance targets to be achieved must be set taking into account the specific characteristics of the tunnel.

During the system design phase, particular attention must be paid to ensuring comprehensive video coverage of the tunnel, image quality, the choice of camera technologies and the system architecture, all of which determine whether performance targets are met.

During the implementation phase, the system must undergo fine-tuning to achieve the best balance between effective detection performance and minimising the number of false alarms. The progressive stages of testing and acceptance must be strictly adhered to.

During operation, it is essential to ensure that the system continues to perform effectively so that operators retain confidence in the equipment. To this end, regular preventive maintenance measures should be carried out, including, in particular, simple periodic tests to verify its performance and, where necessary, corrective action should be taken.

Finally, as the AID system is a large-scale and critical information system, it is important to ensure that the overall cybersecurity and system dependability policy has been fully taken into account during all the aforementioned phases.

11

LIST OF ABBREVIATIONS

AI	Artificial Intelligence
AID	Automatic Incident Detection via image analysis
ANSSI	French National Agency for Information System Security
CCC	Control and Command Centre
DR	Detection Rate
ECN	Emergency Call Network
FA	False Alarm
FAF	False Alarm Frequency
FAR	False Alarm Rate
GA	Genuine Alarm
GDPR	General Data Protection Regulation
GFAF	Genuine False Alarm Frequency
IDI	Initial Detailed Inspection
IP	Internet Protocol
IPSec	Internet Protocol Security
ISSP	Information Systems Security Policy
MA	Misclassified Alarm
ND	Non-Detection
ODR	Overall Detection Rate
OFAR	Overall False Alarm Rate
ORR	Operational Readiness Review
PDI	Periodic Detailed Inspection
RSV	Regular Service Verification
SCADA	Supervisory Control and Data Acquisition
VLAN	Virtual Local Area Network
VOS	Verification of Operational Suitability
VPN	Virtual Private Network

A

APPENDIX A CLASSIFICATION OF INCIDENTS TO BE DETECTED

As a reminder (see paragraph 3.2 – Classification and selection of incidents to be detected), it is important to carefully select the types of incidents to be detected based on their severity and frequency, the system's ability to detect them, and whether or not there are measures in place to respond to their occurrence.

A.1 LEVEL 1 INCIDENTS

A.1.1 Stopped vehicle in free-flowing traffic

The AID system must detect any stopped vehicle at any point on the carriageway. Brief stops – that is, when a vehicle stops and then sets off again immediately – should not be taken into account.

A.1.2 Fire

Detection of loss of visibility (appearance of smoke): the AID system must detect a significant loss of contrast across a significant portion of the image area.

Flame detection: the AID system must detect a flame at any point in the image.

A.2 LEVEL 2 INCIDENTS

A.2.1 Congestion

The AID system must detect a stream of vehicles travelling at low speed or at a standstill.

A.2.2 Stopped vehicle in a congestion situation

The AID system must detect any stopped vehicle in congested traffic at any point on the carriageway; this function must not detect brief stops caused by congestion (where a vehicle stops and then sets off again immediately).

A.2.3 Vehicle travelling in the wrong direction

The AID system must detect a vehicle travelling in the opposite direction to the flow of traffic on the lane in which it is located.

A.2.4 Pedestrian

The AID system must detect a pedestrian moving on the carriageway and/or on walkways (at any point), regardless of their speed (walking, running) and their path of movement (straight or otherwise).

A.3 LEVEL 3 INCIDENTS

A.3.1 Purpose

The AID system must detect a stationary object on the carriageway that could cause a vehicle accident. As the object may be of any shape or size, it is difficult to define minimum characteristics. As a guide, tests are usually carried out using a cube with a side length of 0.8 m, equivalent to 0.5 m^3.

It should be noted that, given the small size of the object, its detection can significantly influence the distance between cameras. If the aim is to detect an object at any point on the carriageway, the camera layout must be planned accordingly.

A.3.2 Slow-moving vehicle

The AID system must detect as "slow" any vehicle travelling at a configurable speed (which depends on the speed limit within tunnel) at any point on the carriageway.

B

APPENDIX B
CONVENTIONAL CAMERAS WITH NEAR INFRARED SENSITIVITY

In tunnels, due to the presence of permanent artificial lighting, cameras sensitive to visible light are generally used.

However, the use of cameras with sensors sensitive to both the visible spectrum and the near-infrared (NIR) spectrum may be considered in certain specific cases.

Such cameras could, for example, be used in unlit tunnels where the operator wishes to be able to detect the presence of pedestrians.

They produce colour images during the day and black-and-white images at night. To achieve this, they feature a removable infrared filter to prevent infrared light from reaching the sensor during the day. This is because, during the day, when infrared light passes through the sensor's three colour filters (*Red Green Blue* – RGB), the colour information is lost and the camera can no longer produce a colour image. This filter is of course configurable and operates automatically so that it is only active during a specific time slot during the day, thereby making use of the colour information. The rest of the time it is not used and only black-and-white images are provided.

Operation in NIR mode generally requires the use of an infrared (IR) light source, such as an *Infrared Light Emitting Diode* (IR LED). This light source is discreet (as it is invisible to the human eye and therefore to the user) and an energy-efficient means of monitoring a tunnel in the dark.

C

APPENDIX C
EXAMPLES OF EQUIPMENT AND SUPPORT FUNCTION TESTS

The table below provides examples of equipment and support function tests that can be carried out during the testing and ORR phases (this is a non-exhaustive list to be supplemented and adapted to the installed system).

It is recommended that these checks be carried out from the local or remote AID client (maintenance centre, control and command centre, backup control and command centre, etc.).

Tests	Actions to be carried out
Display on AID server	Start the AID server. Log in using the various user profiles. Check that the AID services (analysis, administration, visualisation, recording, etc.) have started correctly. Check that there are no technical alerts.
Display camera feeds on the AID client	Check that video feeds from all cameras are visible on the AID interface.
Check the image quality	Visually check the image quality from each camera, as well as ensuring that their identification and timestamp are correctly displayed.
Test for loss of a video feed	Check that the loss of a video feed triggers an alarm for the operator. Check that the alarm clears when the feed becomes available again.
Test for communication between the analyser and the server	Check that when an incident is detected, an alarm is triggered and sent to the operator.
Test for loss of the analysis function	Check that a total or partial loss of the analysis function triggers an alarm for the operator. Check that the alarm clears when the function becomes available again.
Test for loss of the server	Check that a server failure triggers an alarm for the operator. Check that the alarm clears when the server is available again.
Test for redundancy functions	Check that, in the event of an analyser failure, the system switches over to the standby analyser and that the analysis function remains operational. Check that, in the event of a master server failure, the system switches over to the slave server and that the server is operational.
Test for interaction with related systems	Verify that communication between the AID system and the SCADA system is working correctly (information reporting, command transmission). Check that, when a AID alarm is triggered, the video feed from the relevant camera is displayed on the relevant screen at the Control and Command Centre (CCC).
Test the "camera movement" fault	Check that a change in a camera's orientation correctly triggers an alarm for the operator.
Test the "image quality deterioration" fault	Check that a deterioration in image quality triggers an alarm for the operator.
Test the deactivation functions	Check the detection deactivation functions (by camera, by zone, by incident type). Check that feedback regarding override is sent to the operator. Check that the system returns to its initial state when detection functions are reactivated.
Test the filtering rules	Check the filtering functions for recurring alarms.
Test recording, archiving and export functions	Verify that the detection of an incident does indeed trigger the recording of a video sequence. Verify that sequences are archived and can be played back. Check that the sequence can be exported and/or a detection report generated.

D APPENDIX D DETAILS OF INDIVIDUAL INCIDENT DETECTION FUNCTION TESTS FOR AID SYSTEM ACCEPTANCE

The test phase for individual detection functions for the evaluation of an AID system is essential (see paragraph 8.5 – Specific AID system tests).
The resources and time to be allocated to this phase must not be underestimated. They must be specified in the contract for each test.

Details of the tests to be carried out for each detection function are detailed in the following paragraphs.

The resources required to ensure the safety of people and infrastructure (fire extinguishers, PPE, etc.) that must be available for carrying out these tests are not described in this document.

D.1 TEST OF THE "STOPPED VEHICLE" DETECTION FUNCTION

Requirements	A white light vehicle. A dark-coloured light vehicle.
Procedure	A vehicle shall travel through the tunnel at a speed exceeding 30 km/h, stopping in the area designated in the test plan. The vehicle must remain stationary for a duration equal to twice the detection time specified in the contract. The dipped headlights and sidelights of the vehicles used must be switched on, and it must be ensured that their brake lights are working.
Recommended number of tests	A stop is made within the field of view of each camera at the start, middle and end of the field. One test is carried out for each vehicle, for each traffic lane and, where applicable, for the hard shoulder or the hard strip. It is preferable to carry out the tests several times to obtain a representative sample. Tests must be carried out at each specific point along the tunnel (emergency call stations, emergency exits, lay-bys).
Result	The test is successful if the incident is detected within a time equal to or less than the detection time specified in the contract. Calculation of the overall detection rate for the detection function.

D.2 TEST OF THE "FIRE" DETECTION FUNCTION

Three methods may be used to carry out the fire detection test: the cold smoke method, the warm smoke method and the flame method.

With regard to smoke:

- cold smoke, which is easier to produce, can be used, for example, to simulate a turbo engine failure in a heavy goods vehicle. It is fairly easy to produce highly opaque cold smoke, but it is impossible to simulate the behaviour of real fire smoke (such as stratification) dictated by thermal effects;
- warm smoke is more representative of the smoke actually emitted during tunnel fires (in terms of flow and opacity), but its generation requires more substantial resources and certain precautions.

Regardless of the method used for smoke, experience shows that the recommended air velocity for conducting the tests must be less than 2 m/s if only a single smoke machine is available.

It must be ensured that the tunnel is equipped with the necessary facilities to meet this requirement.

Failing this, additional measures must be put in place, such as multiple smoke generators (or simple smoke bombs) or portable fans to control the airflow.

During smoke tests, automatic activation of the smoke extraction system must be disabled so as not to interfere with the tests.

D.2.1 Fire detection test using cold smoke

Equipment required	A cold smoke generator. A generator or fire service power socket located in the emergency stations. A support vehicle for transporting the generator.
Procedure	Two methods may be considered: 1) The smoke generator is mounted on the carrier vehicle, which travels the entire length of the tunnel along one lane in the direction of the air flow at a speed suitable for smoke dispersion (approximately 5 to 15 km/h). It should be noted that, depending on whether the airflow is natural or forced, the smoke may spread without the need to move the carrier vehicle. 2) The generator is powered from fire service power sockets; it must therefore be moved from emergency station to emergency station in order to cover the fields of view of all cameras. It should be noted that, depending on whether the airflow is natural or forced, the smoke may spread without the need to move the device.
Recommended number of tests	One test is carried out within the field of view of each camera. It is preferable to repeat the test three times for each camera, using different positions within the camera's field of view, to obtain a representative sample.
Result	The test is successful if the incident is detected within a time shorter than the detection time specified in the contract. The detection rate at the end of the various tests is calculated.

D.2.2 Fire detection test using warm smoke

Equipment required	A fuel container capable of producing smoke that starts relatively quickly and is sufficiently dense. Preparing this container requires specific skills. This test is carried out by trained and equipped professionals.
Procedure	Switch off the ventilation system during the test. Ignite the fuel and do not stand near the smoke plume due to the irritating nature of the smoke emitted. Extract the smoke via the ventilation system at the end of each test. Position the fuel container on the road surface within the field of view of a camera. Note that, depending on natural or forced airflow conditions, the smoke may spread without the need to move the device.
Recommended number of tests	Due to the complexity of the procedure, the number of tests will be determined on a case-by-case basis.
Result	The test is successful if the incident is detected within a time shorter than the detection time specified in the contract. The detection rate is calculated at the end of the various tests.

D.2.3 Fire detection test based on the production of flames

Equipment required	A flame generator. A fire extinguisher (for safety).
Procedure	Ignite the flame and do not stand near the generator due to the heat generated. Position the flame generator on the road surface within the camera's field of view.
Recommended number of tests	A test is carried out in the field of view of each camera. It is best to repeat each test three times from different positions within the camera field of view to ensure a representative sample.
Result	The test is successful if the incident is detected within a time shorter than the detection time specified in the contract. The detection rate is calculated at the end of the various tests.

D.3 TEST OF THE "CONGESTION" DETECTION FUNCTION

Carrying out the congestion detection test is relatively demanding in terms of human and material resources. For this reason, it is recommended that this test be carried out under real traffic conditions, using a congestion situation occurring on the tunnel during the RSV.

The dipped headlights and sidelights of the vehicles used must be switched on, as is normally the case during actual operation.

Resources required	Several vehicles may be deployed. The number of vehicles and their speed are determined by the tunnel owner based on the characteristics of the tunnel when the contract is drawn up.
Procedure	A group of vehicles travels at a speed lower than the value set for the incident.
Recommended number of tests	One test is carried out for each traffic lane and any hard shoulder. It is preferable to repeat the tests several times to obtain a representative sample.
Result	The test is successful if congestion is detected within a time equal to or less than the detection time specified in the contract. The overall detection rate is calculated for the detection function.

D.4 TEST OF THE DETECTION FUNCTION FOR A STOPPED VEHICLE IN A CONGESTION SITUATION

Conducting a test to detect a stopped vehicle in a traffic jam by deliberately stopping a vehicle sent for the test is not recommended for safety reasons (risk of a collision).

Verification that this function is operating correctly should only be carried out in the event of incidents occurring under real traffic conditions during the RSV.

D.5 TEST OF THE DETECTION FUNCTION FOR A VEHICLE TRAVELLING IN THE WRONG DIRECTION

To test the detection function for a vehicle travelling in the wrong direction, as with the other tests, the dipped headlights and sidelights of the vehicles used must be switched on.

Equipment required	A white light vehicle. A dark-coloured light vehicle.
Procedure	The vehicle drives in the wrong direction, at a speed of between 30 km/h and the maximum speed limit in the tunnel, along the entire length of the tunnel, on the carriageway being tested. It is advisable to carry out the tests at the maximum permitted speed, whilst ensuring that safety conditions within the tunnel are maintained (no concurrent activities, etc.). The test is carried out for each vehicle and for each traffic lane. The test is deemed sucessful if the incident is detected within a time equal to or less than the detection time specified in the contract.
Recommended number of tests	One test is carried out for each vehicle, for each traffic lane and any hard shoulder. It is preferable to repeat the tests several times at different speeds to obtain a representative sample.
Result	The test is successful if the incident is detected within a time shorter than the detection time specified in the contract. The overall detection rate is calculated for the detection function.

D.6 TEST OF THE "PEDESTRIAN" DETECTION FUNCTION

Resources required	A pedestrian.
Procedure	The pedestrian walks without stopping along a traffic lane for which the function is activated, and crosses the entire length of the tunnel.
Recommended number of tests	One test is carried out for each camera and each lane on which the detection function is activated. The number of tests is equal to the number of cameras involved in detection multiplied by the number of traffic lanes on which the pedestrian detection function is activated. The hard shoulder (or hard strip, as applicable) and walkways are to be considered as traffic lanes in their own right. An additional test involving a pedestrian with an erratic trajectory is recommended.
Result	The test is successful if the incident is detected within a time equal to or less than the detection time specified in the contract. The overall detection rate is calculated for the detection function.

D.7 TEST OF THE "OBJECT" DETECTION FUNCTION

Requirements	Two objects with a volume of approximately 0.5 m^3. A light-coloured object. A dark-coloured object.
Procedure	The object must remain within the camera's field of view for a duration of twice the detection time specified in the contract. The test is carried out for each camera and each lane on which the detection function is enabled.
Recommended number of tests	One test is carried out within the field of view of each camera at the start, middle and end of the field. One test is carried out for each object, for each traffic lane and any hard shoulder. It is advisable to repeat the tests several times to obtain a representative sample.
Result	The test is successful if the incident is detected within a time equal to or less than the detection time specified in the contract. The overall detection rate is calculated for the detection function.

D.8 TEST OF THE "SLOW-MOVING VEHICLE" DETECTION FUNCTION

For the test of the slow-moving vehicle detection function, as with other tests, the dipped headlights and sidelights of the vehicles used must be switched on.

Equipment required	A white light vehicle. A dark-coloured light vehicle.
Procedure	The vehicle travels at a speed lower than the value set for the incident, along the entire length of a lane. The test is carried out on each traffic lane and for each vehicle.
Recommended number of tests	One test is carried out for each vehicle, on each traffic lane and, where applicable, the hard shoulder. It is preferable to repeat the tests several times to obtain a representative sample.
Result	The test is successful if the incident is detected within a time equal to or less than the detection time specified in the contract. The overall detection rate is calculated for the detection function.

E

APPENDIX E
EXAMPLES OF TEST RESULT SHEETS FOR DETECTION FUNCTIONS

Light-coloured passenger car						
Date:		Time:		Lighting mode:		Airflow (SCADA):
DETECTION TYPE						
DIRECTION/TUBE						
N° test	N° of caméra	Test result	Detection times(s)	Lane	Field	Note
12	345	1	12	Slow lane	End	
13	346	0		Slow lane	Centre	
14	347	1	15	Middle lane	Start	
15	348	1	13	Middle lane	Centre	
16	349	0		Fast lane	End	
17	350	1	25	Fast lane	End	

An example of a summary sheet of the performance results, based on the tests carried out, is given below.

		Stopped vehicle: general summary, all lanes combined			
		Target percentage	Success rate	Required detection time in seconds	Average detection time in seconds
Number of tests	68	92.00%	100.00%	15	7.23
Number of positive results obtained	68				

		Pedestrians: general summary, all walkways combined			
		Target percentage	Success rate	Required detection time in seconds	Average detection time in seconds
Number of tests	59	75.00%	93.22%	15	6.4
Number of positive results obtained	55				

		Slow-moving vehicle: general summary			
		Target percentage	Success rate	Required detection time in seconds	Average detection time in seconds
Number of tests	21	92.00%	71.43%	12	5.83
Number of positive results obtained	15				

		Fire: general summary			
		Target percentage	Success rate	Required detection time in seconds	Average detection time in seconds
Number of tests	33	80.00%	84.85%	15	6.46
Number of positive results obtained	28				

F

APPENDIX F
INFORMATION ON CYBERSECURITY

This appendix explains concepts and measures to supplement Chapter 7.
In particular, it outlines fundamental concepts relating to cybersecurity in road tunnels (security components, types of threats, robust defence means) and provides details of the security measures that can be implemented at both hardware and software levels (authentication, physical access control, firewalls, SCADA and IT systems).

F.1 SECURITY COMPONENTS

F.1.1 Overview of the components

The security of an Information System (IS) is generally considered in terms of four components: availability, integrity, confidentiality and traceability.

Specific issues related to these four components in the case of a tunnel-based AID system are listed below:

- availability: the operation of the AID system must be protected against failures, as this tool is essential for the early detection of incidents whose progression could endanger tunnel users;
- integrity: data tampering, or the generation of false incidents, may prevent the operator from having a clear idea of the development of the situation or lead to unecessary mobilisation of resources;
- confidentiality: the images and video footage produced by the system contain personal data. They may only be viewed or accessed by persons who have been specifically and individually authorised to do so;
- traceability: access to the system, as well as data queries and extractions, must be logged.

F.1.2 Types of threats

There are four main types of motivation behind attacks on information systems:

- ideological: service disruptions to convey a message, or the misappropriation or disclosure of information (e.g. the Islamic State's attack on TV5 Monde, or Anonymous's takeover of French government websites);
- financial: theft of personal, financial or strategic data; ransom demands so that the victim can recover the stolen data or restore the compromised IT system to operation;
- state-sponsored espionage: eavesdropping, theft of confidential data;
- industrial espionage: theft of data and source code.

The vast majority of attacks on information systems are carried out using social engineering. This term refers to the art of manipulating people by exploiting their naivety to persuade them to disclose information that enables the system to be infiltrated. The most common method is phishing, which involves sending an email asking the recipient to click on a malicious link or to provide their login credentials. Other methods may be used when a group of attackers already possesses information (phone calls, text messages, letters, web or mobile applications).

In recent years, attacks on information systems have received significant media coverage, particularly those targeting healthcare organisations. In most cases, ransomware encrypts all the data on an information system and demands payment of a ransom in cryptocurrency to decrypt the information. Ransom should never be paid and the incident should be reported to law enforcement bodies as soon as possible in order to initiate procedures to manage the associated crisis. Other measures can be put in place, (in France, this is notably with the assistance of ANSSI).

Beyond ransomware, the figures on data breaches (user account data following the theft of logins and passwords) demonstrate the scale of this phenomenon: 533 million accounts for Facebook in 2022, 250 million for Microsoft in 2021.

The emergence of new technologies and new ways of using IT is likely to further increase cybersecurity needs due to an even greater exposure to risk: connected devices, cloud environments, *big data* and artificial intelligence using *deep learning* – which, on its own, creates significant uncertainty in terms of cybersecurity.

F.2 ROBUST DEFENCE MEANS

Cyber protection must involve multiple layers of protection to ensure robust defence.This means that one must not rely on a single layer of protection, but rather multiple layers of defensive mechanisms: if one fails or is bypassed, another remains in place to thwart the attack.

Even with regular patches released to address exposure to the latest cyber security threats on systems and equipment, vulnerabilities may still remain.

Robust defence must not be limited to software: it begins with protecting physical access to hardware.

F.2.1 Authentication

It is essential that equipment only supports sufficiently secure protocols and access methods. Naturally, protocols such as Telnet[31], HTTP[32], FTP[33] must be banned (non-exhaustive list), in favour of protocols such as SSH[34], HTTPS[35] and SFTP[36] (non-exhaustive list). Similarly, any manufacturer-specific security or encryption protocol or mechanism must be banned: security must be based on mechanisms that are wellknown, auditable, standardised and monitored by a broad community.

Even if data flows are protected by an encryption method, simple password-based authentication should also be avoided in favour of certificate-based authentication[37] and, where possible, mutual authentication. This is necessary to guard against so-called "*man-in-the-middle*" interception attacks (a type of cyberattack where an attacker manages to insert themselves between a sender and a recipient, notably by taking control of a device – such as a public Wi-Fi router – that enables them to communicate).

All original authentication credentials (certificates provided by manufacturers, default passwords), which are useful for testing hardware functionality and initiating commissioning, must be replaced by authentication credentials established and renewed in accordance with the credential policy defined by the tunnel operator (password length and complexity requirements, certificate hierarchy, renewal frequencies, etc.).

Care must also be taken with regard to authentication processes that are secure during normal system operation but which could be compromised or degraded (*downgradable*).

F.2.2 Physical access protection

Physical protection is generally provided for the operations control and command centre, its server room and other plant rooms.

In a large-scale infrastructure, it is unrealistic to expect to provide protection against physical intrusion by determined and well-prepared individuals (who are equipped and trained). Nevertheless, it seems necessary to implement simple and cost-effective measures to achieve:

- a level of protection that prevents intrusions by mere curious onlookers or amateur hackers who do not necessarily possess the skills required for physical access;
- a record of all access events: procedures must be put in place to enable the centre to determine whether such access constitutes a potential intrusion, and to take appropriate action where necessary.

All premises and equipment sites must therefore be both physically secured and fitted with an alarm system so that physical intrusions are detected before intruders have been able to gain control of the equipment and security systems.

This protection applies not only to tunnel portal premises housing the main communication nodes, but to any site or field plant rooms containing communication equipment. Communication via a secure tunnel-type VPN (typically IPsec) may make it possible to avoid imposing this constraint on intermediate level sites.

An access security policy is essential for all tunnel operations staff: the identity of any third party on site should always be verified, and access preferably enabled via cards where possible. Certain practices should also be prohibited (passwords left visible on desks, use of unidentified memory sticks, etc.).

31. A communication protocol between a client and a server, now obsolete.
32. *HyperText Transfer Protocol*, a communication protocol between servers and web browsers, allowing the transfer of files with authentication information in plain text.
33. *File Transfer Protocol*, a file transfer protocol that transmits authentication information in plain text.
34. *Secure SHell*, a secure transmission protocol operating via a remote command interface.
35. *HyperText Transport Secure*, a combination of the HTTP and TLS (Transport Layer Security) protocols. Enables web browsing with an enhanced level of security.
36. *Secure File Transfer Protocol*, a file transfer protocol enabling secure communications with a remote computer.
37. The authentication process between a user and a protected resource. The exchange of these certificates provides a higher level of security compared to authentication via username and password. This process requires the implementation of a certificate authority connected to the resource to guarantee the validity of the certificates.

F.2.3 Firewalls

Network Segmentation

Although perimeter security is not the be-all and end-all, and *Zero Trust*[38] approaches are playing an increasingly significant role in security architectures, strict segregation must be established between the various networks: field networks[39], the backbone network, specific operations networks at the tunnel control and command centre, office software networks and, of course, the Internet. Firewalls must only allow traffic that has been predefined for identified users. All incoming traffic leading to remote access that does not pass through specific relay machines must be blocked.

Filtering principle

In addition to the firewalls interconnecting networks, firewall functions (such as *netfilter* for Linux, but also the Windows firewall) must also be enabled on all active equipment; this helps, in particular, to reduce the spread of worms and viruses.

On all firewalls, the default policy must be to delete data packets (*drop*).

To facilitate administration, the ICMP[40] echo (the "ping" command) must be responded to by all devices:

- on their physical interface with the management centre (RJ45 port), if on a private network;
- or only on a virtual interface if communication takes place via a VPN tunnel.

Other ports and protocols may only be opened if the need to do so has been approved. The manufacturer must provide a matrix of the traffic flows to be opened to ensure the project functions correctly, and describe the content of the protocols and their behaviour. The traffic flow matrix must be discussed with the project manager and the tunnel operator's information systems security manager. In all cases, protocols that are unsecure or present potential vulnerabilities must be excluded. Administration and monitoring protocols may only be opened if they are used by the tunnel operator, and only with identified machines located on the tunnel control and command centre's internal networks.

F.2.4 Monitoring

To monitor the availability of the AID system and its supporting systems (power supply and transmission), it is advisable to integrate them into a SCADA system. All transmission equipment can be monitored via the SNMPv3[41] and ICMP protocols. All transmission equipment must be capable of forwarding activity logs to a logging server (e.g. syslog[42]) controlled by the operator and located in a demilitarized zone (DMZ) connected to the external firewall.

F.2.5 Computers

Servers

On servers that exchange files with external parties, at least one antivirus programme must be installed. To enhance security, the addition of *Endpoint Detection and Response* (EDR) software is a significant advantage. It provides a much higher level of detection and protection than "traditional" antivirus programmes (it is also regarded as an "antivirus 2.0").

Operator workstations

Antivirus or EDR software, or even both, must be installed on all operator workstations.

From a cybersecurity perspective, it is preferable for the workstations used to carry out data extraction and analysis functions to be separate from the operator workstation that displays AID alarms in real time in the control room.

These data extraction and analysis functions must only be accessible locally, via dedicated accounts set up for this purpose. The session must lock automatically after a period of inactivity on the part of the operator.

As a general rule, and even for data extraction, no peripheral devices or accessories (USB sticks, CD-ROM, etc.) supplied by a third party must be connected to the workstation without first being scanned by an external antivirus programme (on a dedicated workstation with access to updates, but outside the operations networks).

Access rights to equipment

Direct remote administration of equipment must be prohibited (no *Secure Shell* (SSH) connections via a root account[43] for example). For such administration, several specific user accounts must be created, and only these accounts shall have privilege escalation rights.

All servers and workstations must be fully controlled by the tunnel operator, who must be the only body with super-administrator (root) access. If other identified individuals (such as an installer during the VOS phase or a third party maintainer) require privileged access, dedicated accounts must be assigned to them; however, the operator must retain full control over the machines: in particular, they must be able to audit their configuration at any time. It is recommended that these configuration compliance checks be carried out at least when the system becomes operational and then periodically thereafter. The publisher of the AID solution will also be asked to provide the security-related configuration details for its software suites, so that these can be verified.

---

38. *Zero-trust* architecture: a strategy whereby no person or device is considered trustworthy or secure within a computer network without rigorous verification.
39. See Chapter 7 – Cybersecurity and system dependability.
40. *Internet Control Message Protocol*, a network protocol used to request or provide information on the accessibility of a machine.
41. *Simple Network Management Protocol*: a network monitoring protocol used to monitor the operational status of any active component within a computer network.
42. A protocol providing an incident logging service on a computer network.
43. A user with full privileges on a Linux operating system; they are therefore the system administrator.

G

APPENDIX G
MAINTENANCE

G.1 SPARE STOCK

Corrective maintenance is carried out when equipment unexpectedly fails.

In order to be able to quickly address any downtime of the AID system, a set of spare parts must be provided and made available once the system becomes operational.

The spare parts in question and the number of units must be adapted to:

- the architecture of the AID system;
- any minimum operating conditions associated with the AID.

This stock must include at least:

- complete cameras (including lenses);
- housings;
- fixtures;
- a set of small connection accessories (media converters, connectors, *Power over Ethernet* (PoE) power supplies, etc.);
- …

A backup of the monitoring and analysis software configurations must be made once the system is operational, to enable rapid reinstallation in the event of a server fault.

G.2 EXAMPLE OF A MAINTENANCE PLAN

An example of a preventive maintenance plan is given below. The content and frequency of the tasks to be carried out should be adapted to the specific characteristics of the tunnel and its operating conditions.

Type	Tasks	Location	Frequency
Routine maintenance / continuous monitoring	Logging into the AID servers	From the control and command centre or plant room, without tunnel closure	Daily / weekly
	Checking processor load, memory usage, remaining disk space, etc.		
	Monitoring of image flow and quality		
	Testing for vehicle detection in lay-bys	Inside the tunnel without closing it	
Routine maintenance / continuous monitoring	Checking the level of dirt on camera lenses	From the control and command centre or the plant room, without tunnel closure	Monthly / quarterly
	Verification of the consistency of detection masks in the image (mandatory after each camera wash)		
Scheduled "light" tests	Test to detect stopped vehicles in front of emergency stations/ exits	Inside the tunnel, with tunnel closure or lane closure	
Routine maintenance	Cleaning of the camera system (housing, lenses, etc.)	In the tunnel, with tunnel closure or lane closure	Quarterly / half-yearly / annually
Performance audit	Verification of alarms over a period of x consecutive days	From the control and command centre or the plant room, without tunnel closure	Half-yearly / annually
	Analysis of technical logs over a period of x consecutive days		
	Comparison of the AID alarm log with data from sources external to the AID		
	Comparative monitoring across years		
Scheduled "exhaustive" checks	Exhaustive' detection test campaign	Inside the closed tunnel and from the control and command centre	Annually
Detailed Inspection	Inspection of the condition of equipment	Inside the closed tunnel and from the control and command centre	Every 6 years
	On-site detection tests		

As a reminder, it is important to bear in mind that:

- an AID system is sensitive equipment that can encounter changes in performance over time;
- light but regular maintenance should be prioritised;
- tests can be combined with other maintenance operations or tunnel operation activities (including during construction work);
- it is important to establish a system for tracking the results of the maintenance operations carried out.

G.3 EXAMPLE OF A TEST RESULTS SHEET FOR AN "EXHAUSTIVE" TEST CAMPAIGN

Thursday 21/10/21

		CAM-2	CAM-1	CAM-	CAM-4	CAM-5	CAM-6	CAM-7	CAM-8	CAM-9	CAM-10	CAM-11	CAM-12	CAM-13	CAM-14	CAM-15	CAM-16	CAM-17	CAM-18	CAM-19	CAM-20	OK	NOK
STOP in smooth traffic																						**100 %**	
	LV Start field LV End field	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0	0
		OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	20	0
FL Start field FL End field		OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	20	0
		-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0	0

Object on carriageway	CAM-2	CAM-1	CAM-3	CAM-4	CAM-5	CAM-6	CAM-7	CAM-8	CAM-9	CAM-10	CAM-11	CAM-12	CAM-13	CAM-14	CAM-15	CAM-16	CAM-17	CAM-18	CAM-19	CAM-20	**75 %**	
Fast lane	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0	0
LV with Day+Night +Min. Night lighting	NOK	OK	OK	OK	Slow Vehicle	Slow Vehicle	NOK	NOK	Slow Vehicle	OK	OK	Slow Vehicle	OK	OK	OK	OK	OK	OK	NOK	OK	12	4
LV with minimum night lighting	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0	0

Wrong way	CAM-2	CAM-1	CAM-3	CAM-4	CAM-5	CAM-6	CAM-7	CAM-8	CAM-9	CAM-10	CAM-11	CAM-12	CAM-13	CAM-14	CAM-15	CAM-16	CAM-17	CAM-18	CAM-19	CAM-20	**55 %**	
Fast lane at 70km/h	NOK	OK	NOK	OK	NOK	NOK	OK	OK	OK	OK	NOK	NOK	NOK	NOK	OK	OK	OK	NOK	NOK	OK	10	10
Slow lane at 70km/h	NOK	OK	OK	OK	OK	OK	OK	NOK	OK	OK	OK	OK	NOK	NOK	OK	NOK	OK	NOK	NOK	NOK	12	8

Pedestrian	CAM-2	CAM-1	CAM-3	CAM-4	CAM-5	CAM-6	CAM-7	CAM-8	CAM-9	CAM-10	CAM-11	CAM-12	CAM-13	CAM-14	CAM-15	CAM-16	CAM-17	CAM-18	CAM-19	CAM-20	**80 %**	
Near slow lane	OK	OK	OK	NOK	NOK	OK	OK	NOK	OK	OK	NOK	OK	NOK	NOK	OK	OK	OK	OK	OK	OK	14	6
Near fast lane	OK	OK	OK	OK	OK	OK	OK	NOK	OK	OK	OK	OK	OK	OK	NOK	OK	OK	OK	OK	OK	18	2

Visibility	CAM-2	CAM-1	CAM-3	CAM-4	CAM-5	CAM-6	CAM-7	CAM-8	CAM-9	CAM-10	CAM-11	CAM-12	CAM-13	CAM-14	CAM-15	CAM-16	CAM-17	CAM-18	CAM-19	CAM-20	**89 %**	
	Visib. Deact	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	NOK	Visib. Deact.	NOK	16	2

LV: Light vehicle FL: Fast lane NOK: Not OK

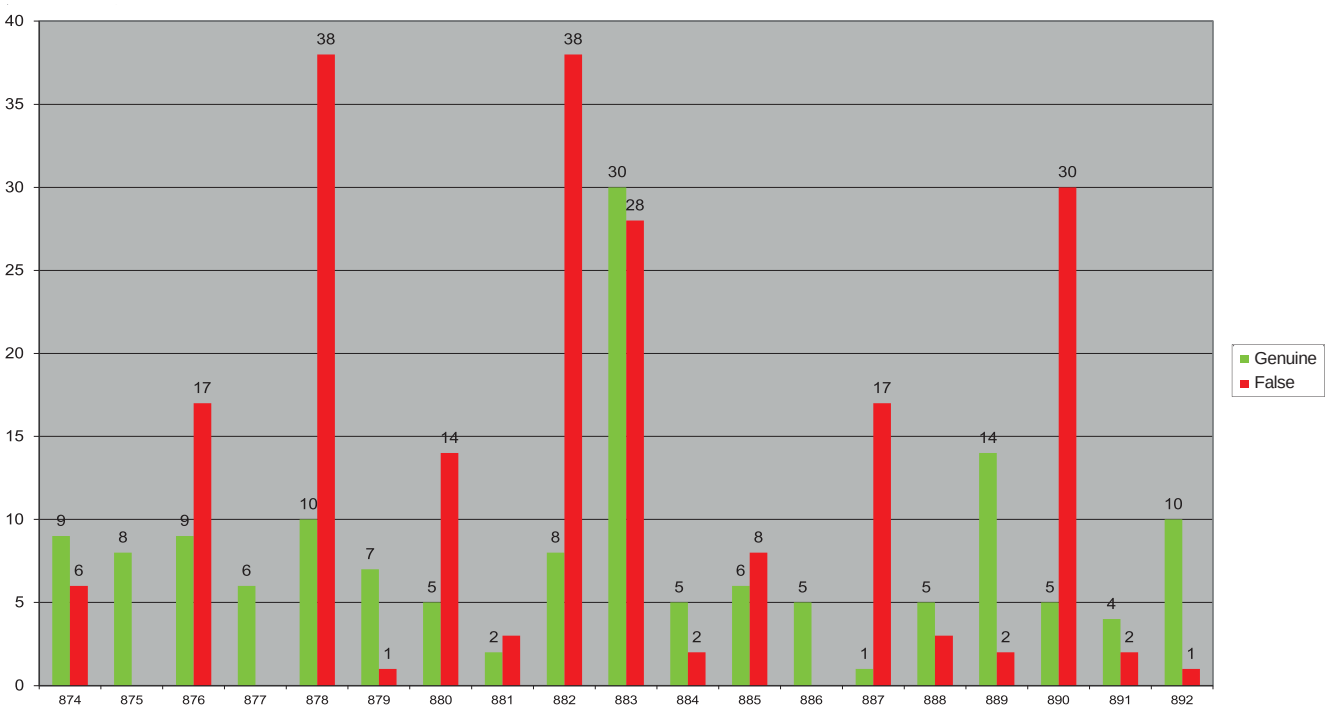
Illustration: © DIR centre-est

The table above shows the results obtained during an annual "exhaustive" test campaign.
In this example, a test was carried out for each type of incident to be detected, on each camera and in each area of interest (slow lane, fast lane, walkways, hard shoulder, etc.). Misclassified alarms were counted as genuine alarms.

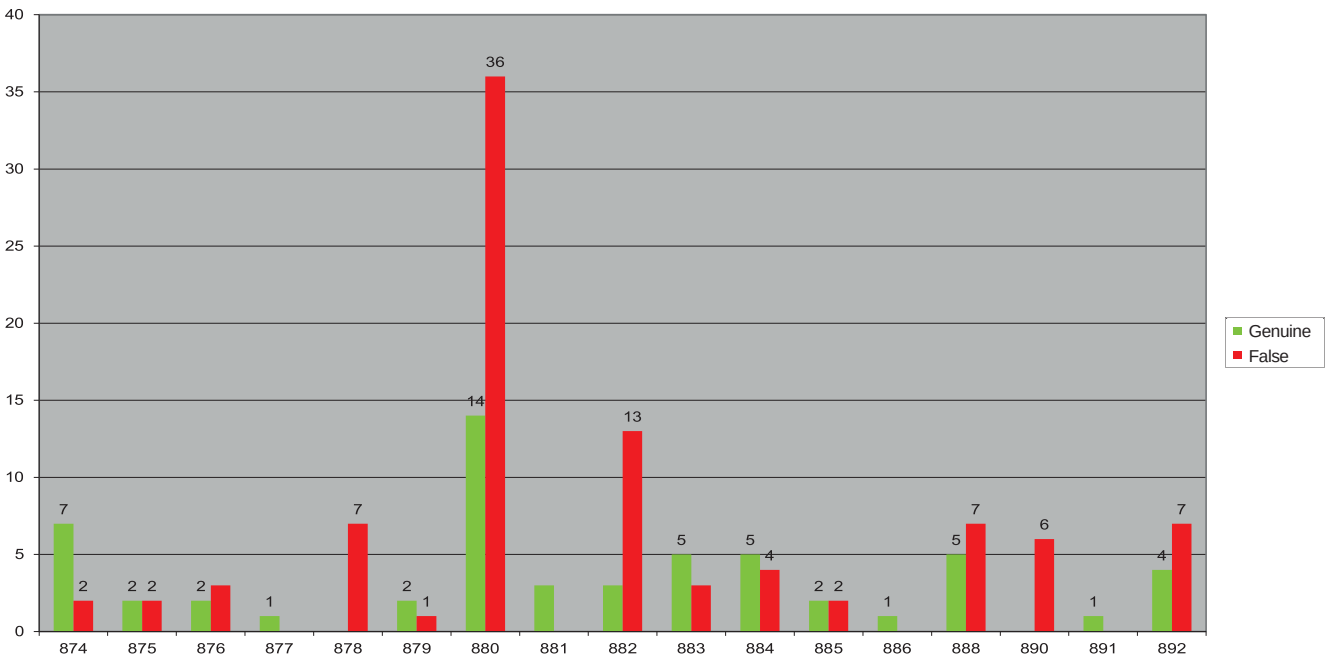
The final column shows the detection rate determined by the type of incident to be detected.

Following this campaign, the results were forwarded to the manufacturer so that corrective action could be taken.

G.4 EXAMPLE OF A COMPARATIVE MONITORING SHEET



Alarm type – year n-1 (© AREA)



Alarm type – year n (© AREA)

The diagrams above illustrate the analysis, by camera, of genuine and false alarms recorded over a given period. Various analyses can be carried out to identify malfunctions or deviations: false-to-true alarm ratio, overall deviation between two periods, malfunction of a particular camera compared to the others…

EDITORIAL TEAM

Christophe BANOS (CETU), Séverine BESSON (CETU), Jérémie BOSSU (Cerema), Christophe CARNISI (CETU), Éric CHARLES (CETU), Florian FRANDIDIER (Cerema), Pierre-Yves TANNIOU (Cerema).

ACKNOWLEDGEMENTS

The CETU wishes to thank the operators (DiRIF, Vinci Autoroutes, ASFA), suppliers (Sprinx Ai, Cyclope Ai, Citilog, Flir) and engineering consultancies (Setec, Egis) for their proofreading.

Photo credits: cover - Arnaud BOUISSOU (Terra); inside pages - CETU - Editing and coordination: CETU staff - Design: PAO Concept - Printing: VASSEL GRAPHIQUE

Centre for Tunnel Studies

25 avenue François Mitterrand
69500 BRON - FRANCE
Tel. +33 (0)1 40 81 30 30
cetu@developpement-durable.gouv.fr

MINISTÈRE
DES TRANSPORTS
Liberté
Égalité
Fraternité

CETU

www.cetu.developpement-durable.gouv.fr