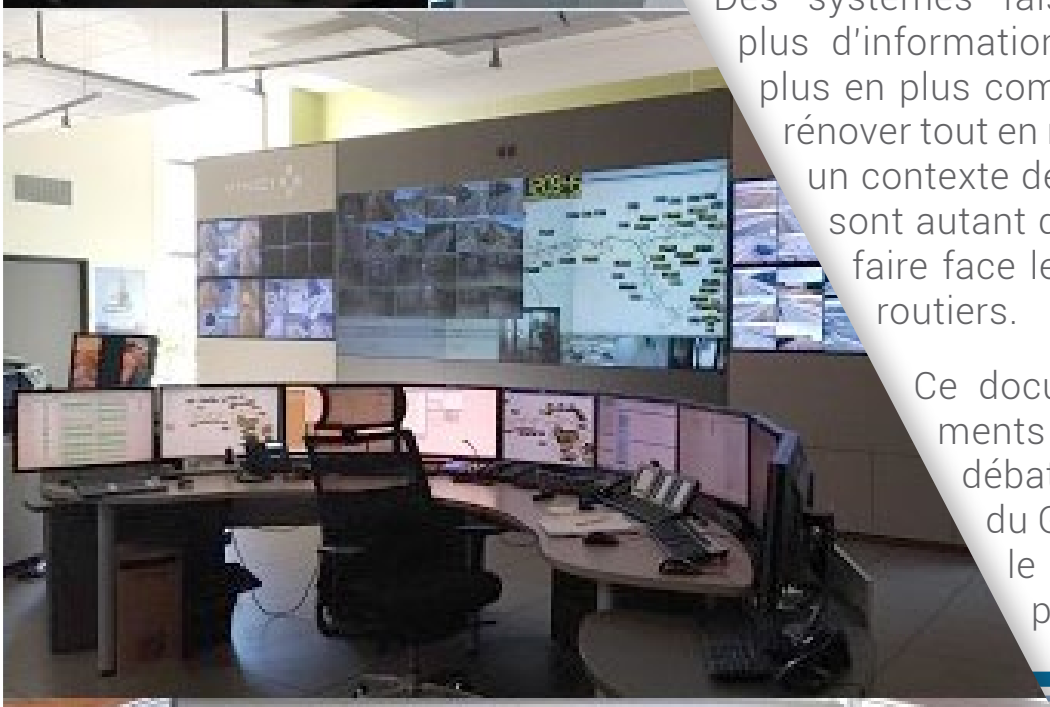


Gestion Technique Centralisée - Supervision

Des systèmes faisant toujours remonter plus d'informations, des exploitations de plus en plus complexes, des dispositifs à rénover tout en maintenant la circulation, un contexte de risque de cyberattaque, sont autant de défis auxquels doivent faire face les exploitants de tunnels routiers.

Ce document présente les éléments de réponses exposés et débattus lors de la rencontre du GTFE de octobre 2019 sur le thème de la GTC – Supervision.

L'ATELIER GTFE

Introduction par Lionel Aubert

Atelier thématique

Première session : **un outil central pour l'opérateur**

- Démarche d'ergonomie impliquant les opérateurs de PCC dans la refonte de l'IHM du système de supervision des tunnels par Florent Dallo (DiRIF)
- Tube 2 Frejus : études ergonomiques concernant l'IHM de supervision et le synoptique du mur d'images des PCC" et mise en place d'un outil dit Module Minimal d'Aide à l'Exploitation (MMAE) combiné avec la supervision par Franck Rotival (BG), Florent Latard (GEIE-GEF)
- Nouvelle GTC incluant un système d'aide à la décision de l'opérateur par Corinne Chiodini (PCC Oslo)
- GTC Tunnel Mont Blanc – fonction simulateur et rejeu par Cédric Petitcolin (GEIE MB)

Seconde session : **point de vue technique**

- Contournement de Neuchâtel : rénovation de la GTC supervision et présentation du concept de passerelle intergénérationnelle par Pierre Sébastien Porret (RN Arc Jurassien – Suisse) et Hubert Galland (BG)
- OSIRIS 2 : déploiement d'un superviseur unique multi-tunnels par Philippe Mansuy (DIR CE)
- Tunnel du Lioran : Virtualisation des serveurs par Julien Soulier (DIR MC)
- Cybersécurité, cas pratique tunnel du Lioran par Jean-Philippe Osty et Cedric Serment (DIR-MC) – Pierre-Yves Tanniou (Cerema)

Table ronde

Participants à la table ronde : Carmen Maria Martinez (Tunnel du Somport), Cédric Petitcolin (GEIE MB), Caroline Lorenz (DiRIF), Alexandre Masneuf (EGIS Tunnel)

\ REMERCIEMENTS

\\ SONT REMERCIÉS POUR LEUR EXPOSÉ OU LEUR PARTICIPATION À LA TABLE RONDE

| Corinne CHIODINI (PCC Oslo)
| Florent DALLO (DiRIF)
| Hubert GALLAND (BG)
| Florent LATARD (GEIE-GEF)
| Caroline LORENZ (DiRIF),
| Philippe MANSUY (DIR CE)
| Carmen Maria MARTINEZ (Tunnel du Somport),
| Alexandre MASNEUF (EGIS Tunnel)
| Jean-Philippe OSTY (DIR MC)
| Cédric PETITCOLIN (GEIE MB)
| Pierre Sébastien PORRET (RN Arc Jurassien – Suisse)
| Franck ROTIVAL (BG),
| Cedric SERMENT (DIR MC)
| Julien SOULIER (DIR MC)
| Pierre-Yves TANNIOU (Cerema)

\\ SOMMAIRE

Gestion Technique Centralisée - Supervision

\\ Atelier du 10 octobre 2019 \\

Novembre 2020

1 CADRE RÉGLEMENTAIRE & TECHNIQUE

INTRODUCTION

Les équipements d'exploitation et de sécurité (accélérateurs, éclairage, auto-évacuation, etc.) **visent à garantir la sécurité des usagers et l'écoulement du trafic**. La présence et la quantité de ces équipements varient en fonction de la longueur du tunnel, de son trafic, de degrés de surveillance etc. Ces équipement permettent ainsi à l'exploitant de superviser le(s) tunnel(s) dont il a la charge.

Pour ce faire, il dispose, au Poste de Contrôle Commande (PCC), d'outils lui permettant de traiter à distance les informations émanant de ces équipements.

La Gestion Technique Centralisée (GTC)-Supervision assure le contrôle-commande de ces équipements. Elle englobe toute la chaîne de traitement des informations depuis les équipements jusqu'au poste de contrôle-commande (PCC).

En plus de gérer des équipements électromécaniques, **la GTC - Supervision est en interface avec d'autres systèmes** comme la vidéosurveillance, le Réseau d'Appel d'Urgence (RAU) ou la radiocommunication.

Ce système, véritable cerveau du tunnel, est au centre de nombreux enjeux. Parmi les préoccupations actuelles, l'interface homme machine (IHM) se doit d'être un outil adapté à l'opérateur.

La GTC - Supervision doit répondre à des exigences d'évolutivité et d'interopérabilité. La rénovation sous exploitation et la prise en compte des risques liés aux cybermenaces sont également des problématiques d'actualité. De plus la conception d'une installation de GTC - Supervision doit s'inscrire dans des politiques d'exploitation et de maintenance contraintes par les moyens humains et matériels à disposition. Les perspectives sont liées à l'essor des systèmes de transport intelligent (ITS) mais aussi au potentiel offert par le développement de nouvelles technologies, comme l'Intelligence Artificielle.

La rencontre du GTFE du 10 octobre 2019 à Nice traitait l'ensemble de ces sujets. **A travers les présentations et les échanges, la rencontre a permis de dresser un panorama sur ces différents enjeux et d'apporter des pistes de solutions.**

Cette note a pour but de poser les grands principes utilisés en GTC - Supervision pour le domaine des tunnels routiers et de synthétiser les principaux apports issus de ces échanges.

CADRE RÉGLEMENTAIRE ET NORMATIF

L'instruction technique (IT – Annexe 2 à la circulaire 2000-63 du 25 août 2000) précise les dispositions et moyens qui doivent être mis en place dans les tunnels de plus de 300 m du réseau routier national. Elle souligne que l'ensemble des dispositions et des moyens doit concourir à assurer les fonctions suivantes :

- la **continuité de l'exploitation** de l'ouvrage (IT §5) ;
- la **sécurité des usagers** (IT §5) ;
- la **traçabilité des événements** en cas d'incident (IT §3).

L'IT introduit la notion d'**unicité de la commande**, à savoir que les mêmes équipements de sécurité du tunnel ne doivent pouvoir être commandés à tout moment que depuis un seul PCC, sans faire obstacle pour autant à l'existence éventuelle de plusieurs postes à condition qu'ils ne puissent pas être en fonction simultanément (IT §5.1.1).

Si l'IT est prescriptive pour les tunnels de plus de 300 m du réseau routier national, ce texte constitue aussi la référence pour les tunnels hors réseau routier national, et ses dispositions pourront être adaptées, en particulier pour les tunnels de moins de 300 m.

Il n'y a pas de cadre réglementaire plus précis pour les solutions techniques et les architectures de GTC - Supervision. Il existe cependant un cadre normatif riche pour les équipements et les logiciels, ainsi que pour les études et les développements. Citons par exemple les normes relatives aux automates programmables industriels (exemple NF EN 61131 X), aux réseaux de transmissions (exemple IEE 802-X), à l'ergonomie de l'interaction homme système (exemple NF EN ISO 9241-X) ou celles relatives aux études de conception (exemple NF EN ISO 9000-3).

Au final, la définition de la solution s'appuie essentiellement sur les règles de l'art, avec des principes partagés entre les exploitants de tunnel, les professionnels et le CETU. Ces principes permettent de définir un cadre technique.

PRINCIPES DE LA GTC - SUPERVISION

Le système de GTC - Supervision est conçu de façon à **fédérer l'ensemble des équipements** du tunnel et proposer une **interface unique** à l'ensemble des installations.

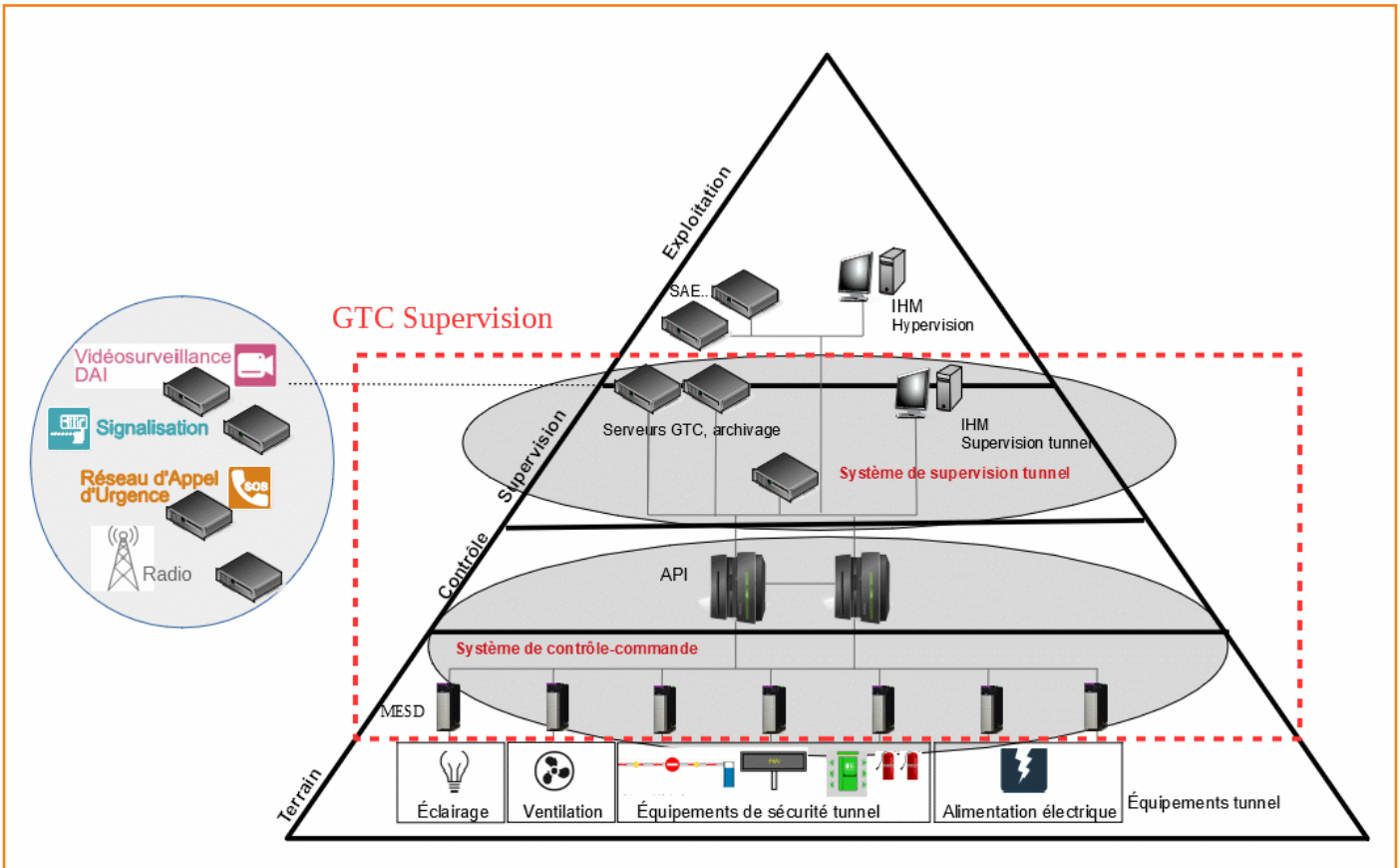
Son architecture peut être représentée à l'aide de la pyramide de l'automatisation. Celle-ci comporte une hiérarchie en plusieurs niveaux en interaction les uns avec les autres. On distingue les niveaux suivants, en partant du bas de la pyramide vers le haut :

- le niveau de terrain, comprenant les capteurs et les actionneurs, soit les différents équipements du tunnel ;
- le niveau de contrôle, comprenant les équipements réalisant les automatismes ;
- le niveau de supervision, comprenant les équipements permettant à l'exploitant de suivre et de piloter les équipements du tunnel ;
- le niveau d'exploitation, comprenant les systèmes qui exploitent les données de différents systèmes informatiques utilisés, comme typiquement un Système d'Aide à la Gestion de Trafic (SAGT).

Les échanges de données utilisent plusieurs réseaux de transmission. On retrouve généralement :

- le réseau de terrain pour les échanges au niveau du système de contrôle commande ;
- le réseau fédérateur, pour les échanges entre systèmes (GTC, vidéosurveillance, RAU, signalisation extérieure...) au niveau du tunnel ;
- le réseau de transport, pour la communication entre le tunnel et le PCC ;
- les réseaux propres du PCC.

Les équipements situés sur le niveau de terrain et le niveau de contrôle forment le **système de contrôle commande**, et ceux situés sur le niveau de supervision forment le **système de supervision**.



Pyramide de l'automatisation appliquée à la GTC - Supervision tunnel

SYSTÈME DE CONTRÔLE-COMMANDE

Le système de contrôle-commande gère les **équipements actifs** du tunnel :

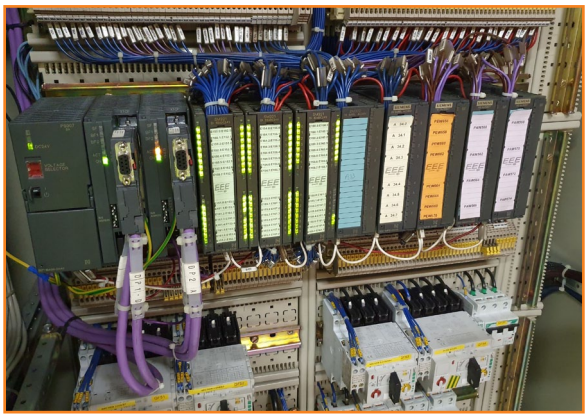
- les équipements de sécurité qui regroupent notamment le dispositif de fermeture du tunnel, les équipements de signalisation et d'accompagnement de l'auto-évacuation des usagers ainsi que divers capteurs comme les capteurs de décroché extincteur ou d'ouverture de porte ;
- les équipements liés à la ventilation ;
- les équipements liés à l'éclairage ;
- les équipements liés à l'alimentation électrique.

Ces équipements sont raccordés par l'intermédiaire de Modules d'Entrées/Sorties Déportées (MESD), mis en œuvre sur un ou plusieurs réseaux de terrain bouclés en fibre optique.

Les **Automates Programmables Industriels** (API) réalisent les tâches d'acquisition des données terrains, les commandes, la réalisation d'automatismes et la communication avec le système de supervision.

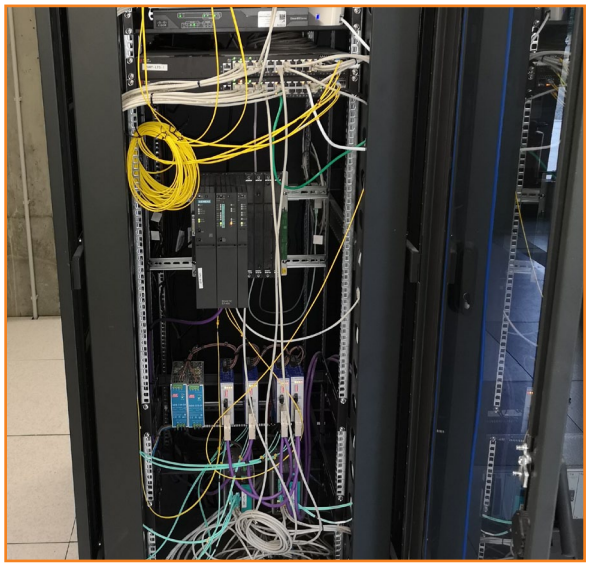
Ces API assurent deux fonctions essentielles :

- la première concerne le pilotage en direct de commandes automatiques comme la gestion de l'éclairage, la ventilation sanitaire en fonction de seuils prédéfinis etc. Dans ce cadre, après traitement des données reçues des différents capteurs connectés au réseau de terrain, l'API exécute automatiquement (sans validation ou d'ordre de la part de l'opérateur) des scénarios préprogrammés plus ou moins complexes. ;
- la seconde concerne son rôle de passerelle entre les niveaux terrains et les niveaux supervision. L'API est alors utilisé :
  - dans le sens montant (terrain vers supervision), pour traiter les données qui lui sont transmises par les équipements connectés au réseau de terrain en vue de les transmettre au serveur d'applications de GTC - Supervision puis à l'opérateur. Il va traduire les données dans un protocole de communication (généralement de type Ethernet) avant de les envoyer au destinataire ;
  - dans le sens descendant, l'API transmet aux équipements les commandes pour exécuter les scénarios ou ordres transmis par l'opérateur via les systèmes de supervision et GTC.



Afin d'élever le niveau de sûreté de fonctionnement, comme les aléas de réseau, **l'intelligence est située au plus près du terrain** c'est à dire dans des locaux techniques à proximité du tunnel.

De plus, la **redondance des API** est généralement mise en œuvre dans tous les tunnels de plus de 300 m afin de se prémunir d'un risque de défaillance. Dans cette optique, deux API sont ainsi couplés pour assurer leur redondance mutuelle en cas de panne de l'un d'eux. Cette redondance est dite « à chaud », c'est-à-dire sans arrêt du système. Pour ce faire, l'un des deux API est identifié arbitrairement comme étant en fonctionnement dit « Normal ». Il traite les données et lance les commandes. En parallèle, l'autre API est en fonctionnement dit « Secours ». Il met à jour ses tables de données et de commandes mais n'agit pas sur le système. De plus, une redondance de type « haute disponibilité », avec module de synchronisation et liens fibre optique dédiés, est préconisée.



SYSTÈME DE SUPERVISION

Le système de supervision permet à l'exploitant, via une Interface Homme Machine (IHM), d'accéder aux **fonctions d'exploitation du tunnel** :

- visualisation en temps réel de l'état du tunnel avec la mise en évidence des anomalies,
- collecte d'information en temps réel de capteurs,
- détection et gestion des événements,
- passage de commande unitaire et groupée d'équipements,
- archivage de données…

Ce système est basé sur une application de supervision (progiciel) qui traite l'ensemble des données provenant du système de contrôle-commande et les met à la disposition des opérateurs au niveau de l'IHM développée sur le client de supervision.

Selon la conception et le besoin de l'exploitant, la supervision peut intégrer des données provenant d'autres familles équipements : vidéosurveillance et Détection Automatique d'Incident (DAI), signalisation hors tunnel, RAU, radiocommunication…

L'application de supervision est déployée sur les **serveurs d'applications**. Pour les tunnels de plus de 300 m, ces serveurs sont redondés. Dans le cas des supervisions multi-tunnels, les variables propres à chaque ouvrage sont généralement gérées par un serveur ou un couple de serveurs dédié à cet ouvrage.

Par l'intermédiaire de **l'IHM** de supervision (cliente de l'application de supervision), les personnels accèdent aux fonctions d'exploitation citées ci-avant. Plusieurs profils d'utilisateurs (visiteurs, opérateurs, mainteneurs, administrateurs...) donnent des droits d'accès différents à l'IHM. Dans le cas des supervisions multi-ouvrages, l'application cliente permet la mutualisation des ouvrages sur une interface unique garantissant une homogénéité des outils et interfaces.

Le **serveur d'archivage** stocke les données archivées de GTC - Supervision . Les données archivées (alarmes, états, commande, mesures...) sont utiles à l'exploitant tant pour le retour d'expérience suite à un évènement que pour la maintenance. Il est conseillé de dimensionner le serveur pour l'archivage minimum d'un an de données et de deux ans concernant les consommations d'énergie. Ce serveur peut être mutualisé entre plusieurs ouvrages, avec mise en œuvre d'une redondance.

2 LA GTC - SUPERVISION, UN OUTIL CENTRAL POUR L'OPÉRATEUR

Les tâches de supervision sont partagées entre le système de GTC - Supervision et l'opérateur. En fonctionnement normal, le système de GTC - Supervision assure le pilotage des équipements du tunnel de manière autonome sous la surveillance de l'opérateur. En situation événementielle ou en cas de dysfonctionnement, l'opérateur va assurer les tâches de décision, tout en s'appuyant sur la supervision qui va lui fournir les informations pertinentes, lui permettre d'agir et, le cas échéant, l'assister dans ses actions. Une bonne interaction entre cet outil central et l'opérateur participe à la sécurité à l'intérieur et aux abords du tunnel.

En plus de fournir des services pour l'exploitation en temps réel, certains systèmes de GTC - Supervision disposent de fonctionnalités visant à améliorer l'exploitation ou à fournir une assistance en cas d'évènement.

INTERACTIONS ENTRE LE SYSTÈME ET L'OPÉRATEUR

Le système de GTC supervision interagit avec l'opérateur par l'intermédiaire de l'IHM de supervision. Une bonne conception de l'IHM de supervision est ainsi primordiale pour faciliter la compréhension de la situation et optimiser la réactivité de l'opérateur, et par conséquent l'efficacité du système.

La conception doit aussi intégrer une réflexion sur la quantité et la nature des informations à faire remonter à l'opérateur. Plus spécifiquement, le sujet des alarmes est important. L'ensemble de ces informations doit constituer une aide et ne pas devenir contre-productif en polluant le travail de l'opérateur.

Conception de l'IHM et de l'environnement de travail

Une bonne conception de l'IHM est obtenue par la mise en œuvre d'une **démarche ergonomique,** dont le périmètre peut aussi intégrer plus largement l'environnement de travail de l'opérateur.

Cette démarche vise, à travers l'homogénéisation des interfaces, à faciliter la prise en main des outils par les utilisateurs, la formation de ceux-ci et leur utilisation quotidienne. Il est donc important que cette démarche implique les opérateurs dès son démarrage : ils sont les principaux utilisateurs de l'outil.

La **limitation de la charge mentale** de l'utilisateur est l'un des critères de la qualité ergonomique d'une IHM. Elle comprend la prise en compte de la charge visuelle, la limitation du nombre d'actions à effectuer par l'opérateur et une organisation des vues intuitive.

\ RETOUR D'EXPÉRIENCE

L'EXEMPLE DE LA DiRIF

Une démarche ergonomique impliquant les opérateurs a été mise en œuvre par la DiRIF dans la réalisation du nouveau Système d'Aide à la Gestion de Trafic Tunnel (SAGTu). Celle-ci, conduite par un ergonome, s'est déroulée en trois phases :

- Analyse du contexte : l'ergonome a tout d'abord observé durant une demi-journée dans chaque PCC le contexte de travail et analysé certains indicateurs pour chaque action de l'opérateur ;
- Conception itérative : l'ergonome a ensuite échangé lors d'ateliers avec les opérateurs (un par PCC) à partir d'une maquette interactive dans l'objectif de trouver la meilleure ergonomie pour chaque fonction ou thématique ;
- Spécifications : maquettage de l'outil et rédaction d'un cahier des charges.

Charge visuelle

Le contrôle de la charge visuelle passe par une **interface épurée** à la fois sur la représentation des ouvrages et sur l'utilisation des couleurs. L'un des enjeux est de **favoriser la détection d'un événement ou un dysfonctionnement**, en mettant en valeur seulement les singularités (évènements, dysfonctionnements...). La couleur ne doit jamais être la seule méthode utilisée pour transmettre une valeur ou un état, mais elle est un outil très efficace pour attirer l'attention de l'opérateur. Pour garantir une conception optimale de l'IHM, il est notamment primordial de définir une charte de couleurs et de s'y tenir. De nombreuses IHM modernes de supervision tunnel utilisent des dégradés de gris pour le fond et les éléments non dynamiques permettant ainsi de faire ressortir tous les états non nominaux avec des couleurs vives.

Organisation des vues

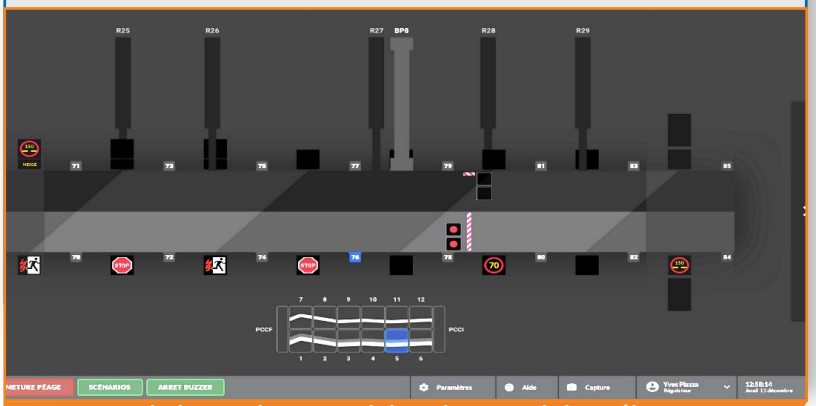
La navigation entre les différentes fenêtres doit être facilitée, avec l'utilisation **d'une vue de synthèse** qui doit faire ressortir les singularités, les bandeaux métiers, les raccourcis vers les commandes d'actions (scénarios, fermetures...) et les **raccourcis** vers les différentes sections de l'ouvrage ou de la voie.

\ RETOUR D'EXPÉRIENCE

L'EXEMPLE TUNNEL DE FRÉJUS // TUNNEL DU SOMPORT

La future IHM du tunnel du Fréjus, qui présente un affichage sobre avec une utilisation de dégradés de gris, afin de mettre en valeur les informations les plus importantes : alarmes, événements en cours, équipement en défaut ou inhibé...
Pour faciliter la navigation, cette IHM présente en partie basse, une carte synthétique « mini map » dans les vues de détail pour passer rapidement d'une section à l'autre.

Un choix différent a été réalisé au Tunnel du Somport, où l'ensemble des sections est visible en permanence avec la mise en place d'écrans panoramiques.



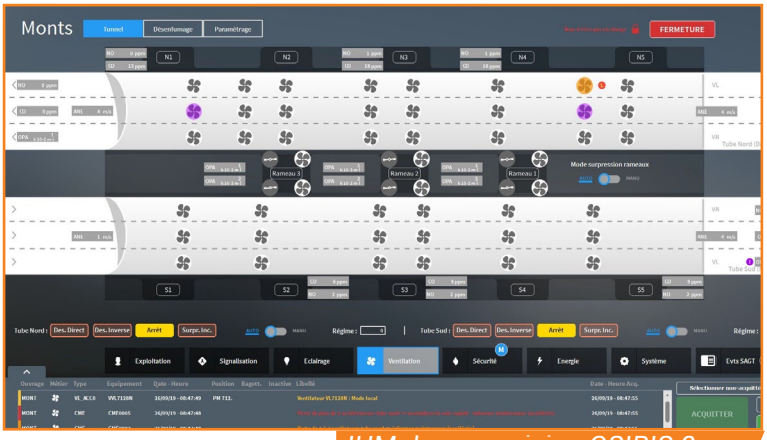
Maquette de l'IHM de supervision du tunnel du Fréjus

Les alarmes doivent, quant à elles, être visibles sur toutes les vues par l'intermédiaire d'un tableau situé en partie basse appelé **« fil de l'eau »**. Ces alarmes visuelles sont complétées par des alarmes sonores, dont le son peut varier en fonction du niveau d'alarme.

\ RETOUR D'EXPÉRIENCE

L'EXEMPLE OSIRIS 2

L'IHM de supervision OSIRIS 2 présente l'ensemble des alarmes dans le fil de l'eau ainsi qu'au niveau du bandeau « tunnels » (partie haute) sous la forme de pastilles de couleur. Une pastille par tunnel présente la couleur de l'alarme la plus critique et le nombre d'alarmes en cours, permettant à l'opérateur de voir très rapidement la situation de chaque tunnel.



IHM de supervision OSIRIS 2

Volume d'actions

Les actions à effectuer doivent être réduites à l'essentiel afin de limiter la charge mentale de l'utilisateur (par exemple limitation du nombre d'étapes pour accéder à une vue ou lancer un scénario). Il est particulièrement important que les scénarios d'urgence (incendie, fermeture) soient lancés avec un minimum d'actions, en mettant en place **des boutons de type « coup de poing »** sur toutes les vues. Le nombre de « clics », renseignant ainsi le volume d'actions, est l'un des indicateurs analysé lors de la démarche ergonomique de la DiRIF.

La gestion des alarmes

Afin de ne pas perturber le travail de l'opérateur et gagner en efficacité, il est recommandé de trier et/ou de filtrer les alarmes afin de ne conserver que celles qui lui seront utiles.

Tri et classement des alarmes

Toutes les alarmes sont prises en compte et traitées, mais il est recommandé de procéder à un tri entre les **alarmes techniques**, qui concernent l'état d'un équipement, et les **alarmes d'exploitation**, qui concernent un événement. Pour les alarmes qui n'impactent pas l'exploitation du tunnel, il n'est pas nécessaire de les porter à la connaissance de l'opérateur mais uniquement aux techniciens de maintenance.

Ce tri est réalisé au niveau de la GTC - Supervision ou du Système d'Aide à la Gestion de Trafic (SAGT) dans les paramètres de programmation en fonction des différents profils utilisateur en cohérence avec l'organisation de l'exploitation du PCC.

Pour chaque catégorie d'alarmes, il est ensuite possible de les classer en niveau d'importance pour faire ressortir les niveaux les plus critiques. Généralement, ces alarmes sont classées en trois niveaux d'importance avec une différenciation visuelle dans le «bandeau d'alarme» (couleur par exemple). L'objectif est de faire ressortir les alarmes nécessitant une action rapide de l'opérateur (incendie par exemple).

Le filtrage des alarmes

Certaines alarmes doivent être filtrées pour **ne pas engendrer des cascades d'alarmes** au risque de masquer celles qui sont importantes.

En effet, l'objectif des alarmes est bien d'avertir l'opérateur d'une situation anormale afin qu'il puisse l'identifier rapidement et agir en conséquence. Ainsi, si une alarme ne lui donne pas une information nouvelle et utile, il est préférable de ne pas la porter à connaissance de l'opérateur.

Le filtrage s'envisage plus particulièrement pour les alarmes techniques (exemple des cascades d'alarmes de perte d'alimentation électrique ou d'un bagotement consécutif à faux contact) ainsi que pour certaines alarmes d'exploitation comme celles liées à la DAI. Dans ce cas, le filtrage est souvent géré par le système DAI lui même.

\ RETOUR D'EXPÉRIENCE

DES EXEMPLES DE TRI D'ALARMES

Le tri des alarmes a été réalisé dans les supervisions du tunnel du Fréjus et OSIRIS 2. Pour le tunnel du Fréjus, la séparation des alarmes techniques de celles d'exploitation est complétée par une identification par des stimuli visuels et sonores distincts. Pour le superviseur OSIRIS 2, en plus des alarmes d'exploitation, seules les alarmes techniques qui ont un impact sur les CME sont remontées vers le profil de l'opérateur. Les autres alarmes techniques remontent seulement sur le profil mainteneur.

LES OUTILS CONNEXES DE LA SUPERVISION

Pour les PCC multi-tunnels ou avec des enjeux forts, la gestion de l'exploitation peut être facilitée grâce à la mise en œuvre d'outils connexes associés ou intégrés à la GTC - Supervision.

Il s'agit d'outils destinés à l'amélioration de la qualité de l'exploitation, en lien avec la formation des opérateurs ou au retour d'expérience suite à un événement.

Certains outils peuvent également assister les opérateurs dans la détection et dans la prise de décision, via un système d'aide à l'exploitation.

Outils connexes pour améliorer la qualité de l'exploitation

Le simulateur

Le simulateur est un outil au service de la **formation** et de l'**entraînement**. Il permet de former principalement les opérateurs, mais également, selon le niveau de fonctionnalité du simulateur, d'autres acteurs de la sécurité tels que les patrouilleurs ou les cadres d'astreinte. La simulation est réalisée sur une représentation du tunnel et permet d'utiliser l'ensemble des équipements sans conséquence sur le terrain.

Le système modélise les équipements (commande, état, mesure), réalise les remontées d'alarme et peut simuler les phénomènes physiques observés dans la réalité lors du fonctionnement de ces équipements. Le simulateur est parfois associé à d'autres systèmes virtualisés pour renforcer le réalisme de l'exercice comme la vidéosurveillance, la communication (RAU, radio, téléphone...), la simulation du trafic.

L'IHM du simulateur peut aller jusqu'à une **représentation exacte du superviseur**. La fidélité de cette reproduction va de pair avec l'acquisition des automatismes et des réflexes lors des exercices sur simulateur. Afin de garder sa pertinence dans le temps, le simulateur doit être mis à jour à chaque nouvelle version du superviseur. Ceci peut être réalisé de manière automatique par le système si l'option a été prévue préalablement.

\ RETOUR D'EXPÉRIENCE

L'EXEMPLE DU MONT-BLANC

La nouvelle supervision du Mont-Blanc, mise en œuvre en 2016 et nommée LOGOS (Localiser Organiser Gérer les Opérations de Sécurité), intègre un simulateur, mis en place avec un outil de rejeu et un serveur de développement. Ces outils ont été développés en même temps que la supervision, et présentent des IHM et des modes de fonctionnement identiques.

Le simulateur du tunnel du Mont-Blanc est destiné en premier lieu à la formation des opérateurs. Il permet aussi de valider et/ou tester les modifications réalisées sur la GTC - Supervision.

Le simulateur du tunnel du Mont-Blanc utilise un éditeur complet permettant de configurer l'événement à simuler, de paramétrer les équipements ou de créer de nouveaux scénarios de signalisation. Cet éditeur est identique à celui utilisé dans l'environnement de production.

Pendant une session de formation, le simulateur permet à un formateur d'agir en direct sur les états des équipements afin de tester la capacité de détection et d'analyse des opérateurs en cas de défaillance technique.

Enfin, il est possible, à travers un applicatif, de générer un rapport de formation directement alimenté par le simulateur.

Les simulateurs peuvent être équipés d'**un éditeur de scénarios de formation plus ou moins élaborés**. Les scénarios proposés sont soit basés sur des événements réels qui se sont produits, soit sur des situations imaginaires, soit une combinaison des deux. Ils peuvent être enregistrés dans la base de données du simulateur ou élaborés au cours de la formation.

Ils peuvent proposer deux types de formation : le **mode « exercice »** qui est encadré par un formateur ou le **mode «e-learning»** afin d'apprendre de manière autonome.

Pour que cet outil soit utile et utilisé, il est essentiel pour l'exploitant de s'investir dans la mise en place de ces formations (préparations, encadrement, corrections,...) et de donner de la disponibilité à l'opérateur pour qu'il puisse se former.

Outre l'intérêt d'améliorer les compétences des personnels, l'analyse d'une session de formation apporte un **retour d'expérience** à l'exploitant qui peut mettre en place des actions comme l'actualisation des procédures.

Enfin, certains simulateur offre la possibilité de tester, avant leur déploiement, soit des modifications de supervision soit une action ou un ensemble d'actions.

Le rejeu

À travers un applicatif de la supervision, la fonction de rejeu **reproduit des situations d'exploitation qui se sont réellement produites**. Il est ainsi possible d'analyser a posteriori la gestion de cette situation particulière dans le cadre du **retour d'expérience** ou de la **formation**.

Cette fonction se base sur les données archivées de GTC - Supervision. Elle peut rejouer un événement avec les actions d'exploitation engagées sur une plage de temps donnée.

Une session de rejeu se matérialise généralement par :

- L'animation de l'état et des mesures des équipements ;
- L'animation des différentes listes (alarmes techniques, alarmes d'exploitation, équipements inhibés, ...) ;
- L'apparition d'un bandeau de commande de la session de rejeu sous la forme d'un lecteur (état d'avancement dans la session de rejeu, lecture, pause, avancement...).

\ RETOUR D'EXPÉRIENCE

DES EXEMPLES DE REJEU

Les superviseurs OSIRIS 2 de la DIR CE et LOGOS du tunnel du Mont-Blanc disposent d'un outil de rejeu conçu conjointement avec le système de supervision.

L'outil de rejeu d'OSIRIS 2 permet de rejouer une situation sur un ouvrage et une période donnée. Il dispose d'une console de pilotage permettant d'éditer des marqueurs : marqueurs d'informations, pour repérer des moments spécifiques dans la séquence ou marqueurs de QCM (questions à choix multiples), pour mettre en pause le lecteur afin de poser une question à l'élève dans le cadre d'une séance de formation.

En plus de choisir la période d'analyse, l'outil de rejeu du Mont-Blanc permet de sélectionner les «métiers» à rejouer. Il est par exemple possible de rejouer une situation uniquement sur le «métier ventilation».

Aide à l'exploitation

Les systèmes d'aide à l'exploitation (SAE) sont très utilisés en gestion du trafic. En cas d'évènement, ces systèmes proposent un **plan d'action** en relation avec une **fiche événement**, constitué d'un ensemble d'actions cohérentes : commande d'équipements, proposition de communication aux services de secours et autres parties prenantes, consignes sous forme de texte...

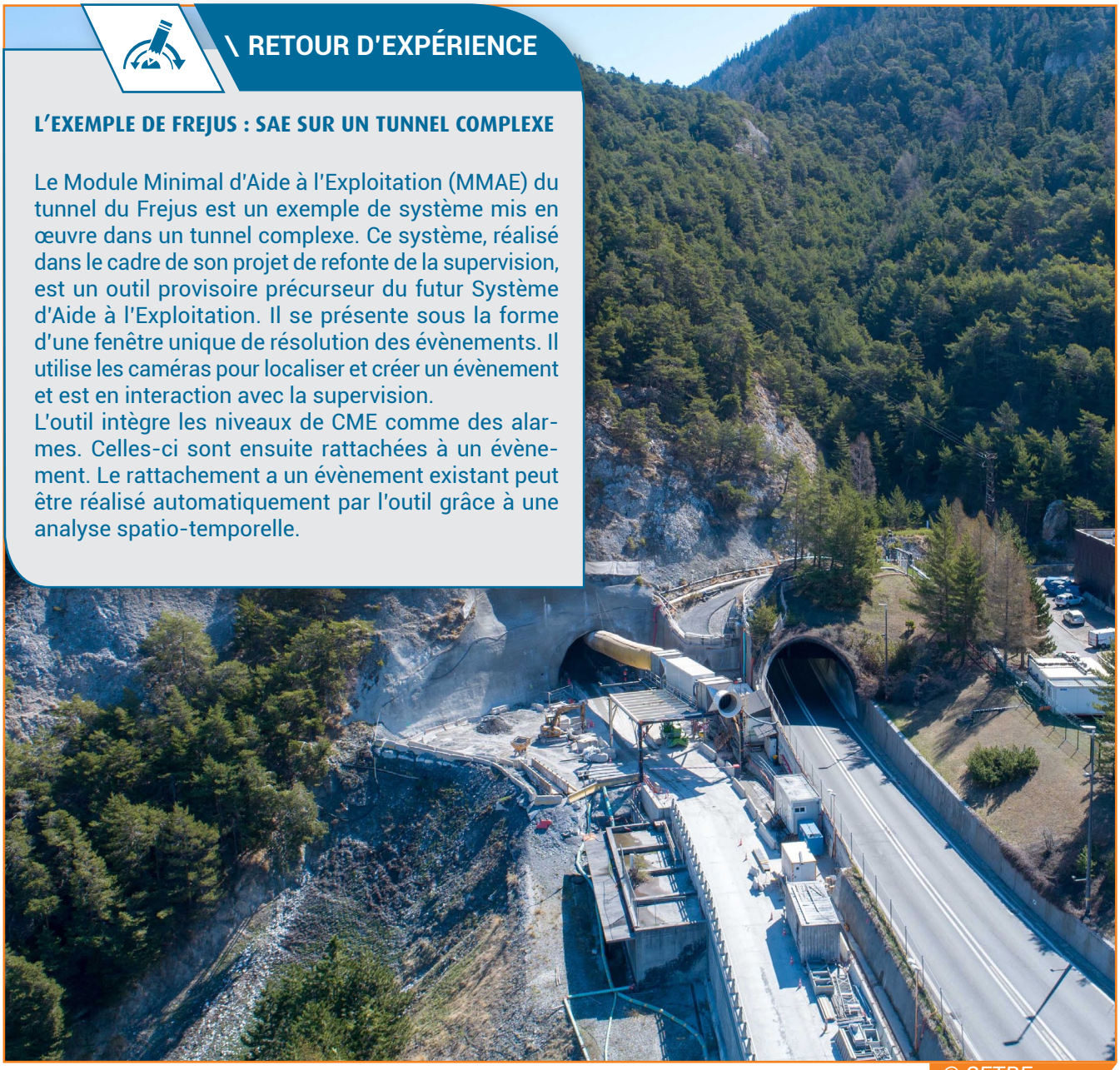
La Commission Nationale d'Évaluation de la Sécurité des Ouvrages Routiers (CNESOR), **recommande aux exploitants de tunnels de s'équiper d'un SAE** au fur et à mesure que s'élargit le périmètre d'intervention d'un PCC, avec la modernisation des tunnels surveillés par ce PCC ou le rattachement d'autres tunnels (Rapport d'Activité 2009-2012).

Pour la gestion de **tunnels complexes** (exemple du Frejus) ou **d'itinéraires comportant plusieurs tunnels** (exemple DIRIF), les SAE constituent être un vrai atout pour assister l'opérateur dans sa gestion de l'événement.

\ RETOUR D'EXPÉRIENCE

L'EXEMPLE DE FREJUS : SAE SUR UN TUNNEL COMPLEXE

Le Module Minimal d'Aide à l'Exploitation (MMAE) du tunnel du Frejus est un exemple de système mis en œuvre dans un tunnel complexe. Ce système, réalisé dans le cadre de son projet de refonte de la supervision, est un outil provisoire précurseur du futur Système d'Aide à l'Exploitation. Il se présente sous la forme d'une fenêtre unique de résolution des évènements. Il utilise les caméras pour localiser et créer un évènement et est en interaction avec la supervision.
L'outil intègre les niveaux de CME comme des alarmes. Celles-ci sont ensuite rattachées à un évènement. Le rattachement a un évènement existant peut être réalisé automatiquement par l'outil grâce à une analyse spatio-temporelle.



© SFTRF

LA GTC - SUPERVISION, UN OUTIL CENTRAL POUR L'OPÉRATEUR

L'interfaçage du SAE avec la GTC-Supervision permet d'agréger les alarmes et d'intégrer l'application des scénarios dans les plans d'actions proposés.

En cas de gestion d'un itinéraire avec présence d'un ou plusieurs tunnels, il est important que les actions proposées soient cohérentes avec la gestion globale de l'itinéraire.

De plus, si la surveillance de ce réseau est effectuée depuis plusieurs PCC, un SAE offre alors une interface harmonisée et facilite la mise en œuvre de procédures communes (exemple norvégien).

En outre, certains SAE disposent de fonctionnalités avancées, telle que la gestion de conflits avec d'autres plans d'actions, ou l'assistance aux services de secours.

\ RETOUR D'EXPÉRIENCE

L'EXEMPLE DE LA DIRiF : SAE SUR UN ITINÉRAIRE COMPORTANT PLUSIEURS TUNNELS

La DiRIF possède deux couches de systèmes d'aide à l'exploitation :

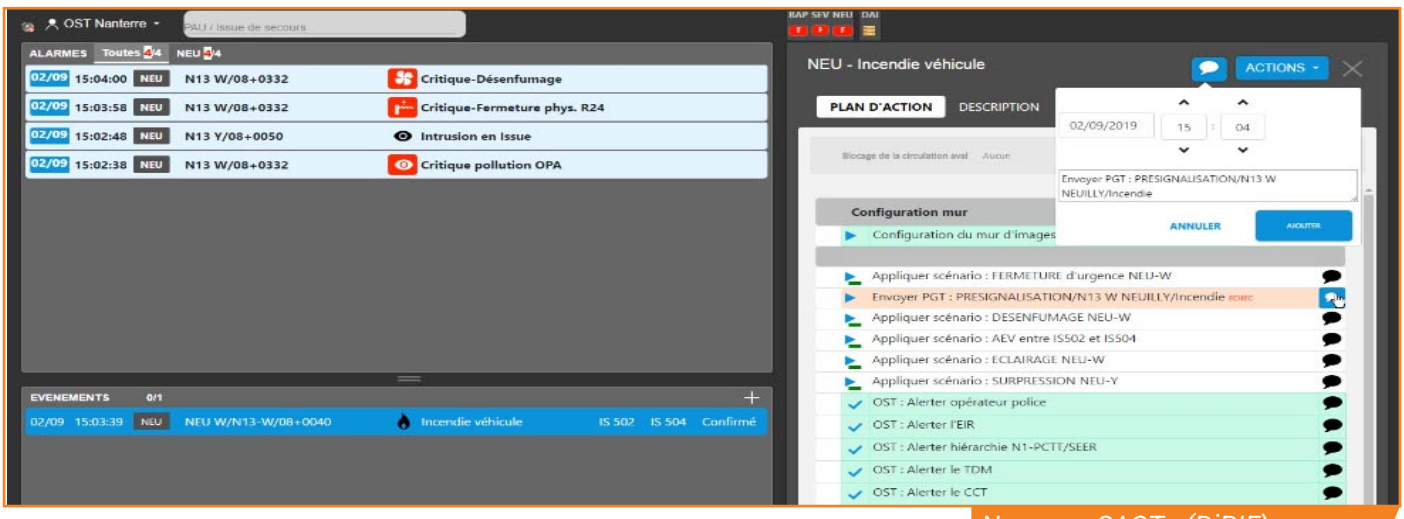
- Le Système d'Aide à la Gestion de Trafic SIRIUS, qui pilote l'ensemble des équipements de gestion de trafic;
- Le nouveau Système d'Aide à la Gestion des Tunnels (SAGTu) qui pilote l'ensemble des équipements de sécurité en Tunnel grâce à un interfaçage avec la GTC - Supervision.

Un évènement peut être créé par le SAGTu (après validation de l'opérateur) suite aux alarmes issues de la GTC - Supervision. Le plan d'action proposé peut imposer au SAGT Sirius l'application d'un Plan de Gestion de Trafic (PGT). Inversement, un événement de type bouchon peut être créé dans le SAGT Sirius. S'il impacte la sécurité des tunnels, il proposera un PGT et transmettra une alarme d'exploitation au SAGTu.

\ RETOUR D'EXPÉRIENCE

L'EXEMPLE NORVÉGIEN : UN SAE POUR UNIFORMISER LES PROCÉDURES ENTRE PCC

Un outil d'aide à l'exploitation sera bientôt déployé dans les cinq PCC des routes nationales norvégiennes. En particulier, le PCC d'Oslo exploite un réseau complexe comportant de nombreux tunnels avec un bon niveau d'équipement. Cet outil a pour vocation de remplacer les fiches opérateurs et d'harmoniser les procédures entre PCC. Il automatise les procédures en cas d'événement, depuis l'ouverture de la fiche événement suite à un signalement (annonces travaux, appels usager, détection par l'opérateur) jusqu'à la proposition d'actions et transmet automatiquement les informations aux usagers par le biais des PMV. Un logigramme dynamique permet de suivre l'ensemble de la procédure du traitement de l'événement. L'outil n'est pour l'instant pas interfacé avec la GTC-Supervision des tunnels, mais il est prévu qu'il le soit à terme.



Nouveau SAGTu (DiRIF)

3 LA RÉNOVATION D'UNE GTC - SUPERVISION

La rénovation d'une GTC - Supervision existante est un enjeu d'actualité pour beaucoup d'exploitants, notamment en France où de nombreuses installations ont été réalisées au début des années 2000 suite à la publication de l'IT.

Le renouvellement des équipements de GTC - Supervision relève, comme les autres équipements, d'une **démarche anticipée de renouvellement**. Le fascicule 40 donne des indications sur les durées de vie type de ces équipements. Celles-ci, indicatives, se situent entre 10 et 20 ans selon le type d'équipement. Cette période est cohérente avec l'évolution rapide de ce type de matériel et de logiciel, qui engendre en fin de vie des problématiques de réapprovisionnement des pièces de rechange ou de mise à jour de certains logiciels.

Parallèlement à cette problématique de renouvellement des matériels ou des logiciels, les projets de rénovation peuvent aussi être motivés par des objectifs de **mise à niveau d'architecture** ou de **mutualisation** de systèmes ou de PCC.

L'une des contraintes principales d'un projet de rénovation de GTC est celle des **travaux sous exploitation**. Celle-ci implique de trouver des solutions techniques pour maintenir une solution de supervision pendant la durée du chantier et limiter les fermetures pour réaliser les basculements et les essais, sans entraîner de régression du niveau de sécurité. Les projets de rénovation d'Osiris 2 et du contournement de Neuchâtel, présentés ci-après, illustrent des solutions techniques possibles pour répondre à cette problématique.

Par ailleurs, la conception d'une **GTC - Supervision durable** est un enjeu important. Cela signifie que celle-ci puisse, de la manière la plus économique possible, s'adapter aux nouvelles conditions d'exploitation tout en suivant les dernières évolutions technologiques.

On constate aussi que la **virtualisation de serveurs** est mise en œuvre dans de nombreux projets de rénovation, car elle permet de répondre aux problématiques d'obsolescences tout en offrant des fonctionnalités supérieures en matière de maintenance.

RÉNOVER SOUS EXPLOITATION

Afin de **gérer les contraintes d'exploitation**, les gestionnaires du contournement de Neuchâtel (Route Nationale Arc Jurassien en Suisse) et d'OSIRIS 2 (DIR CE) ont trouvé des **solutions techniques** pour leur projet de rénovation de GTC - Supervision.

Les deux objectifs de la rénovation de la GTC de Neuchâtel étaient, d'une part, de remplacer des équipements vieillissants et d'autre part, de mettre en conformité l'architecture de GTC - Supervision au regard des dernières prescriptions de l'OFROU (Office Fédéral des Routes -Suisse-).

Le projet de rénovation du superviseur OSIRIS 2 (DIR CE) avait, quant à lui, pour but principal d'harmoniser les supervisions de huit tunnels exploités depuis un PCC unique.

Le point commun entre ces deux solutions est la **mise œuvre d'équipements entre la couche automate et la nouvelle couche supervision**, de manière transitoire pour la GTC de Neuchâtel ou définitive dans le cas du superviseur OSIRIS 2.

\ RETOUR D'EXPÉRIENCE

L'EXEMPLE DE NEUCHÂTEL : LES OUTILS PASSERELLE ET LA PLATEFORME D'INTÉGRATION

La passerelle s'intercale entre les anciens automates et le système de supervision. Elle est constituée d'une partie automate, permettant l'interfaçage avec les anciens automates et d'une partie informatique, utilisant des serveurs virtualisés.

Cette passerelle découple la rénovation des équipements de terrain et la rénovation de la partie supervision. La partie IHM a ainsi pu être modernisée rapidement sans corrélation avec le renouvellement des équipements.

La plateforme d'intégration et de simulation a été réalisée en acquérant d'anciens automates pour reconstituer une plateforme identique à celle du terrain. Elle a ainsi permis de simuler les systèmes, les interfaces (passerelle/terrain et passerelle/système de gestion), et les fonctionnalités de l'ancien système de supervision avant la bascule vers le nouveau système.

\ RETOUR D'EXPÉRIENCE

L'EXEMPLE DE OSIRIS 2 : MISE EN PLACE D'AUTOMATES FRONTAUX

La solution retenue utilise des automates frontaux comme passerelle. Ceux-ci sont placés à l'interface des automates ouvrages (existants) et des nouveaux serveurs de supervision. Leur rôle est de convertir les données hétérogènes du terrain (émanant des automates ouvrages) en données homogènes et de les transmettre à la couche de supervision. Pour chaque ouvrage, les automates frontaux et les nouveaux serveurs de supervision sont redondants. Le système est unifié au niveau des postes client de supervision.

Cette solution a eu pour intérêt de faciliter le déploiement en n'impactant pas le système en place. Les automates ouvrages n'ont pas été modifiés, limitant d'une part la requalification des développements suite à l'intégration des nouvelles fonctions et d'autre part les tests de non régression.

Le développement s'est fait en parallèle de l'ancien système, qui restait le système d'exploitation tant que les tests sur le nouveau système n'étaient pas achevés.

Cette solution présente aussi des atouts en termes d'adaptation et d'évolutivité, car le travail est réalisé uniquement sur le nouveau système, homogène et maîtrisé.

RÉALISER UNE GTC - SUPERVISION DURABLE

Une GTC - Supervision est un objet coûteux et complexe et la **durabilité de ce système doit être une préoccupation constante**.

Le caractère durable d'une installation de GTC - Supervision est lié aux solutions techniques ainsi qu'à la façon dont elles sont mises en œuvre . Elle s'évalue selon divers critères tels que l'interopérabilité, l'évolutivité ou la maintenance.

L'interopérabilité, c'est-à-dire la capacité du système de supervision à fonctionner avec d'autres systèmes, est souvent obtenue en imposant certains protocoles de communication standards comme les protocoles Modbus ou OPC UA (Open Platform Communications Unified Architecture).

Au niveau du système de supervision, les plateformes logicielles « ouvertes » sont des solutions diffusées à des milliers d'exemplaires et qui peuvent être proposées par n'importe quel fournisseur. Elles permettent notamment des modifications et des développements ultérieurs par n'importe quel prestataire, favorisant ainsi l'évolutivité et la maintenance.

Le développement, tant au niveau automate qu'au niveau supervision, doit être réalisé dans les règles de l'art. Les langages standards sont à privilégier et en particulier les langages graphiques pour la programmation des automates. L'ensemble des développements doit être suffisamment commenté, à la fois dans le code de programmation qu'au niveau de la documentation technique fournie dans le cadre du dossier des ouvrages exécutés.

LA VIRTUALISATION DES SERVEURS

La virtualisation des serveurs s'est progressivement généralisée pour devenir désormais la norme tant pour les projets neufs que pour les projets de rénovation.

Il s'agit d'un mécanisme informatique qui consiste à **faire fonctionner plusieurs systèmes**, serveurs ou applications, sur un **même serveur physique**. Ce serveur héberge le système hôte, nommé hyperviseur. Un hôte peut accueillir plusieurs systèmes d'exploitation « invités » dans des environnements clos et indépendants appelés machines virtuelles (anglais «virtual machine» - VM).

Plusieurs architectures sont possibles pour le stockage des VM, soit dans une baie de stockage, soit directement dans les serveurs de virtualisation.

La première méthode, qui est nécessaire notamment pour disposer de la **fonction haute disponibilité** de l'architecture de virtualisation, est la plus lourde en termes de matériel et de développement.

Lorsqu'elle est correctement mise en œuvre, la virtualisation **présente de nombreux atouts** comme notamment une meilleure allocation des ressources informatiques, une plus grande disponibilité des systèmes, des gains potentiels d'énergie et d'encombrement ainsi que des économies financières possibles. Cette solution permet aussi de faire fonctionner des systèmes obsolètes, pour lesquels il n'existe plus de support physique capable de les supporter. La maintenance et les mises à jour sont facilitées grâce aux fonctionnalités de la virtualisation : VM facilement cliquable et réplicable (comme des dossiers informatiques), utilisation d'environnement de tests pour contrôler des modifications avant mise en production...

\ RETOUR D'EXPÉRIENCE

L'EXEMPLE DE LA VIRTUALISATION DES SERVEURS DE GTC DU TUNNEL DU LIORAN

La DIR MC a mis en œuvre la virtualisation dans le cadre du projet de rénovation des serveurs de GTC - Supervision du tunnel du Lioran.

Les deux serveurs de GTC - Supervision et le serveur d'archivage ont été virtualisés. Le choix a été fait de stocker directement les VM dans les serveurs de virtualisation, ce qui est la solution la moins lourde en matière de matériel et de développement. En effet, certaines fonctions proposées par le stockage centralisé en baie de stockage, comme la fonction haute disponibilité de l'architecture de virtualisation, n'étaient pas nécessaires dans ce projet.

Le retour d'expérience sur ce projet fait état de certaines difficultés comme le manque de qualification en virtualisation de l'entreprise en charge des travaux, la gestion des licences de supervision (support physique) ainsi que des problèmes d'affichage du logiciel de supervision.

En plus de répondre aux problématiques d'obsolescence et de regroupement des serveurs, la virtualisation a apporté des gains en matière de maintenance, pour un coût maîtrisé. Cette rénovation constituait aussi une étape dans la démarche de sécurisation des systèmes d'information du réseau de la DIR MC.

4 LES ENJEUX DE CYBERSÉCURITÉ

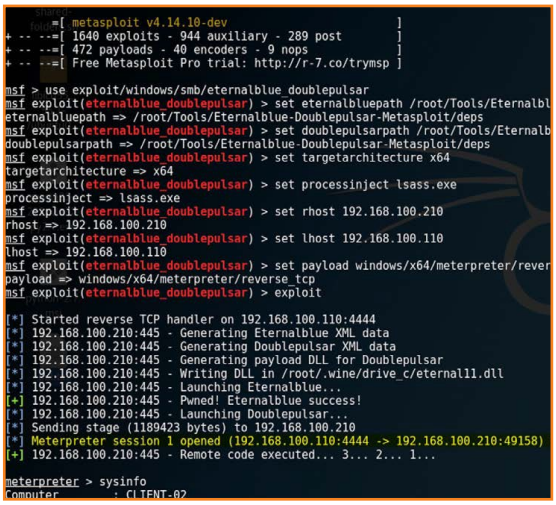
Les organisations font actuellement face à une **hausse importante de la cybercriminalité**. En particulier, le secteur industriel éveille un intérêt grandissant des malfaiteurs avec une multiplication des attaques depuis 2010.

L'exemple le plus connu est l'attaque du système SCADA[1] des centrifugeuses d'une usine d'enrichissement d'uranium iranienne en 2010 par le ver informatique STUXNET. Cependant, la majorité des attaques contre les systèmes industriels ne sont pas nécessairement ciblées et peuvent concerner n'importe quelle installation, stratégique ou non.

1 Supervisory Control And Data Acquisition

SPÉCIFICITÉS DES SYSTÈMES INDUSTRIELS

Les systèmes industriels sont tout autant concernés par les cybermenaces que les systèmes informatiques. Les évolutions récentes, avec l'utilisation de composants standardisés, le recours systématique à une maintenance externalisée, la numérisation massive, les interconnexions avec les systèmes informatiques, ont **augmenté le risque et la surface d'attaque**.



Les systèmes industriels présentent, par rapport aux systèmes informatiques, un certain **nombre de fragilités** :

- systèmes pensés avant tout pour assurer la **continuité d'exploitation**, ce qui a plusieurs conséquences : difficultés pour procéder aux mises à jour, architecture complexe, surface d'attaque importante, équipements dans des locaux non protégés ;
- **durée de vie importante** : risque d'obsolescence et d'arrêt de développement des correctifs de sécurité par les fabricants ;
- **superposition** de systèmes d'âges différents ;
- **fausse impression de sécurité** même avec des systèmes industriels dits isolés ou lorsqu'ils sont basés sur des protocoles industriels...

Ce dernier point est illustré par l'incident «Stuxnet» qui a impacté un réseau pourtant non relié au monde extérieur. Des portes d'entrées au système existent toujours, et sont même particulièrement nombreuses dans les installations industrielles, qui disposent souvent d'un grand nombre de composants sur un périmètre important, comme dans le cas des tunnels.

QUELQUES PISTES DE MESURES

La cybercriminalité est une **menace réelle** qui doit être traitée de façon globale et intégrée dans toute l'organisation.

Il s'agit, pour les exploitants de tunnels de prendre des **mesures adaptées** pour gérer ce risque.

Pour cela, il est important d'intégrer les exigences de sécurité des systèmes d'informations (SSI) dans toutes les phases du cycle de vie d'une GTC - Supervision, du cahier des charges jusqu'aux contrats de maintenance.

Il est indispensable pour l'exploitant, de bien connaître son système d'information et industriel, en réalisant notamment une **cartographie du système**, avec une veille sur les menaces potentielles et les vulnérabilités possibles.

La réalisation **d'audits de cybersécurité** réguliers est une autre mesure importante pour améliorer le niveau de sécurité des installations.

La **sensibilisation des personnels** aux bonnes pratiques par des formations régulières est nécessaire.

Le **cadrage des intervenants** sur le système doit être anticipé : problématique des connexions et des supports amovibles, interventions des prestataires extérieurs…

Les mesures de protection sont nécessaires mais pas suffisantes, l'exploitant doit aussi se **préparer à la gestion d'une crise cybersécurité** : détection, plans de continuité et de reprise de l'activité.

\ LE RÉFÉRENTIEL RÉGLEMENTAIRE ET NORMATIF

La norme CEI 62443 constitue le référentiel pour aider le monde industriel à faire face aux cybermenaces. En parallèle, il existe la norme CEI 27000 qui est dédiée aux systèmes d'information.

L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) est un acteur incontournable en France concernant la problématique de la cybersécurité. Elle rédige et met à la disposition de tous des guides techniques ou des recueils de bonnes pratiques, dont certains concernent spécifiquement les systèmes industriels en tunnel[1] ou certains équipements. En outre, l'ANSSI certifie ou qualifie des équipements, comme les pare-feux ou les automates.

Au niveau national, le cadre de protection des infrastructures vitales pour la sécurité de la nation est traité par la Loi de Programmation Militaire (LPM) qui identifie les OIV (Opérateurs d'Importance Vitale). La LPM contient des dispositions pour renforcer le niveau de sécurité informatique des Opérateurs d'Importance Vitale : règles de sécurité, notification des incidents, audits et mesures en réponse aux crises. En tant qu'autorité nationale en matière de cybersécurité et de cyberdéfense, l'ANSSI est en charge de piloter ce dispositif et accompagne les OIV dans la mise en œuvre des nouvelles mesures. La liste des OIV est fixe et confidentielle.

Au niveau européen, la directive NIS (Network and Information Security) définit les Opérateurs de Services Essentiels (OSE). Elle a été transposée en droit français par un décret du 23 mai 2018 dont l'annexe précise la liste des services essentiels comprenant notamment les infrastructures routières.

Les OSE sont soumis à un certain nombre de règles : audit, déclarations d'incident, règles d'organisation et de conformités. Les exploitants routiers (publics et privés) figurent dans cette liste confidentielle. La liste des OSE est amenée à évoluer : le premier ministre peut compléter la liste par arrêté, en concertation avec l'ANSSI, le ministère et l'organisme concerné.

1 «La cybersécurité des systèmes industriels : étude de cas dans un tunnel routier, ANSSI , 2016

Quelques mesures techniques permettent d'améliorer le niveau de protection (liste non exhaustive et à adapter) :

- cloisonnement des réseaux avec l'utilisation de pare-feux certifiés et correctement programmés et la mise en place de réseaux locaux virtuels (VLAN) : GTC, administration, vidéo, voix… ;
- filtrage des adresses MAC (Media Access Control) sur les ports utilisés et le blocage des ports inutilisés ;
- bonne gestion de l'authentification des intervenants, et notamment la création de profils utilisateur individuels (consultation, exploitation, maintenance, administration…) et la mise en place du principe de moindre privilège (c'est-à-dire accorder à l'utilisateur le niveau d'accès minimum requis pour accomplir son travail) ;
- modification systématique et au plus tôt des mots de passe par défaut lorsque les systèmes en contiennent ;
- mise à jour systématique de l'ensemble des logiciels, et notamment les logiciels de supervision et automate. La configuration des pare-feux doit permettre cette mise à jour.

Un travail de recherche est en cours au CETU pour aider les exploitants à prendre en compte à cette menace.

5 PERSPECTIVES

L'atelier thématique du GTFE du 10 octobre 2019 a réuni exploitants de tunnels et professionnels pour rendre compte des pratiques et enjeux dans le domaine de la GTC - Supervision de tunnel. Les échanges ont été riches et ont permis de dégager des perspectives à court et moyen termes.

PERSPECTIVES À COURT TERME

L'objectif d'un système de GTC - Supervision est de faire fonctionner les équipements de sécurité du tunnel. Depuis quelques années, on assiste à une évolution vers des systèmes de plus en plus perfectionnés et complexes, qui gèrent un grand volume de données et sont en interface avec de nombreux métiers.

Les nouvelles GTC - Supervision offrent de nombreuses possibilités pour faciliter et optimiser l'exploitation ou la maintenance des tunnels. Des outils annexes tels que les simulateurs répondent aussi à des besoins de formation et retours d'expérience pertinents pour la montée en compétence de l'exploitant.

Si toutes ces évolutions peuvent effectivement apporter une aide intéressante à des PC souvent de plus en plus centralisés et distants du terrain, la sécurité des usagers et la bonne gestion du patrimoine doivent rester au cœur du sujet. Il semble alors important que l'exploitant conserve le contrôle et la compréhension de son système, tant pour l'exploitation que pour la maintenance de ses ouvrages. Une autre préoccupation est de trouver le bon niveau entre les fonctionnalités d'aide et la surabondance d'informations qui peut nuire à la réactivité.

Au regard du coût et de la complexité de rénovation des systèmes de GTC - Supervision, la durabilité reste un paramètre essentiel. Un équilibre est à trouver entre des systèmes de plus en plus intégrés et innovants et la nécessité de durabilité et d'interopérabilité de la GTC - Supervision.

PERSPECTIVES À MOYEN TERME

La révolution numérique en cours, que ce soit dans le domaine des transports, avec l'avènement dans un futur proche des véhicules connectés, ou dans le domaine de l'informatique, avec le développement de l'Intelligence Artificielle, impactera certainement les systèmes de GTC - Supervision.

D'un côté les GTC - Supervisions constituent déjà le support des équipements de demain pour accueillir les nouveaux véhicules connectés : les futurs systèmes pourront interagir avec ces véhicules pour avoir des données précises comme l'état et le type de véhicule, le nombre d'occupants, ou la source d'énergie et l'infrastructure sera en capacité de transmettre aux véhicules des informations et consignes de sécurité. D'un autre côté de nouveaux enjeux doivent être appréhendés pour garantir le bon fonctionnement et la sécurité des systèmes comme la cybersécurité et la sûreté de fonctionnement. Dans ce contexte évolutif, plusieurs actions de recherche sont à conduire pour une meilleure adéquation des systèmes de GTC - Supervision et de l'organisation de l'exploitant avec ces perspectives.

L'Intelligence Artificielle et plus spécifiquement le « Machine Learning » (apprentissage automatique), dont le développement est encore à ses balbutiements, pourrait apporter un jour une aide dans la gestion et l'analyse de ce grand volume de données. On pense en particulier à un système capable de prédire les incidents ou adapter les actions d'exploitation. Mais là aussi, la question de la pertinence de la technologie et de la maîtrise du système devra être posée.

\ ACTIONS DE RECHERCHES DU CETU

- **Sûreté de fonctionnement** : définition d'une méthodologie permettant d'attribuer aux moyens techniques des tunnels routiers, dont les systèmes de GTC Supervision, des niveaux de « sûreté de fonctionnement » quantifiables en fonction de leur contribution à la maîtrise des risques ;
- **Démarche de professionnalisation pour l'exploitation des tunnels routiers et modalités de mise en œuvre** : l'objectif est de fournir aux exploitants de tunnels routiers des éléments leur permettant de mettre en place, d'adapter et de décliner au mieux, dans le contexte spécifique de leurs ouvrages, la démarche de professionnalisation pour leurs personnels (opérateurs, mainteneurs, agents d'exploitation, cadres d'astreinte …).
- **Cybersécurité dans le domaine des tunnels routiers** : définition du cadre de la cybersécurité en tunnel et de recommandations adaptées au contexte de chaque tunnel tant au niveau organisationnel que technique ;
- **Système de Transport Intelligent (STI) et communications en tunnel** : accompagnement de la communauté STI aux contraintes et aux opportunités liées aux tunnels et exploration des possibilités offertes par les STI en tunnel, en lien avec les expérimentations en cours ou en projet.

GLOSSAIRE

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
API	Automate Programmable Industriel
CME	Condition Minimale d'Exploitation
DAI	Détection Automatique d'Incidents
GTC	Gestion Technique Centralisée
IHM	Interface Homme Machine
IT	Instruction Technique / Annexe 2 à la circulaire interministérielle 2000-63 du 25 août 2000 relative à la sécurité dans les tunnels du réseau routier national
LOGOS	Localiser Organiser Gérer les Opérations de Sécurité
LPM	Loi de Programmation Militaire
MESD	Modules d'Entrée/Sortie Déportées
MMAE	Module Minimal d'Aide à l'Exploitation
NIS	Network and Information Security
OIV	Opérateur d'Importance Vitale
OSE	Opérateur de Services Essentiels
PCC	Poste de Contrôle-Commande
PGT	Plan de Gestion de Trafic
PMV	Panneau à Message Variable
RAU	Réseau d'Appel d'Urgence
SAE	Système d'Aide à l'Exploitation
SAGT	Système d'Aide à la Gestion du Trafic
SAGTu	Système d'Aide à la Gestion du Trafic Tunnel
SSI	Sécurité des Systèmes d'Informations
VM	Machine Virtuelle

La GTC - Supervision est un système clé pour permettre les bonnes conditions de trafic et pour assurer la sécurité des usagers. Ce système qui possède un cadre réglementaire et technique, est en constante évolution.

Les exploitants de tunnels et des acteurs impliqués dans cette thématique ont fait part de leur retours d'expériences lors de l'atelier du GTFE du 10 octobre 2019.

Ce document synthétise les échanges autour du sujet de la GTC - Supervision.

Il aborde l'interaction du système avec l'opérateur, présente ensuite des solutions liées aux contraintes de rénovation sous exploitation, aborde la thématique d'un système durable et présente une technologie qui se généralise : la virtualisation.

Enfin, ce document sensibilise l'exploitant à la cybersécurité en fournissant des éléments de cadrage et des préconisations.

Centre d'Études des Tunnels
25, avenue François Mitterrand
69800 BRON Cedex

Tél. +33 (0)4 72 14 34 00
Fax. +33 (0)4 72 14 34 30
gtfe@developpement-durable.gouv.fr

GTFE