Organisme d'Enquête sur les Accidents et Incidents Ferroviaires

Rapport d'enquête de sécurité

INCIDENT DE SIGNALISATION
OTTIGNIES - 28 JUILLET 2014

.be

Juin 2015

Toute utilisation de ce rapport dans une perspective différente de celle de la prévention des accidents - par exemple celle de définir des responsabilités, et a fortiori des culpabilités individuelles ou collectives - serait effectuée en distorsion totale avec les objectifs de ce rapport, les méthodes utilisées pour le bâtir, la sélection des faits recueillis, la nature des questions posées, et les concepts qu'il mobilise, auxquels la notion de responsabilité est étrangère. Les conclusions qui pourraient alors en être déduites seraient donc abusives au sens littéral du terme.

TABLE DES MATIERES

1. RÉSUMÉ

Le lundi 28/07/2014 vers 21h21, un train (E2020) circule selon un itinéraire tracé qui traverse de multiples aiguillages dans le gril de la gare d'Ottignies.

Alors que ce train a fini de parcourir son itinéraire et qu'il continue son trajet en sortant du gril d'Ottignies, l'opérateur du poste de signalisation remarque que l'itinéraire de ce train ne se libère pas.
Vers 21h22'24", conformément aux procédures et à la réglementation, l'opérateur applique une fonction de secours NT du système EBP afin de détruire l'itinéraire.

A 21h22'45", un autre itinéraire est tracé automatiquement par le système Automatic Route Setting (ARS) pour un second train (E6592). Le système ARS commande le signal à l'ouverture et le train commence à parcourir l'itinéraire.
Alors qu'il en a parcouru la première partie, la seconde partie de cet itinéraire se détruit.

L'opérateur peut suivre, sur son écran, le parcours des itinéraires des trains circulant dans la zone qu'il contrôle. Lorsqu'un itinéraire a été enclenché, c'est-à-dire confirmé pour un train, la représentation des zones enclenchées se colore en vert. En fonction de l'évolution du train, la représentation des zones occupées par le train se colore en rouge.
Si un train occupe un itinéraire non enclenché, l'occupation est qualifiée d'intempestive et l'image du tronçon correspondant se colore de bistre/orange, un message apparait à l'écran et le système EBP engage automatiquement certaines mesures de protection: c'est ce qu'observe l'opérateur pour le train E6592 suite à la destruction de la seconde partie de son itinéraire.
Sur le terrain, rien ne permet au conducteur de se rendre compte que la zone qu'il parcourt n'est pas enclenchée et il poursuit donc son trajet. Le train sort du gril d'Ottignies.
Il n'y a pas de danger, c'est pourquoi l'opérateur laisse le train poursuivre son trajet.

Le franchissement irrégulier par un train d'un signal desservi protégeant une zone non enclenchée est détecté par le système comme une anomalie nommée DOBMI (Detectie/Détection Ontijdige Beweging Mouvement Intempestif) et est enregistrée par le système informatique du poste de signalisation.
Selon les procédures en place chez Infrabel, les enregistrements de DOBMI font l'objet d'une analyse afin d'en déterminer les causes (SPAD, défaillance d'un organe de détection dans la voie,…).
L'analyse de l'anomalie survenue à Ottignies a mis en évidence les conditions particulières ayant entraîné la libération de l'itinéraire du second train alors qu'il était parcouru.

Cet incident n'est pas un accident grave et ne devait pas être signalé directement à l'Organisme d'Enquête. Sur base des informations contenues dans le rapport des faits envoyé automatiquement par le gestionnaire d'infrastructure, l'Organisme d'Enquête a décidé d'ouvrir une enquête afin de déterminer les causes directes, indirectes et sous-jacentes ayant mené à cet incident, et de vérifier les mesures prises par Infrabel.

Le poste de signalisation d'Ottignies commande la signalisation du gril d'Ottignies : son rôle consiste, en toute sécurité, à placer les aiguillages dans la bonne position et à ouvrir les signaux devant les trains afin de les diriger vers les voies qu'ils doivent emprunter.
Le poste de signalisation assure cette gestion à 2 niveaux : le niveau "commande" et le niveau "enclenchement". Le niveau commande est assuré par le système EBP développé par la société Siemens. Il reçoit les requêtes des opérateurs de signalisation et les transmet au niveau "enclenchement" qui traite ces requêtes en sécurité.
A Ottignies, le niveau enclenchement est assuré par un enclenchement électronique/informatique de type SmartLock : c'est dans ce système informatique que sont programmées les règles de sécurités et les incompatibilités de manœuvre.

La gestion de l'interface entre les deux sous-systèmes EBP et SmartLock permettait l'envoi simultané de commandes normales et de commandes de secours : cette gestion de l'interface entre le système EBP et le système SmartLock est une des causes indirectes de l'incident.
Les analyses réalisées par Infrabel suite à l'incident d'Ottignies ont démontré que ce mode de gestion permettait que des commandes de tracé de route s'imbriquent dans des commandes de sécurité issues de la fonction NT initiée par l'opérateur. Cette imbrication des commandes de tracé de routes et des commandes de sécurité a entraîné la destruction de l'itinéraire du second train alors que l'itinéraire était parcouru.

Les enclenchements de type SmartLock remplacent un autre type d'enclenchement informatique, les enclenchements de type Solid State Interlocking (SSI). Les analyses réalisées par Infrabel pour ce remplacement n'avaient pas mis en évidence l'existence d'un problème potentiel suite à l'introduction de ce nouveau protocole entre le système EBP et l'enclenchement : la gestion des interfaces entre l'enclenchement SSI et l'EBP n'autorise pas l'envoi de commandes normales tant que les commandes de secours n'ont pas toutes été exécutées, ce qui n'était pas le cas pour l'enclenchement SmartLock.
Infrabel a mis en place un système de gestion du changement (*change management*), qui prévoit de réaliser des analyses en cas de modification importante avec un impact sur la sécurité du trafic ferroviaire. Ces analyses réalisées lors du changement de type d'enclenchement n'ont pas permis d'identifier le problème potentiel induit par la différence de protocole de gestion des interfaces.

La présence de boucle de récupération (ou boucle de rattrapage) a permis d'identifier le dysfonctionnement, qui ne pouvait apparaitre que dans des cas très rares et dans des circonstances particulières.
Les circonstances d'apparition du problème rencontré à Ottignies sont exceptionnelles; cependant, dans tout système de sécurité ferroviaire, il est nécessaire d'apporter rapidement une correction à un dysfonctionnement identifié.
L'étude réalisée conjointement par Siemens et Infrabel a confirmé le besoin d'adapter la programmation côté EBP pour éviter que l'enclenchement ne doive traiter des commandes de sécurité imbriquées dans des commandes de tracé de route.
Cette programmation a été modifiée, testée et implémentée au niveau local et a été étendue à l'ensemble du réseau. La mesure prise par le gestionnaire d'infrastructure permet d'éviter une reproduction du problème identifié.

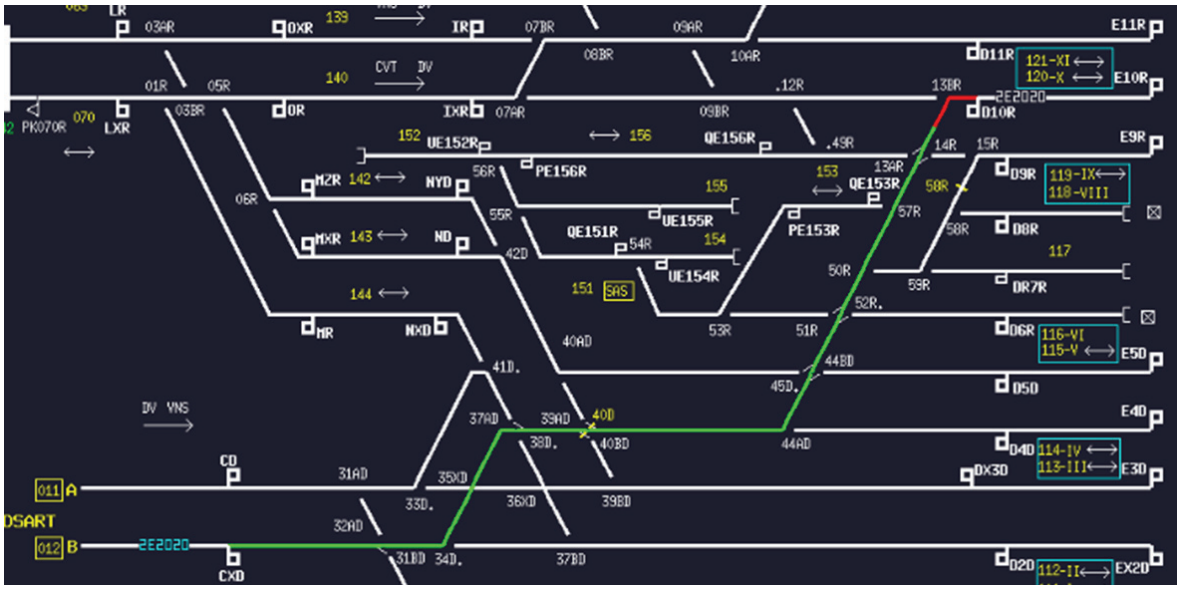
L'analyse de ces mesures, du système de gestion des incidents et du système de gestion des actions correctives conclut que l'incident a été géré de façon professionnelle, argumentée et reproductible et n'amène pas à de recommandation.

2. LES FAITS IMMEDIATS

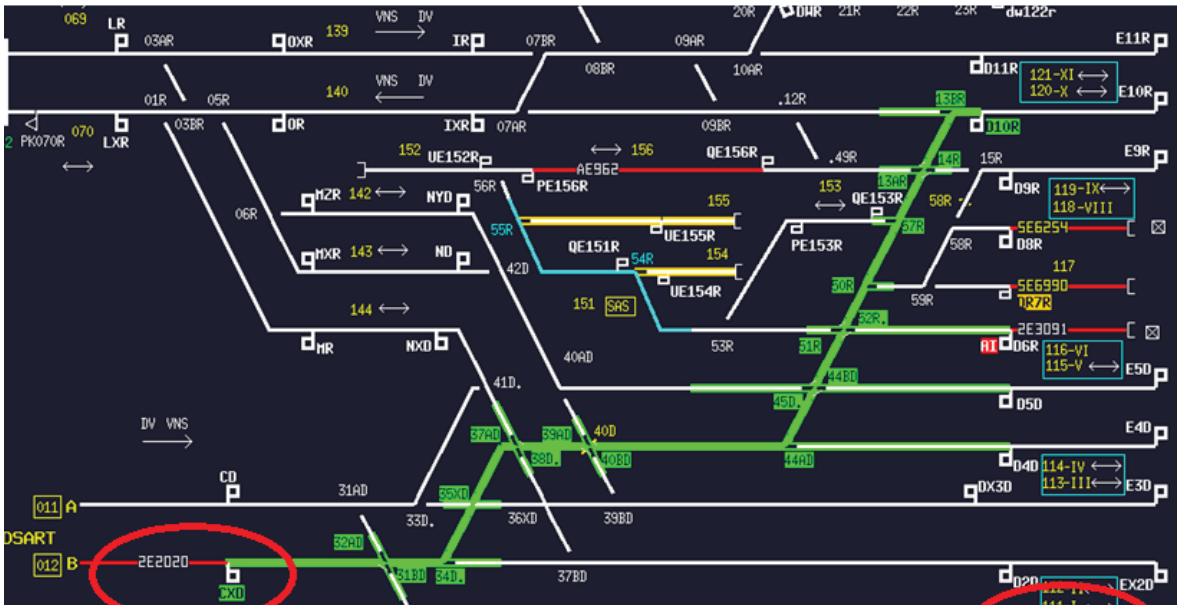
2.1. L'EVENEMENT

2.1.1. DESCRIPTION DE L'ÉVÉNEMENT

Le lundi 28/07/2014 vers 21h21, dans le gril de la gare d'Ottignies, le train E2020 circule du signal D10R.29 de la voie 120 vers la voie 012 selon un itinéraire tracé. Cet itinéraire traverse de multiples aiguillages dans la gare d'Ottignies.

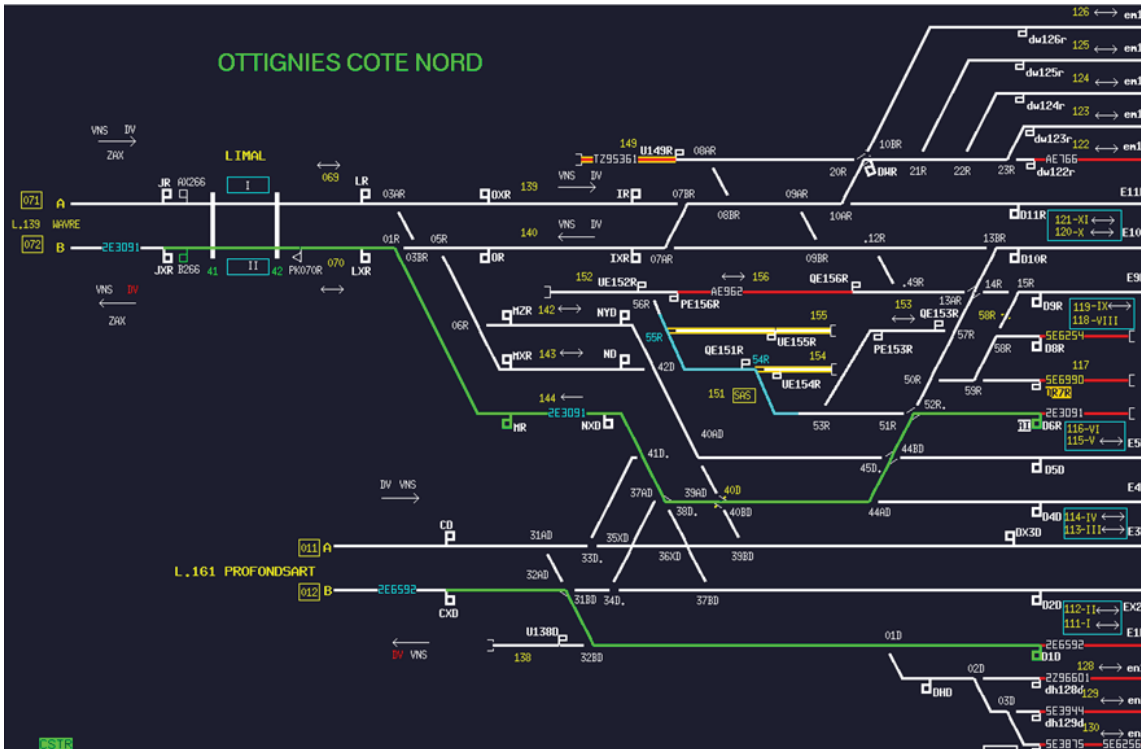


Un peu avant 21h22, alors que le train E2020 a fini de parcourir cet itinéraire et qu'il continue son parcours en sortant du gril d'Ottignies, l'opérateur du poste de signalisation EBP remarque que l'itinéraire entre le signal D10R.29 et le signal CXD.29 ne se libère pas.

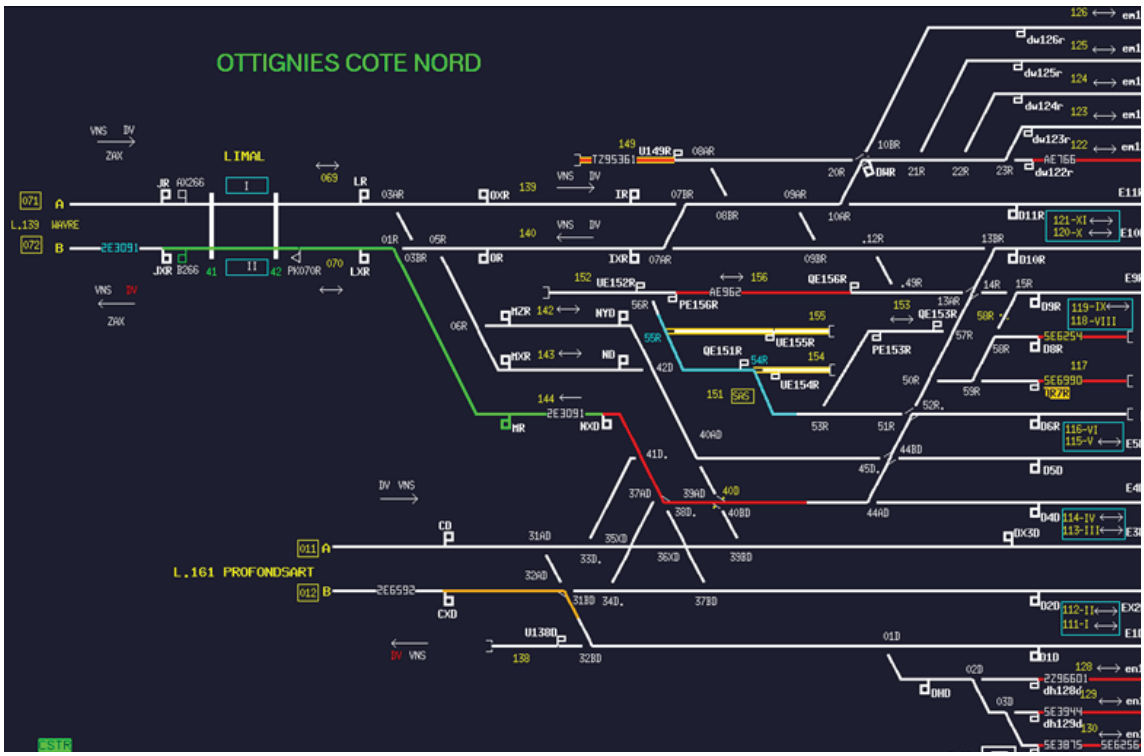


Vers 21h22'24", il applique une fonction de secours NT du système EBP afin de détruire cet itinéraire.

A 21h22'45", un itinéraire est tracé automatiquement par le système ARS (*Automatic Route Settings*[1]) pour un second train portant le numéro E6592 de la voie 111 vers la voie 012. Le train E6592 commence à parcourir cet itinéraire.



Alors qu'il en a parcouru une première partie, la seconde partie de son itinéraire est détruite. L'opérateur du poste de signalisation voit alors sur son écran une partie du tracé du train E6592 coloré de bistre, signalant ainsi une occupation sans enclenchement.



Sur le terrain, rien ne permet au conducteur de se rendre compte que la zone qu'il parcourt est une zone non enclenchée et il poursuit donc son trajet. Le train sort du gril d'Ottignies.

1 *ARS : cf. 2.2.2.1*

2.1.2. DÉCISION D'OUVERTURE D'ENQUÊTE

Conformément au paragraphe 1er de l'article 93 de la loi du 30 août 2013 portant le Code Ferroviaire, l'incident ne doit pas faire l'objet d'une notification immédiate à l'Organisme d'Enquête. Il a été rapporté à l'OE par l'envoi d'un compte-rendu d'incident conformément aux prescrits du paragraphe 3 de l'article 93 de la loi du 30 août 2013 portant le Code Ferroviaire.

L'incident a mis en lumière une défaillance dans la gestion de l'interface entre deux sous-systèmes de signalisation. L'ouverture de l'enquête par l'OE permet une analyse approfondie de l'incident, une vérification des mesures prises par le GI et d'éventuellement émettre des recommandations de sécurité.

2.1.3. COMPOSITION DE L'ÉQUIPE

Organisme d'appartenance	Rôle
Organisme d'Enquête	Enquêteur principal
Organisme d'Enquête	Enquêteurs
SSICF	Expertise technique et assistance documentaire
Infrabel	Expertise technique et assistance documentaire

2.1.4. CONDUITE DE L'ENQUÊTE

2.1.4.1. GÉNÉRAL

L'incident survenu le 28/07/2014 ne fait pas partie des événements pour lesquels l'OE doit recevoir une notification immédiate du GI (cf 2.1.2): l'enquêteur de l'OE ne s'est donc pas rendu sur place. C'est suite à la réception du compte-rendu de l'incident que l'OE a organisé une réunion d'échange avec Infrabel afin de recevoir du GI les premières informations et explications à propos de l'incident.

Des informations techniques complémentaires ont été demandées à Infrabel pour permettre à l'OE d'effectuer ses premières analyses. Diverses réunions avec le service technique d'Infrabel et avec le SSICF ont ensuite été organisées afin d'obtenir des explications et précisions complémentaires.

2.1.4.2. ETUDE DU SYSTÈME DE GESTION DE LA SÉCURITÉ

Un éclairage organisationnel et opérationnel est apporté à l'analyse de l'accident au travers de l'examen des extraits les plus significatifs du SGS du gestionnaire d'infrastructure Infrabel.

2.2. CIRCONSTANCES DE L'ÉVÉNEMENT

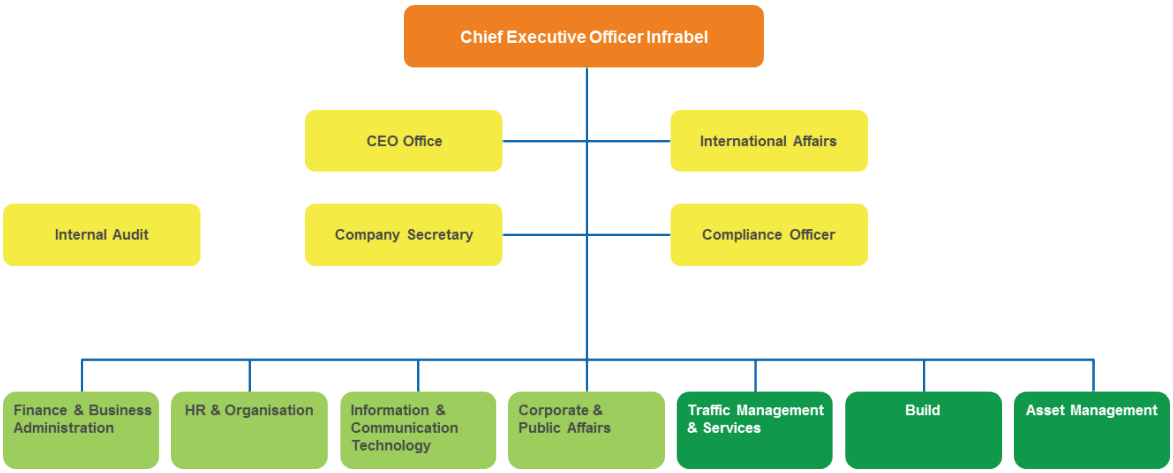
2.2.1. ENTREPRISE CONCERNÉE : INFRABEL

Suite à l'Arrêté Royal du 14 juin 2004, Infrabel est le gestionnaire d'infrastructure.
Le gestionnaire assure :

- l'acquisition, la construction, le renouvellement, l'entretien et la gestion de l'infrastructure;
- la gestion des systèmes de régulation et de sécurité de cette infrastructure;
- la fourniture aux entreprises ferroviaires de services relatifs à l'infrastructure ferroviaire;
- la répartition des capacités de l'infrastructure ferroviaire disponibles (horaires et sillons);
- la tarification, la facturation et la perception des redevances d'utilisation de l'infrastructure ferroviaire et des services.

Le gestionnaire de l'infrastructure doit veiller à l'application correcte des normes techniques et des règles afférentes à la sécurité de l'infrastructure ferroviaire et à son utilisation.

Suite à la réorganisation de ses services en 2014, l'organigramme d'Infrabel est le suivant :



Les départements concernés par cet incident sont :

- la direction Traffic Management & Services
  Cette direction assure la gestion opérationnelle quotidienne du trafic ferroviaire sur le réseau belge. La direction entretient également les contacts avec les clients d'Infrabel (entreprises ferroviaires, entreprises raccordées et clients industriels désireux de transporter leurs produits par voie ferroviaire) et gère la distribution et l'allocation de la capacité du réseau. Enfin, la direction Traffic Management & Services assure la sécurité et la ponctualité du trafic ferroviaire via le développement et l'amélioration continue du système de gestion de la sécurité et de la ponctualité.
- la direction Asset Management
  La direction Asset Management gère la maintenance et le renouvellement de l'infrastructure ferroviaire : voies, signaux, caténaires, sous stations de traction, etc. Elle réalise également des inspections sur le terrain, et gère également le support logistique et spécialisé.
- le service Information & Communication Technology
  ICT vient en support des directions et services d'Infrabel pour tout ce qui a trait à l'informatique et aux télécommunications.

2.2.2. DESCRIPTION DE L'INFRASTRUCTURE ET DU SYSTÈME DE SIGNALISATION

Le poste de signalisation d'Ottignies (Block 29) est équipé de la technologie EBP, en liaison avec un enclenchement à logique programmée (PLP).

Le poste de signalisation assure la gestion des circulations ferroviaires à 2 niveaux:
le niveau commande et le niveau d'enclenchement.
Le niveau commande (ou exploitation) reçoit les requêtes des opérateurs de signalisation et les transmet au niveau d'enclenchement qui traite ces requêtes en sécurité.

Le poste de signalisation gère le trafic ferroviaire à un niveau local, au sein de sa zone d'action. Concrètement, son rôle consiste, en sécurité, à placer les aiguillages dans la bonne position et à ouvrir les signaux devant les trains. C'est ainsi que le train est aiguillé vers les voies qu'il doit emprunter.

2.2.2.1. LE NIVEAU COMMANDE

Le poste EBP

Un "poste de commande électronique" EBP est un poste de signalisation dont l'ordre de commande des aiguillages, des routes, des signaux, etc. est donné par un opérateur et exécuté sous conditions et en sécurité par un ordinateur.

Une installation EBP fonctionne grâce à un logiciel générique EBP (logiciel développé et maintenu par Siemens), auquel est appliqué un fichier de configuration reprenant les spécificités des installations contrôlées par le poste de signalisation.

Le système EBP assure en outre:

- la gestion du service des trains;
- l'automatisation éventuelle du tracé de l'itinéraire, de l'enclenchement des routes et de l'ouverture du signal;
- le suivi de la circulation des trains et la distribution de ces données vers des systèmes périphériques (régulation (régionale), système de téléaffichage, etc.);
- le recueil d'informations et les commandes relatives aux installations techniques (chauffage des aiguillages, zones d'éclairage, d'alimentation, …);
- l'archivage des données relatives aux opérations de desserte, à la circulation et aux problèmes survenus.

Le tracé des itinéraires et la commande à l'ouverture des signaux sont réalisés par le traitement des lignes de mouvement gérées à l'écran au moyen du clavier de dialogue ou de la souris.
C'est également par ce biais qu'est commandée l'exécution de certaines fonctions de secours.
L'opérateur peut, en fonction des besoins, créer ou modifier la ligne de mouvement. Si elle correspond au trajet à effectuer, l'utilisateur procède à l'acquittement, et la ligne de mouvement apparaîtra :

- dans la zone de commande de son écran de dialogue;
- dans la zone d'édition de l'écran de dialogue des autres utilisateurs impliqués dans l'exécution du mouvement.

Les routes peuvent être tracées et les signaux commandés à l'ouverture (automatiquement ou manuellement). Toutes les modifications apportées aux lignes de mouvement par l'utilisateur (par ex. édition, commande de signal, etc.) ou par le mouvement lui-même (par ex. fermeture automatique des signaux, libération des routes, etc.) sont enregistrées dans le Logbook ou livre de bord.

Une fois l'itinéraire tracé et les signaux commandés à l'ouverture, le train parcourt le tracé. Au fur et à mesure de l'avancement du mouvement et de la libération des routes, les points de trajet impliqués dans l'itinéraire sont supprimés de la ligne de mouvement.

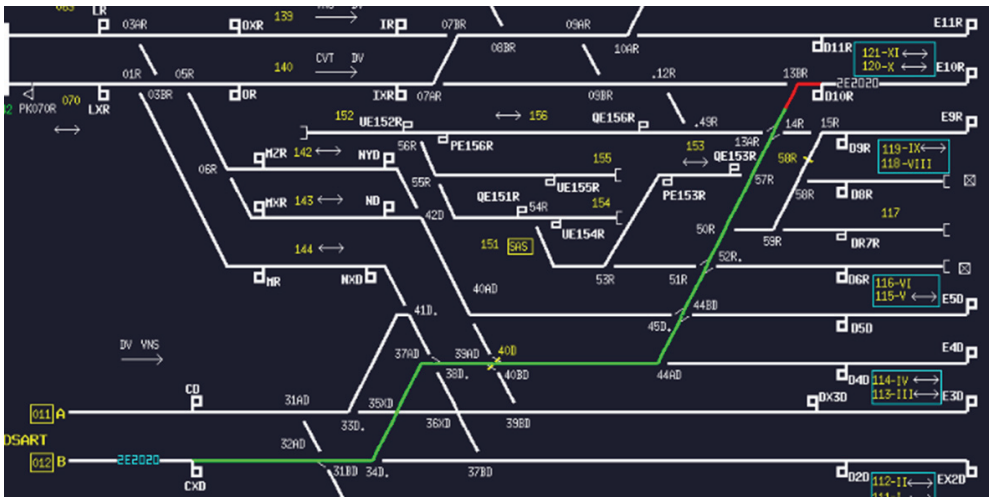


Illustration : vue (partielle) de l'image EBP du gril d'Ottignies avec le train E2020 parcourant l'itinéraire depuis le signal D10-R.29 vers la voie 012. La partie de l'itinéraire enclenché est colorée en vert, et la/les section(s) de voie occupée(s) par le train est/sont colorée(s) de rouge.

Lorsque le système EBP détecte l'entrée d'un mouvement (ou train) dans la zone qu'il gère, et que ce mouvement est prévu au programme du service des trains, le système EBP peut réaliser automatiquement le tracé et/ou l'ouverture du signal. Ils seront initiés par le mouvement lui-même, lors de l'occupation de la zone d'approche du signal qui couvre l'itinéraire. Cet automatisme de la commande de route et de la commande à l'ouverture des signaux est nommé *Automatic Route Setting* (ARS).

Le personnel au poste EBP

Le système EBP est réglé de manière telle que certaines commandes sont inaccessibles ou soumises à des restrictions pour certains utilisateurs. Les utilisateurs EBP se distinguent par leur compétence et leur responsabilité :

- une compétence donne le droit à un utilisateur de faire quelque chose : pour pouvoir exécuter une tâche donnée, l'utilisateur devra disposer de la compétence requise.
- une responsabilité impose à un utilisateur une certaine obligation pour (une partie de) la zone EBP

Compétence	L'utilisateur est autorisé à exécuter…
Desservant	des commandes et fonctions normales et auxiliaires qui ne mettent pas en danger la sécurité.
Surveillant	des commandes et fonctions normales, de secours et auxiliaires qui peuvent mettre en danger la sécurité.
ELM	des fonctions auxiliaires nécessaires à la maintenance (compétence et responsabilité ELM).
Répartiteur ES	des fonctions auxiliaires qui exigent une compétence de répartiteur ES.

Catégories	Description
Observateur	Un observateur n'a aucune responsabilité. Il ne peut que vérifier ce qui se passe dans la zone EBP concernée (par exemple : suivre le déroulement des mouvements).
Desservant	Cette responsabilité n'est confiée qu'à un seul et unique utilisateur par zone de base. Il est responsable de la commande des installations de signalisation, à l'exception des fonctions de secours, à l'intérieur des zones de base en question.
Surveillant	Cette responsabilité n'est confiée qu'à un seul et unique utilisateur par zone de base. Il peut être responsable de la commande des installations de signalisation, y compris des fonctions de secours Les fonctions lancées sur l'initiative du système EBP lui-même ou par des utilisateurs ne disposant pas de la compétence requise, sont transmises à l'utilisateur qui détient un droit de surveillance sur la zone de base concernée.
Opérateur	Cet utilisateur a, en principe, tant une obligation de surveillance que de desserte dans une zone de base.
Régulateur	Cet utilisateur est chargé : - de réguler la circulation dans l'ensemble de la zone EBP ; - de traiter les messages généraux générés par le système EBP Cette compétence n'incombe qu'à un seul utilisateur par zone EBP.
Chef de gare (adj)	Cet utilisateur détient les mêmes compétences qu'un opérateur, mais est en outre chargé de la gestion des utilisateurs du poste EBP concerné.
Opérateur elm	Cette catégorie de commande est réservée aux agents des services I-signalisation. Ces utilisateurs sont compétents pour : - la commande des installations de signalisation, y compris des fonctions de secours, - certaines fonctions, propres aux services I-signalisation.

Du point de vue de l'organisation du poste de signalisation, le rôle du régulateur est étendu :

- il assure la direction du service;
- il assure la régulation du trafic dans l'ensemble de la zone d'action du poste, notamment la surveillance des circulations, des mises à quai et des correspondances, les dérogations à l'affectation des voies, ...
- il fait rappeler le personnel en cas de nécessité;
- il instruit les irrégularités;
- il est responsable de la tenue des documents présents au poste;
- il assiste les surveillants dans l'application des mesures de sécurité en cas de travaux, dérangements, incidents ou accidents multiples;
- il répartit les tâches en cas d'absence momentanée d'un agent;
- il est responsable de la justification (ARTWEB) des retards.

2.2.2.2. LE NIVEAU "ENCLENCHEMENT"

Un enclenchement ferroviaire est un ensemble d'appareillages de signalisation qui matérialise physiquement une incompatibilité de manœuvre entre différents organes de commande d'appareils de voie ou de signaux dans le but de n'autoriser le passage d'un mouvement que lorsque toutes les conditions de sécurité nécessaires à celui-ci sont réunies.
Ces conditions, bien que particularisées pour chaque installation, découlent des principes généraux de signalisation et dépendent des qualités et principes de fonctionnement propres des équipements.

L'enclenchement assure ainsi un itinéraire sécurisé et évite tout risque de conflit entre les trajets des trains.

Historiquement, le secteur ferroviaire a utilisé successivement:

- les enclenchements mécaniques : les incompatibilités étaient matérialisées par des jeux de barres reliant les leviers de commandes des aiguillages et des sémaphores de signalisation;
- les enclenchements électriques : les relais sont reliés entre eux par des circuits électriques dont la logique permet de réaliser les conditions de sécurité par l'alimentation ou non des relais de commandes des signaux et des appareils de voie;
- les enclenchements électroniques/informatiques (PLP) où les règles de sécurités sont programmées et où les incompatibilités de manœuvre sont reprises via des flags d'état.

Illustration d'un SmartLock

Les enclenchements électroniques utilisés par Infrabel sont de 2 types :

- les premiers installés furent les enclenchements Solid State Interlocking (SSI) en 1993;
- depuis 2006, de nouveaux enclenchements issus des évolutions technologiques sont utilisés, les SmartLock 400.

Les installations de la gare d'Ottignies utilisent un enclenchement de type SmartLock 400.

3. COMPTE RENDU DES INVESTIGATIONS ET ENQUÊTES

3.1. RÉSUMÉ DES TÉMOIGNAGES

Des interviews et prises d'informations réalisées au cours de l'enquête, il apparait que :

- l'anomalie apparue à Ottignies lors de la circulation du train E6592 le 28 juillet 2014 n'a pas eu de conséquence sur la circulation du train;
- cette anomalie a été analysée par Infrabel;
- le résultat de cette analyse a entraîné le remplissage d'une fiche eBugp;
- la solution à ce dysfonctionnement a été développée, testée et contrôlée par Siemens et Infrabel.

3.2. SYSTÈME DE GESTION DE LA SÉCURITÉ D'INFRABEL

La Directive 2004/49/CE sur la sécurité d'exploitation prescrit que tout gestionnaire d'infrastructure et toute entreprise ferroviaire doivent établir un Système de Gestion de la Sécurité (SGS) garantissant la maîtrise de tous les risques créés par leurs activités.

Selon la Directive sécurité 2004/49/CE, les procédures et les méthodes d'évaluation et de maitrise des risques sont considérées comme un élément de base du Système de Gestion de la Sécurité.
La Directive 2004/49/CE sur la sécurité ferroviaire stipule qu'il appartient au gestionnaire de l'infrastructure (et aux entreprises ferroviaires) d'élaborer des procédures et des méthodes en vue de l'exécution d'évaluations de risques et de l'implémentation de mesures de contrôle des risques à chaque changement dans les conditions d'exploitation ou en présence de matériel nouveau présentant de nouveaux risques pour l'infrastructure ou l'exploitation.

Pour faciliter la reconnaissance mutuelle entre États membres, les méthodes d'identification et de gestion des risques qu'utilisent les acteurs participant au développement et à l'exploitation du système ferroviaire, ainsi que les méthodes permettant de démontrer que le système ferroviaire situé sur le territoire de la Communauté est conforme aux exigences de sécurité, ont été harmonisées: les méthodes sont adoptées dans le Règlement 352/2009 de la Commission.

Le Règlement (CE) 352/2009 de la Commission du 24 avril 2009 établit une méthode de sécurité commune (MSC) relative à l'évaluation et à l'appréciation des risques visée à l'article 6, paragraphe 3, point a), de la directive 2004/49/CE.
La MSC relative à l'évaluation et à l'appréciation des risques a pour objet de maintenir ou, lorsque cela est nécessaire et raisonnablement réalisable, d'améliorer le niveau de sécurité des chemins de fer de la Communauté.
La MSC a également pour but de faciliter l'accès au marché des services de transport ferroviaire par l'harmonisation:

- des processus de gestion des risques utilisés pour évaluer les niveaux de sécurité et la conformité avec les exigences de sécurité;
- de l'échange d'informations relatives à la sécurité entre les différents acteurs du secteur ferroviaire afin de gérer la sécurité entre les différentes interfaces qui existent dans ce secteur;
- des preuves résultant de l'application du processus de gestion des risques.

3.2.1. CHANGE MANAGEMENT – ANALYSE DE RISQUE

Un processus de gestion du changement a été mis en place au sein du SGS d'Infrabel. Il permet :

- de contrôler des changements (dans les projets existants et de nouveaux projets) en identifiant les risques potentiels, et
- de définir des mesures de contrôle appropriées avant la mise en œuvre d'un changement.

Lorsqu'un changement important avec un impact sur la sécurité du trafic ferroviaire se présente, et si cela se révèle nécessaire, Infrabel :

- homologue les installations concernées ou le matériel concerné;
- adapte son système de gestion de la sécurité;
- présente une demande de révision de son agrément de sécurité.

De plus, une évaluation de risque est réalisé à chaque fois qu'Infrabel présente un changement important avec un impact sur la sécurité du trafic ferroviaire qui n'est pas prévu dans son agrément de sécurité.

Lors de l'introduction du nouveau système d'enclenchement (SmartLock 400) dans les installations en remplacement des enclenchements de type SSI, le processus prévu a été suivi et respecté. Les analyses menées dans le cadre de la gestion du changement n'ont pas mis en évidence l'existence d'un problème potentiel suite à l'introduction d'un nouveau protocole d'interface entre ces deux sous-systèmes de signalisation.
L'EBP communique avec le SmartLock 400 selon un protocole qui permet l'envoi de commandes normales et de secours de manière concomitante, tandis que l'enclenchement Solid State Interlocking utilise un protocole qui n'autorise pas de commande normale tant que les commandes de secours n'ont pas toutes été effectuées.
Cette différence est, entre autres, à l'origine de l'anomalie observée.

3.2.2. GESTION DES COMPÉTENCES

Le système de gestion des compétences est établi afin de garantir, dans la mesure du possible, que les employés soient conscients :

- de la pertinence et de l'importance de leurs activités et
- de la façon dont ils contribuent à la réalisation des objectifs de sécurité.

Les formations fondamentales et permanentes existent pour les fonctions de sécurité au sein du gestionnaire d'infrastructure, d'une part en fonction des règles reprises dans les "conditions particulières d'accès aux emplois" (RGPS fascicule 501 – Titre III – Partie III), et d'autre part en fonction des règles spécifiques en vigueur à la Direction Traffic Management & Services (auparavant Direction Réseau).
Les plans d'enseignement sont adaptés immédiatement en cas réglementation modifiée ou de parution de nouvelles instructions mais également lors d'introduction de nouveaux produits dans le secteur ferroviaire.

Chaque formation fondamentale fait l'objet d'un plan de formation spécifique approuvé.
Les procédures désignent :

- les responsables de la formation et des recyclages du personnel exerçant des fonctions de sécurité,
- les conditions d'admission, d'aptitudes médicales,
- le système pédagogique
- la formation permanente du personnel de sécurité.

3.2.3. RAPPORTAGE D'INCIDENT – ANALYSE - APPRENTISSAGE

L'existence d'un outil de rapportage d'incidents est essentielle au sein d'une organisation :

- elle permet le bon déroulement du processus "identification, analyse et correction" des opérations effectuées;
- elle constitue un indicateur tant de l'implication du personnel dans la sécurité que de la sécurité de ses opérations.

Le rapportage d'incidents revêt plusieurs formes au sein d'Infrabel : à côté des enquêtes réalisées après un accident, chaque membre du personnel peut réaliser un feedback sur les risques rencontrés lors de l'exploitation du système ferroviaire.
Il s'agit d'une collecte (compilation d'événements, de mentions, de faits relatifs aux événements), d'une analyse, de l'enregistrement (classement et conservation) et du traitement des informations relatives aux faits et risques rencontrés.
Ce feedback permet aux responsables de disposer d'informations utiles à l'évaluation du système de sécurité, à l'identification des points fragiles (qu'ils soient liés à la dimension humaine, technique , organisationnelle ou environnementale), à la détection des problèmes de cohérence et à la proposition d'améliorations.

L'incident survenu à Ottignies s'est manifesté par l'apparition à l'écran d'un DOBMI (Detectie/ Détection Ontijdige Beweging Mouvement Intempestif). Ces DOBMI sont enregistrés dans le logbook EBP et, selon les procédures mises en place chez Infrabel, ces enregistrements font régulièrement l'objet d'une recherche et d'une analyse.
L'analyse des DOBMI enregistrés permet d'en dégager la cause :

- un SPAD[2],
- une défaillance d'un organe de détection dans la voie,
- …

Un feedback est donné par le Chef de Surveillance Générale aux agents concernés pour d'éventuelles actions correctrices. L'analyse du DOBMI survenu à Ottignies a permis d'identifier le problème et de l'analyser en profondeur. Les actions correctrices appropriées ont été rapidement enclenchées.

3.2.4. COMMUNICATION

Les processus de communication en place au sein de l'organisation permettent au SGS de fonctionner efficacement. L'échange structuré d'informations pertinentes sur la sécurité est essentiel, tant au sein de l'organisation elle-même, qu'avec des sociétés externes, notamment les fournisseurs et sous-contractants, avec qui une communication n'est efficace que si elle a lieu dans les deux sens.
Le feedback du personnel d'exploitation est crucial lors des tests et contrôles des équipements et services fournis.

L'analyse et la résolution de l'incident d'Ottignies a nécessité des échanges entre Infrabel et Siemens, fournisseur du système EBP, système sur lequel des modifications de programmation se sont avérées nécessaires.
Les échanges entre les deux parties sont structurés de façon à rendre la communication entre les parties efficace et sécurisée : chaque personne impliquée a un rôle bien déterminé et fait partie d'un board créé pour la résolution du problème rencontré.
C'est ce board qui a déterminé la faisabilité des potentielles solutions : leur analyse a permis le choix de la solution la plus adaptée et d'en planifier le développement et le déploiement. Les communications et décisions de ce board sont enregistrées dans un outil informatisé de suivi (eBugp). La traçabilité des communications est importante car elle fait partie des éléments évalués dans le cadre du SGS.

2 *SPAD = Signal Passed At Danger = Signal franchi alors qu'il est fermé*

3.2.5. ORGANISATION DU TRAVAIL

Le SGS demande à ce qu'il y ait une description claire et sans ambiguïté de la structure organisationnelle de l'entreprise, ainsi que des tâches nécessaires.
Une répartition adéquate des tâches en facilite la conformité et permet d'éviter une sous-charge de travail, du stress et / ou un niveau de vigilance diminuée, autant de facteurs potentiellement réducteurs de sécurité.

En outre, la bonne structuration du travail avec des parties externes permet à Infrabel de s'assurer:

- de la participation adéquate de chaque partie, et
- de la capacité d'agir rapidement ou de réagir dans tout type de situations, normales ou dégradées.

Tant du côté de Siemens que du côté d'Infrabel, chaque personne impliquée dans la résolution du problème a un rôle bien déterminé, fonction de ses compétences. Au sein du board créé, les tâches sont assignées. Cette structuration permet le développement de la solution sans interférence, tout en optimalisant son contrôle et sa sécurisation. Elle permet également aux décideurs de conserver une vue complète du projet et au management d'Infrabel de s'assurer de la conformité de ces règles au SGS.

3.2.6. CONTRÔLE DES FOURNISSEURS

Lorsque le gestionnaire d'infrastructure s'appuie, pour ses activités, sur les prestations de fournisseurs et de sous-contractants, il doit contrôler qu'ils délivrent leurs services et livraisons en toute sécurité.

L'analyse de l'incident par Infrabel débouche, après des échanges avec Siemens, sur la programmation par Siemens de modifications de l'EBP. Celles-ci, après avoir été vérifiées par Siemens lui-même, ont été contrôlées par Infrabel.
Les tests sont réalisés par des équipes différentes de celles qui analysent le problème initial : le résultat est un contrôle indépendant. Les tests sont réalisés par Infrabel sur ses propres installations dans 2 environnements différents de simulation et de test. Ceci permet à Infrabel de s'assurer de la conformité des adaptations aux requis et de vérifier l'absence de bug de programmation.
Une fois testé, le programme EBP adapté est installé sur une zone EBP particulière où il n'y a aucun trafic de trains de voyageurs : ceci permet de valider le fonctionnement en situation réelle. Le déploiement sur tous les sites EBP est ensuite seulement réalisé.

3.3. RÈGLES ET RÉGLEMENTATION

3.3.1. RÈGLES ET RÉGLEMENTATION PUBLIQUE COMMUNAUTAIRE ET NATIONALE APPLICABLES

3.3.1.1. ARRÊTÉ ROYAL DU 09/07/2013 DÉTERMINANT LES EXIGENCES APPLICABLES AU PERSONNEL DE SÉCURITÉ

Divers articles de cet AR précisent les exigences applicables à l'ensemble du personnel de sécurité.
Les annexes de cet AR listent, fonction par fonction, les compétences à acquérir par le personnel de sécurité.
Plus particulièrement, l'annexe N3 en son point 2.18.a reprend la liste des connaissances particulières à l'exécution de la fonction de sécurité "agent du mouvement affecté à un poste de signalisation".

3.3.2. AUTRES RÈGLES, TELLES QUE LES RÈGLES D'EXPLOITATION, LES INSTRUCTIONS LOCALES, LES EXIGENCES APPLICABLES AU PERSONNEL, LES PRESCRIPTIONS D'ENTRETIEN ET LES NORMES APPLICABLES

3.3.2.1. INSTRUCTION LOCALE DU BLOCK 29 (OTTIGNIES)

ANNEXE 1 : FICHE DE CONSTATATION DES DÉRANGEMENTS
Lorsqu'un utilisateur EBP constate une anomalie sans que cela ne soit causé par une avarie, il complète un exemplaire du document en complétant les 3 premières lignes et la rubrique : Rapport de la constatation/irrégularité.
Ce document est ensuite transmis au Bureau de la Surveillance Générale de la GRI-R (et uniquement à ce bureau) pour analyse et envoi vers IR 011.
Cette fiche peut être aussi bien être complétée à la main que de manière informatique.

3.4. FONCTIONNEMENT DES INSTALLATIONS TECHNIQUES

3.4.1. GÉNÉRALITÉS SUR LA CIRCULATION D'UN TRAIN

Pour qu'un train puisse circuler depuis le départ jusqu'au terminus, son trajet doit avoir été fixé c'est le rôle des postes de signalisation en concertation avec Traffic Control, et en fonction des horaires.

Le poste de signalisation assure la gestion de 2 niveaux fonctionnels : le niveau commande et le niveau d'enclenchement. Le niveau commande (ou exploitation) reçoit les requêtes des opérateurs de signalisation et les transmet au niveau d'enclenchement qui traite ces requêtes en sécurité.

Le poste de signalisation gère le trafic ferroviaire à un niveau local, au sein de sa zone d'action. Concrètement, son rôle consiste à placer les aiguillages dans la bonne position et à régler les signaux correctement. C'est ainsi que le train est aiguillé vers les voies qu'il doit emprunter.

3.4.2. NOTIONS ET DÉFINITIONS

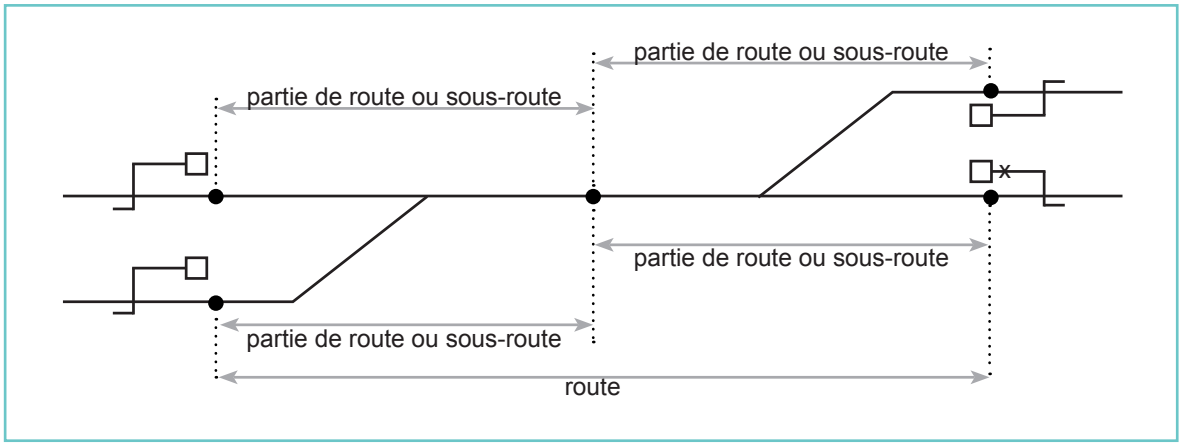
3.4.2.1. TRAJET - ITINÉRAIRE - ROUTE

L'itinéraire est constitué d'un ensemble de routes et de sous-routes et comprend en principe un ou plusieurs appareils de voie. Il permet la circulation d'un mouvement entre un signal d'arrêt desservi et le signal d'arrêt desservi le protégeant pour les mouvements dans l'autre sens.

Une route est une partie de l'itinéraire comprise entre deux points de libération et qui comprend des appareils de voie. Un tracé de route et une commande à l'ouverture d'un signal ne seront exécutés que si l'identification du mouvement est le premier mouvement devant le signal.

Un point de route permet de choisir sans ambiguïté des routes différentes qui permettent de parcourir un des itinéraires différents entre les mêmes point de départ et de destination d'un gril. Ils apparaissent dans la ligne de mouvement.

Une partie de route est une portion de la route qui peut être libérée séparément par le mouvement.



Le trajet est l'ensemble des itinéraires et des sections de block que va parcourir un train dans la zone EBP concernée. Il correspond à l'ensemble de la ligne de mouvement.

Lorsqu'un mouvement parcourt un itinéraire, divers éléments permettent au système de détecter le train :

- le contrôle voie libre : effectué soit par des circuits de voie (CV) soit par des détecteurs d'essieux (CAT) placés dans la voie,
- l'enregistrement du passage d'un véhicule à un certain point de la voie : il est réalisé par les pédales. Les pédales sont caractérisées par une référence au signal, à l'appareil de voie ou au passage à niveau situé à proximité.

Dans un enclenchement, un aiguillage est immobilisé lorsqu'une commande de tracé empruntant cet aiguillage est actionnée. Cette immobilisation dure jusqu'à la libération de l'itinéraire / la zone d'immobilisation. L'immobilisation rend non seulement la manœuvre de cet aiguillage impossible, mais elle neutralise également l'établissement de tout autre tracé incompatible.

3.4.2.2. LIBÉRATION NORMALE D'UNE ROUTE

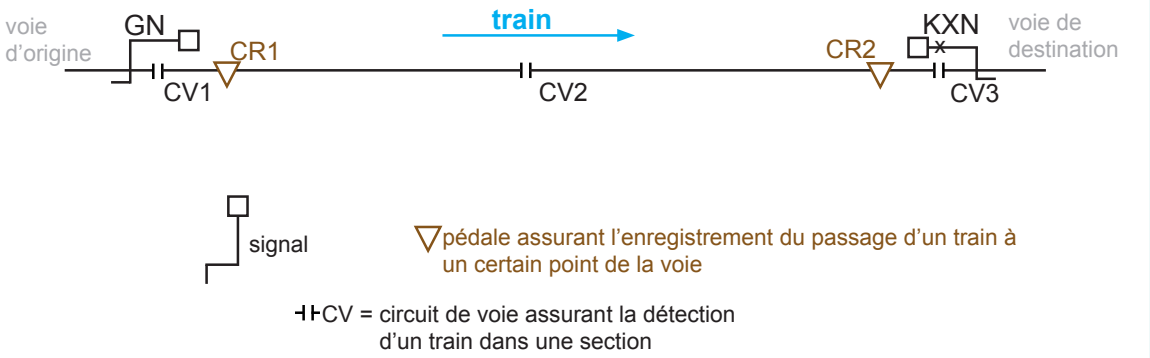
La logique de libération normale se trouve dans l'enclenchement PLP, l'EBP n'intervenant pas dans ce processus.
Pour qu'une route soit libérée, il faut que les 4 conditions suivantes soient remplies :

- que le (les) CV de la route soit (soient) libre(s)
- que le KFS[3] soit réobtenu au signal (aux signaux) ayant été commandé(s) à l'ouverture
- qu'il n'y ait pas de CIR[4] dans la ligne de mouvement
- qu'un fonctionnement régulier des points de libération ait été observé
- qu'il y ait eu un séquencement normal des conditions entre elles.

Un itinéraire composé de plusieurs routes est libéré selon une séquence d'étapes successives de libération de chaque fraction des routes/sous-routes concernées : il existe un chaînage entre les routes/sous-routes, de sorte qu'une route ne pourra être libérée que si la fraction qui la précède a été libérée elle-même.
Il en est de même pour une route composée de plusieurs sous-routes.

3 KFS = Contrôle signal fermé
4 CIR = Commande d'Immobilisation de Route

3.4.2.3. PARCOURS THÉORIQUE D'UN TRAIN



En fonctionnement normal, l'itinéraire d'un train entre la voie d'origine et la voie de destination se déroule de la façon suivante (l'exemple considère qu'il n'y a pas de libération intermédiaire entre GN et KXN):

- le signal GN est mis au passage
  Au niveau de l'écran EBP, le numéro du train apparait en bleu sur la voie de destination.
- la tête du train franchit le signal GN
- la tête du train occupe le premier CV (CV1), ce qui entraîne le passage au rouge du signal GN.
  Au niveau de l'écran EBP, ce tronçon passe au rouge et le symbole du signal GN devient blanc.
- la tête du train foule la pédale CR1.
  Au niveau de l'écran EBP, le numéro du train disparaît de la voie d'origine et le numéro du train apparaît en blanc sur la voie de destination.
- la tête du train occupe le deuxième CV (CV2).
  Au niveau de l'image EBP, ce tronçon passe au rouge.
- la tête du train foule la pédale CR2.
- la tête du train occupe le troisième CV (CV3).
  Au niveau de l'image EBP, le tronçon passe au rouge.
- la queue du train dépasse le CV1.
- la queue du train n'occupe plus le CV1.
  Au niveau de l'écran EBP, le tronçon passe de rouge à vert.
- la queue du train n'occupe plus le CV2.
  Au niveau de l'écran EBP, le tronçon passe de rouge à vert.

L'enclenchement vérifie les 4 conditions de libération de la route :

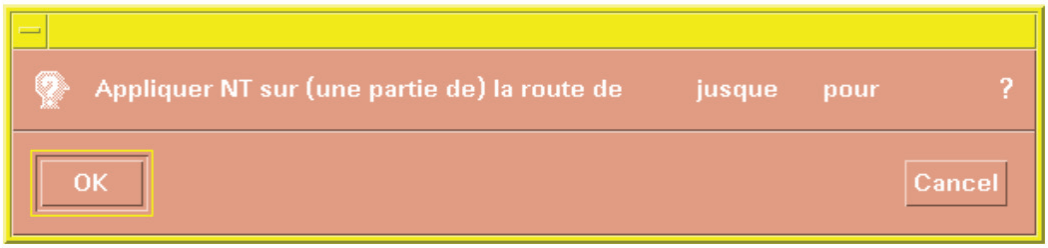
- les CV1 et CV2 ont été occupés et sont libres
- les pédales CR1 et CR2 ont été foulées et libérées par le train
- il n'y a pas de CIR
- le KFS du signal (des signaux) de la route a été obtenu

Si les 4 conditions sont vérifiées au final et si le séquencement s'est déroulé normalement, l'enclenchement libère la route et l'affichage des tronçons sur l'écran EBP passe de la couleur verte à la couleur blanche.

3.4.2.4. LIBÉRATION D'UN ITINÉRAIRE PAR UTILISATION D'UNE CLEF DE SECOURS: THÉORIE

Si et seulement si la libération automatique n'a pas été obtenue, l'opérateur EBP a alors la possibilité de démarrer une fonction NT[5], finalisée par le surveillant. Elle a pour objectif d'envoyer les commandes de sécurité qui vont libérer les zones d'immobilisation de l'itinéraire via des commandes de secours NIR[6].

La fonction NT peut être lancée par un utilisateur ayant la compétence de desservant au départ d'une ligne de mouvement si un utilisateur ayant une compétence de surveillant est loggé sur l'un des postes de travail de la zone EBP. La fonction NT ne peut seulement être exécutée que par un utilisateur ayant une compétence de surveillant.



Exemple de boîte de dialogue présentée à l'écran pour confirmation de la fonction NT

Préalablement à l'envoi des commandes NIR, des commandes SDG[7] de remise à l'arrêt des signaux encadrant l'itinéraire sont envoyées. Le but est de s'assurer qu'aucun mouvement de train ne pourrait se retrouver sur l'itinéraire à annuler.

Le système EBP présente ensuite au surveillant une série de questions qui permettent de confirmer l'application de la commande de secours.

```
NT_D10R_212158
NT D10R pt 2

Etes-vous certain que le mouvement <2E2020> se trouve en amont du signal  et qu'il ne franchira pas ce signal ?
*Yes =
*No  = n
*J'attends confirmation; sinon NT se poursuivra à 21:37.
Answer is D10R
Controler les éléments surlignés en vert et/ou mauve sur la fenetre de detail!
Voulez vous appliquer la fonction NT sur la route surlignée en vert et/ou mauve? (Yes =  / No = n)
Answer is CXD
Sur base de quelle information etes vous certain que le mouvement <2E2020> se trouve en amont du signal  et ne va pas dépasser ce signa
1. Confirmation du conducteur
2. Confirmation par un agent de mouvement
3. Vous avez attendu 15 min. depuis la fermeture du signal
4. Confirmation par un autre agent ayant les compétences
5. Je voudrais interrompre la fonction NT
Faites votre choix:
Answer is 2
```

Exemple de type d'écran présenté au surveillant

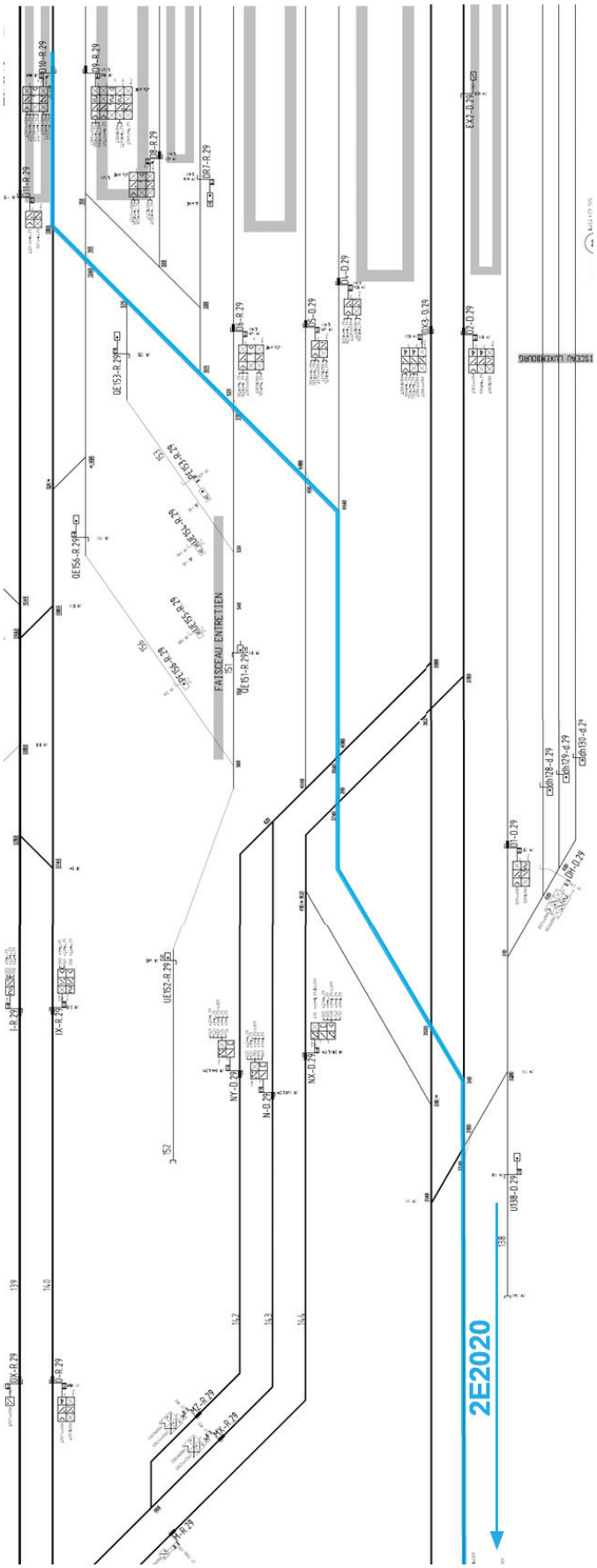
Une fois confirmée par les réponses du surveillant, deux systèmes distincts, l'AFS (*Auxiliary Function System*) et le SAFS (*Safety Auxiliary Function System*), vont lister l'ensemble des commandes NIR à appliquer pour libérer la route. En utilisant ces 2 systèmes pourvus d'une logique différente, une redondance sécuritaire est obtenue et c'est seulement si les résultats de ces deux systèmes concordent que les commandes NIR sont envoyées une à une à l'enclenchement.

En tant que commande de sécurité, une commande NIR s'effectue en deux temps :

- la préparation : l'enclenchement reçoit la commande de la part de l'EBP et il lui répond par une demande de confirmation sur la fraction à libérer;
- la confirmation : l'EBP envoie la confirmation et la fraction est alors libérée.

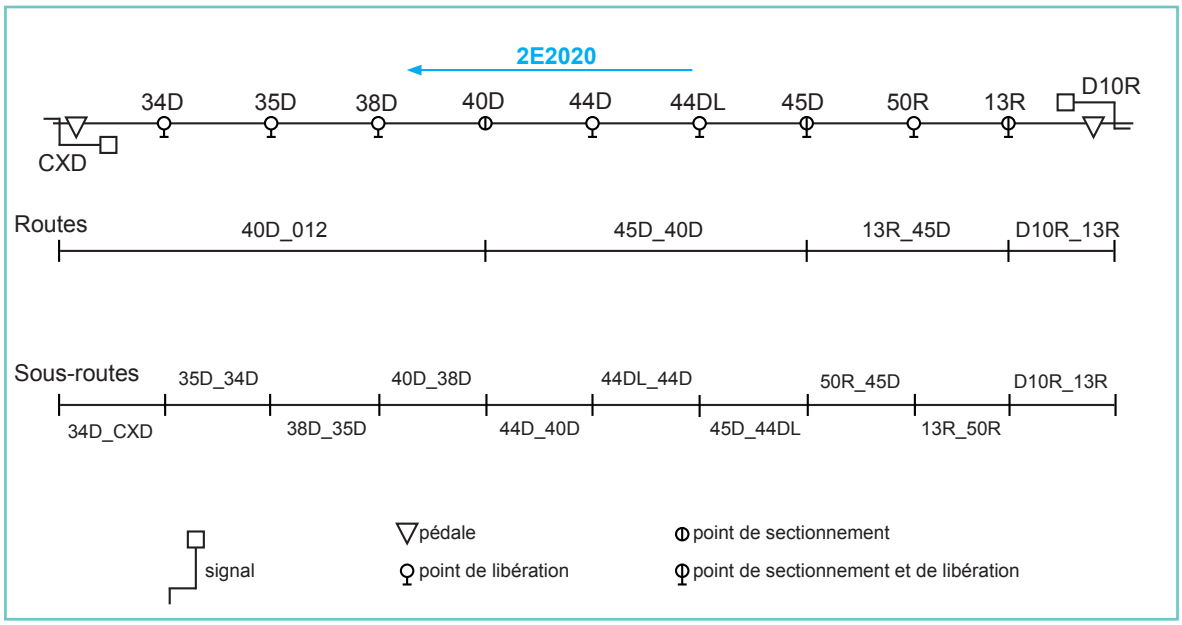
5 *NT = Nietiging Traject / aNnulation Trajet = fonction de secours EBP pour l'annulation d'une route*
6 *NIR = Nietiging Inklinging Reisweg / aNnulation Immobilisation de Route = commande de secours permettant de forcer la libération de la route lorsque celle-ci n'a pas été obtenue automatiquement.*
7 *SDG = fonction de fermeture d'urgence d'un signal*

3.4.3. PARCOURS DU TRAIN 2E2020 LE JOUR DE L'INCIDENT



Le jour de l'incident, le point de départ du parcours du train 2E2020 dans les installations de la gare d'Ottignies est le signal D10-R.29 (aussi nommé D10R ci-après) et le train quittait la gare par la voie 012 (sur laquelle se trouve le signal CX-D.29, aussi nommé CXD ci-après).

La figure ci-dessous représente les éléments intervenant dans l'itinéraire D10R-012 :
les 4 routes, les 10 sous-routes et les 8 points de fractionnement.



Lorsqu'il parcourt l'itinéraire entre le signal D10-R.29 et la sortie de la gare d'Ottignies (voie 012, matérialisée sur l'itinéraire du train par la pédale du signal CX-D.29), le train 2E2020 emprunte successivement 10 sous-routes.

C'est lors du parcours de la première sous-route D10R_13R qu'un problème dû à la pédale associée au signal D10R est survenu : celle-ci a transmis l'information sur son changement d'état avec un léger retard (de l'ordre de la centaine de millisecondes).
Dès lors, lorsque le train a eu terminé de parcourir cette sous-route, les 4 conditions de libération de la sous-route n'étaient pas vérifiées pour que l'enclenchement libère la sous-route D10R_13R.
Les sous-routes 2 à 9 (sous-routes 13R_50R →35D_34D) ne comportent pas de pédale, ce qui rend les conditions de libération légèrement différentes :

- tous les CV de la sous-route doivent être libres
- la sous-route d'amont doit être libérée (chaînage)
- le premier CV de la sous-route suivante doit être occupé

Du fait de son chaînage avec la première sous-route qui n'avait pas été libérée, la deuxième route (13R_50R) n'a pas été libérée lorsque le train parcourait l'itinéraire. De même pour le chaînage de la troisième sous-route avec la deuxième et ainsi de suite jusqu'à la neuvième sous-route.

La dixième sous-route comporte une pédale : les 4 conditions de libération (voir point 3.4.3.2) sont donc à vérifier, en plus de la condition de libération de la neuvième sous-route, imposée par le chaînage.

Au final, alors que du point de vue du train, l'itinéraire a été parcouru normalement et complètement et qu'il continue son trajet et sort de la gare d'Ottignies, l'enclenchement ne libère pas l'itinéraire.

3.4.4. LIBÉRATION PAR LA CLEF DE SECOURS DE L'ITINÉRAIRE NON LIBÉRÉ DU TRAIN 2E2020

Alors que le train 2E2020 a parcouru l'itinéraire et qu'il continue de rouler vers Profondsart, l'opérateur remarque la non-libération de l'itinéraire.
Après avoir vérifié que le train 2E2020 a parcouru normalement l'itinéraire et qu'il se trouve en aval du signal CX-D.29, l'opérateur applique la fonction NT.
L'AFS (*Auxiliary Function System*) a déterminé les commandes NIR requises à la destruction de l'itinéraire.
La commande SDG est automatiquement envoyée aux signaux D10-R.29 et CX-D.29 : déjà au rouge, ces 2 signaux ne doivent pas changer d'état.

Ensuite, la liste des NIR est établie et chaque NIR est envoyée par le système EBP vers l'enclenchement, en utilisant le système en 2 temps (préparation et confirmation) :

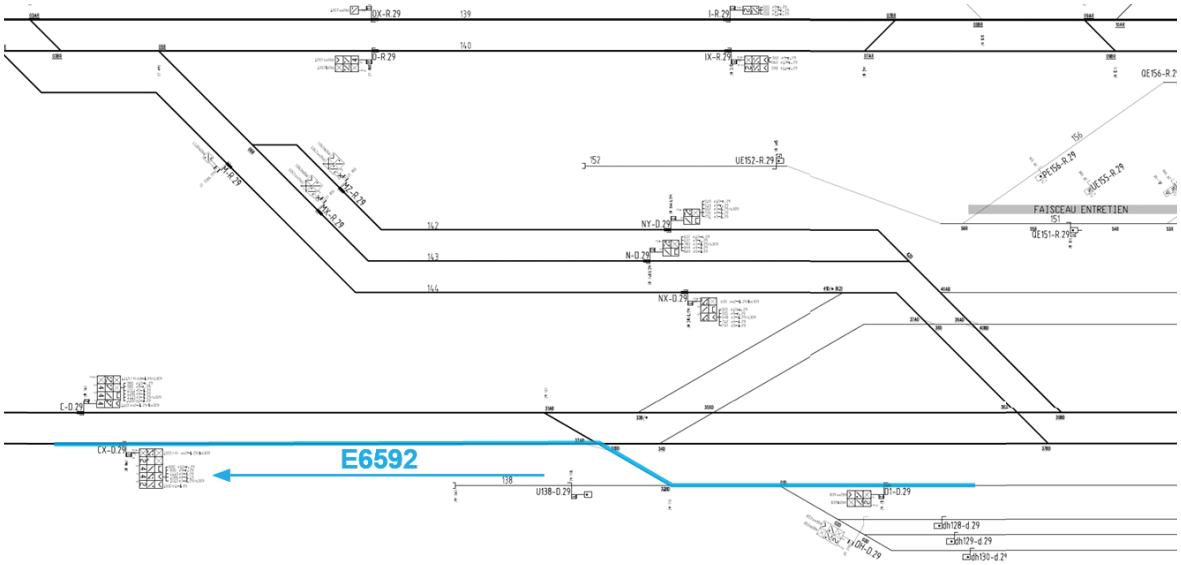
- NIR sur la sous-route D10R_13R
- NIR sur la sous-route 13R_50R
- NIR sur la sous-route 50R_45D
- …

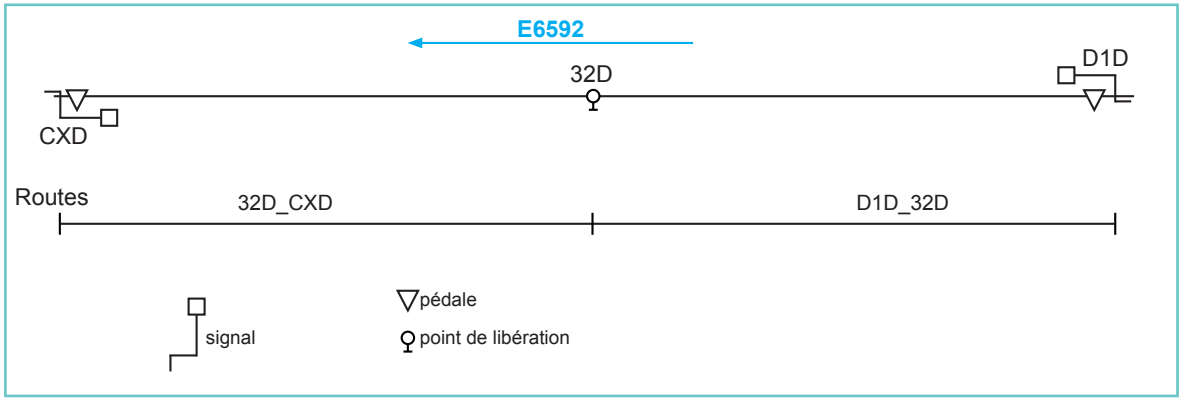
Lorsque le système applique la NIR sur la sous-route 35D_34D, le chaînage permet de libérer l'itinéraire complètement. En effet, la dernière sous-route est différente des 8 précédentes, en ce sens qu'elle comporte une pédale. Dès lors, les conditions de libération de cette dernière sous-route sont :

- que la sous-route précédente soit libérée (à cause du chaînage), ce qui est le cas par la NIR sur la sous-route 35D_34D
- que les CV de cette sous-route soient libérés, ce qui est le cas puisque le train n'occupe plus cette sous-route (le train continue de rouler vers Profondsart),
- que la pédale CXD ait bien fonctionné, ce qui est le cas : elle a enregistré le passage du train et s'est libérée lorsque le train a continué son trajet et ne l'enclenche plus,
- qu'il n'y ait pas de CIR, ce qui est le cas,
- le KFS du signal (des signaux) de la route a été obtenu : le signal CX-D.29 est bien au rouge

Dès lors, la dernière sous-route 34D_CXD se libère, ce qui a comme conséquence que toutes les sous-route constituant l'itinéraire sont libérées, entraînant la libération de l'itinéraire.

L'itinéraire libéré, le système de gestion de tracé de route (ARS = *Automatic Route Setting*) obtient les conditions pour tracer une nouvelle route pour un autre train : la route du train E6592 est tracée de la voie 111 vers la voie 012, composée de 2 sous-routes : D1D_32D et 32D_CXD.
L'EBP vérifie que toutes les conditions pour cette route sont réunies (= check route), et le signal D1-D.29 est alors commandé à l'ouverture. Le train E6592 commence à parcourir l'itinéraire.





Cependant, dans la liste des commandes NIR qu'a constitué le système, il reste encore les commandes NIR pour la sous-route 34D_CXD : elle doit encore être envoyée par l'EBP à l'enclenchement.

Lorsqu'elles sont lancées, elles restent dans un premier temps sans effet dans l'enclenchement : en effet, deux zones IR (31BD, CXD) sont communes au tracé du train E6592. Du fait du chaînage des 2 sous-routes de l'itinéraire du train E6592 qui vient d'être enclenché, les commandes NIR ne peuvent avoir d'effet (les conditions pour une libération ne sont pas réunies).

Dès que le train E6592 a dépassé,le point de libération 32D, la première sous-route D1D_32D se libère. Les conditions sont réunies pour que les commandes NIR appliquées soient effectives : les 2 zones IR (31BD, CXD) se "dé-immobilisent", libérant ainsi la sous-route 32D_CXD alors qu'elle est parcourue par le train E6592.

L'opérateur EBP voit apparaître une détection d'un mouvement intempestif, puisque le train E6592 a atteint la pédale CXD appartenant à une zone d'immobilisation non enclenchée. Sur l'image EBP, le tronçon sur lequel circule le train est coloré de bistre.

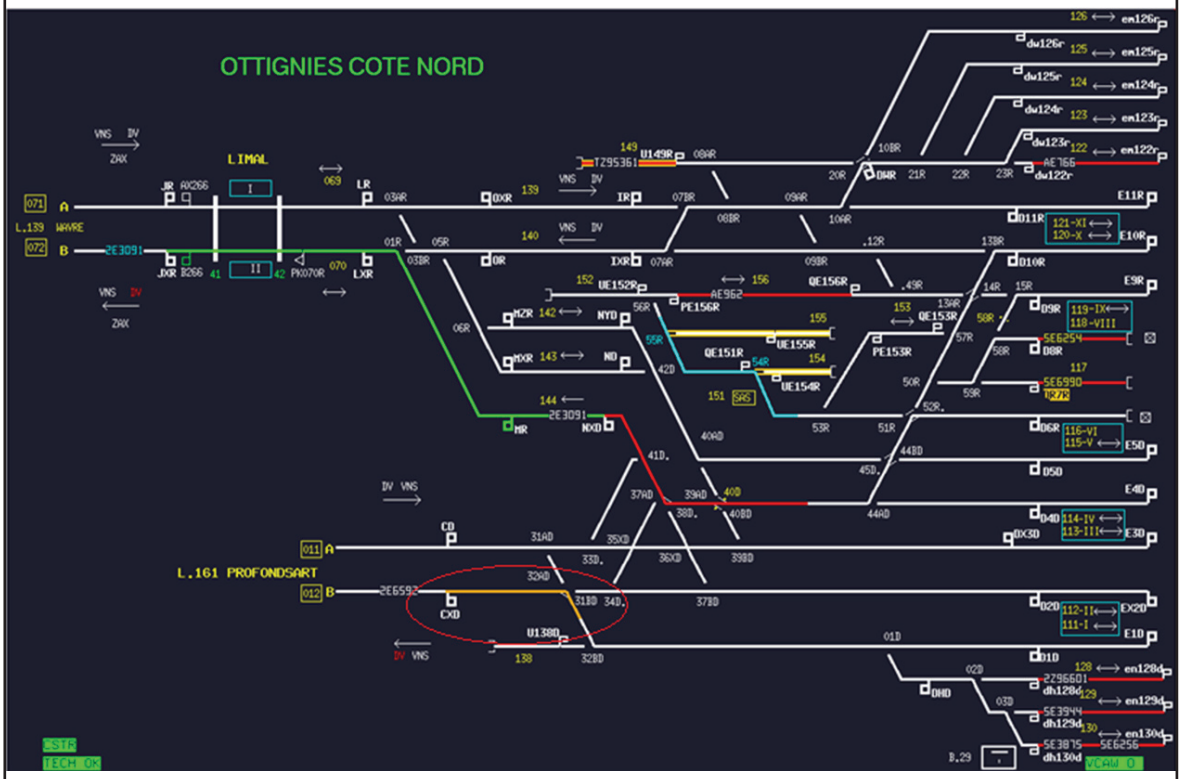
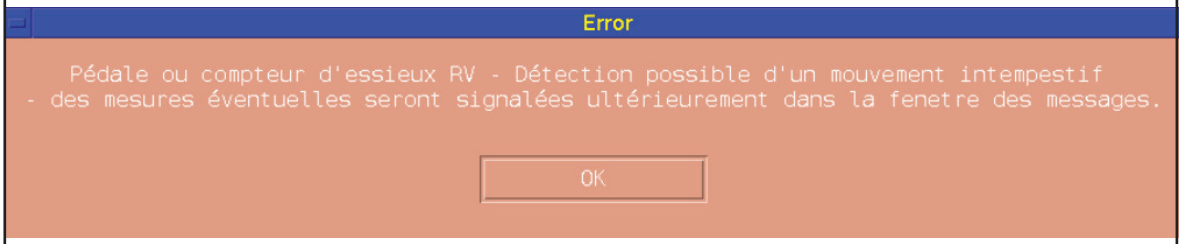


Illustration : écran EBP avec le train E6592 occupant l'itinéraire qui n'est plus enclenché



Du point de vue du conducteur du train E6592, rien ne change ni ne matérialise cet état : il poursuit son itinéraire et sort de la gare d'Ottignies.

3.4.5. ANALYSE DES DOBMI

L'analyse du DOBMI enregistré le jour de l'incident a permis de déceler une anomalie dans le système EBP/PLP. Cette analyse a permis de :

- comprendre les conditions d'occurrence de cette anomalie,
- s'assurer de la bonne compréhension du problème en le reproduisant sur simulateur,
- initier la mise en place d'un correctif.

3.4.6. ANALYSE ET DÉVELOPPEMENT D'UN CORRECTIF

L'analyse des logs[8] a mis en évidence la condition "primaire" pour la survenance du DOBMI :

- la destruction de la dernière sous-route de l'itinéraire du train E6590 alors que le train la parcourait.

Cette destruction était elle-même la résultante de diverses causes indirectes :

- une commande NT avait dû être lancée par l'opérateur suite au souci de la pédale D10R qui, avec le chaînage des sous-routes, n'a pas permis la libération de l'itinéraire une fois que le train 2E2020 l'avait parcouru,
- les diverses commandes NIR qui découlaient de la commande NT se sont intercalées dans les commandes de tracé de route,
- le retard entre la commande et son action effective, qui a été rendu possible par le mode de gestion de l'interface entre l'EBP et l'enclenchement de type SmartLock. L'EBP communique avec le SmartLock 400 selon un protocole qui permet l'envoi de commandes normales et de secours de manière concomitante.

La solution à apporter passait par une programmation de l'EBP pour éviter que l'enclenchement ne traite des commandes de tracé de route avant d'avoir exécuté toutes les commandes de sécurité.

Cette programmation a été gérée conjointement par Siemens et Infrabel, et constitue la mesure prise par le gestionnaire d'infrastructure en réaction au problème identifié (cf. chapitre 5)

8 *Log : terme employé notamment en informatique pour désigner un historique d'événements et, par extension, le fichier contenant cet historique*

3.5. DOCUMENTATION DU SYSTÈME OPÉRATOIRE

3.5.1. MESURES PRISES PAR LE PERSONNEL POUR LE CONTRÔLE DU TRAFIC ET LA SIGNALISATION

Au moment où le train E6592 parcourait la partie d'itinéraire qui n'était plus enclenchée, sur les voies, rien ne matérialisait cette occupation d'un itinéraire non enclenché : le train E6592 poursuivait son trajet en parcourant l'itinéraire tracé.

Du point de vue du système EBP/enclenchement, cette occupation est caractérisée de "probablement intempestive" et, pour assurer la sécurité, le système EBP prend un certain nombre de mesures :

- affichage d'un "popup" sur l'écran de dialogue ;
- application d'une protection par tableau 4 sur les appareils de voie concernés ;
- exécution automatique d'une SDG pour les autres mouvements ;
- affichage des mesures prises (SDG et Tableau 4) dans la fenêtre des messages de l'écran de dialogue.

L'anomalie manifestée par l'occupation intempestive a fait l'objet d'une analyse a posteriori : le but de l'analyse est de faire la distinction entre les occupations intempestives résultant d'un franchissement de signal intempestif (SPAD) et celles imputables à un dérangement.

3.6. INTERFACE HOMME-MACHINE-OPÉRATION

3.6.1. FORMATION/EXPÉRIENCE

Par sa formation, l'agent du mouvement est à même de commander le tracé des routes sur un poste EBP, de même que réagir aux messages apparaissant sur son écran.
La formation doit permettre à l'agent d'organiser et de coordonner efficacement et en toute sécurité la circulation des trains, ainsi que de rétablir la régularité du trafic en cas de dérangement ou d'incident.
La formation intègre :

- la théorie sur la réglementation, l'organisation et les tâches dévolues à l'agent du mouvement
- des exercices pratiques sur simulateur.

3.6.2. CONCEPTION

3.6.2.1. LOG

Le système de signalisation est composé de différents sous-systèmes dont l'EBP et les enclenchements électroniques. A des fins d'analyse et de monitoring, un enregistrement est réalisé, tant des commandes initiées par un opérateur que des actions entreprises par les automatismes ainsi que des captures des états d'éléments (signaux, appareils de voie, CV,…) : ce sont les logs.

3.6.2.2. DÉTECTION D'UN MOUVEMENT NON AUTORISÉ

Le contrôle de voie libre réalisé par les appareils de détection placés dans la voie envoie les informations au poste de signalisation.

Lors de la détection d'un mouvement non autorisé (mouvement intempestif), le système EBP :

- affiche un "popup" sur l'écran de dialogue ;
- applique une protection par tableau 4 sur les appareils de voie concernés ;
- exécute, éventuellement, automatiquement une SDG pour les autres mouvements ;
- affiche les mesures qu'il a prises (SDG et Tableau 4) dans la fenêtre des messages de l'écran de dialogue.

Au niveau de l'image EBP, un point rouge s'affiche à la pédale ou au compteur d'essieux qui a détecté le mouvement intempestif. Lorsqu'aucun itinéraire n'est tracé, le point rouge s'accompagne de la colorisation bistre sur la voie occupée. Les mouvements intempestifs sont enregistrés dans le logbook EBP et sont analysés selon des modalités définies.

3.6.2.3. VÉRIFICATIONS DES FONCTIONS DE SÉCURITÉ

Lorsqu'il applique la fonction de sécurité NT, l'agent du mouvement doit répondre à une série de questions générées par le système EBP afin de vérifier la pertinence de la commande initiée. La commande ne sera acceptée par le système que si les réponses aux questions programmées sont conformes à ce qui est attendu de l'opérateur.

3.6.3. PROCÉDURES

3.6.3.1. PROCÉDURE NT

Le système EBP est réglé de manière telle que certaines commandes sont inaccessibles ou soumises à des restrictions pour certains utilisateurs. Pour le système EBP, une distinction existe donc entre :

- une compétence, qui donne le droit à un utilisateur de faire quelque chose
- une responsabilité, qui impose à un utilisateur une certaine obligation pour la zone EBP (en tout ou en partie).

On distingue, entre autre :

- le desservant, responsable de la commande des installations de signalisation, à l'exception des fonctions auxiliaires de secours, à l'intérieur de la zone EBP;
- le surveillant, qui peut être responsable de la commande des installations de signalisation, y compris des fonctions auxiliaires de secours. Les fonctions lancées sur l'initiative du système EBP lui-même ou par des utilisateurs ne disposant pas de la compétence requise, sont transmises à l'utilisateur qui détient un droit de surveillance sur la zone de base concernée

Lors de l'application de la procédure de sécurité NT par un desservant, le système EBP a été programmé pour vérifier qu'un agent ayant un rôle de surveillant soit connecté au système pour la zone EBP concernée. Le desservant peut initier la commande NT mais le surveillant doit l'accepter et la continuer.

3.6.4. DISPONIBILITÉ TECHNIQUE

Une pédale est un appareil de détection qui enregistre le passage d'un train. Le jour de l'incident, la pédale associée au signal D10-R.29 n'a pas transmis l'information du passage du premier train comme attendu. Il s'agit d'un problème fugitif dont l'examen des différents logs n'a pas permis d'observer d'autres survenances sur une période de 6 mois.

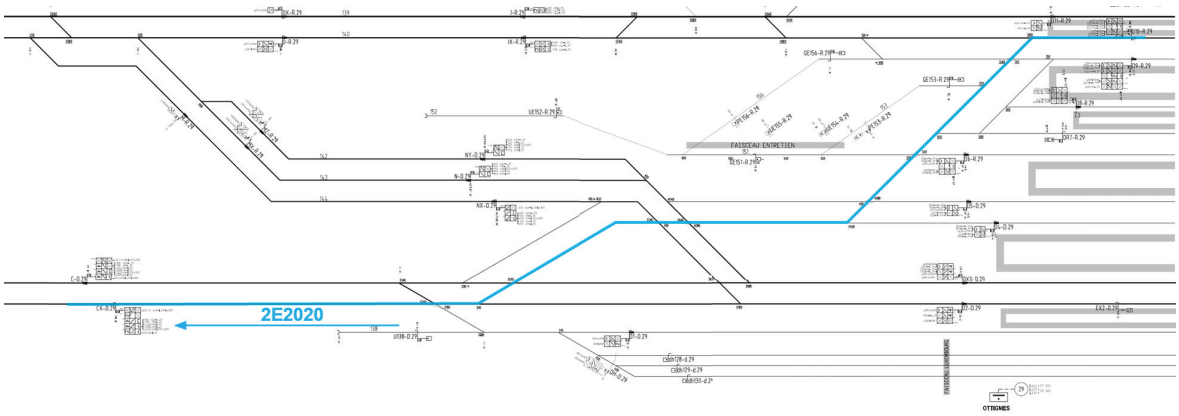
3.6.5. COMMUNICATIONS

A la suite de l'analyse du DOBMI, des mesures immédiates temporaires ont été décidées et transmises à tous les postes de signalisation EBP.
Le but des actions temporaires étaient d'empêcher toute autre manifestation du même type de phénomène que celui survenu à Ottignies.

4. ANALYSE ET CONCLUSIONS

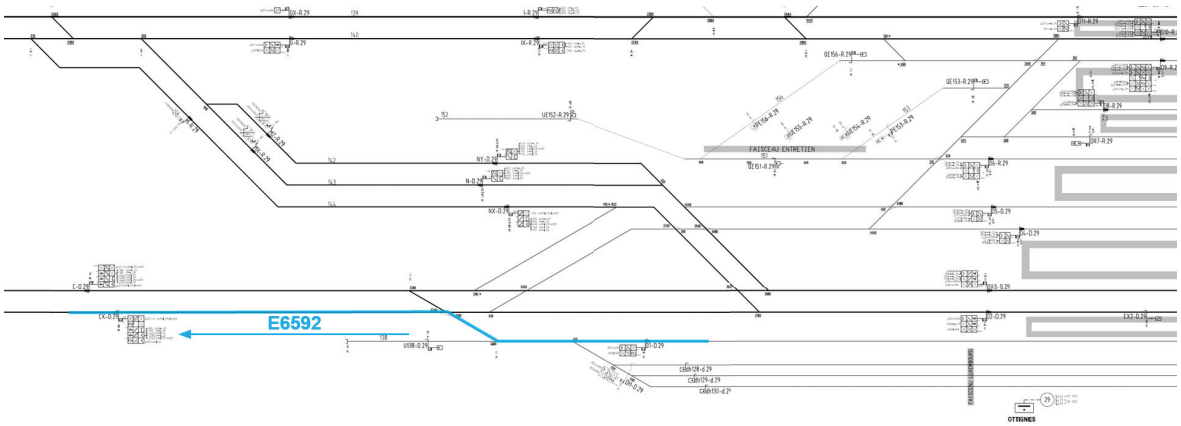
4.1. COMPTE-RENDU FINAL DE LA CHAÎNE D'ÉVÉNEMENTS

Le lundi 28/07/2014 vers 21h21, dans le gril de la gare d'Ottignies, le train E2020 circule du signal D10-R.29 de la voie 120 vers la voie 012 selon un itinéraire tracé. Cet itinéraire traverse de multiples aiguillages dans la gare d'Ottignies.



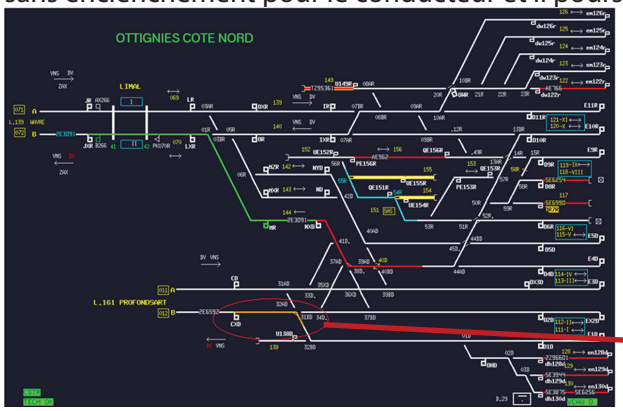
Un peu avant 21h22, alors que le train E2020 a fini de parcourir cet itinéraire et qu'il continue son parcours en sortant du gril d'Ottignies, l'opérateur du poste de signalisation EBP remarque que l'itinéraire entre le signal D10-R.29 et le signal CX-D.29 ne se libère pas.
Vers 21h22'24", conformément aux procédures et à la réglementation, il applique une fonction de secours NT du système EBP afin de détruire cet itinéraire.

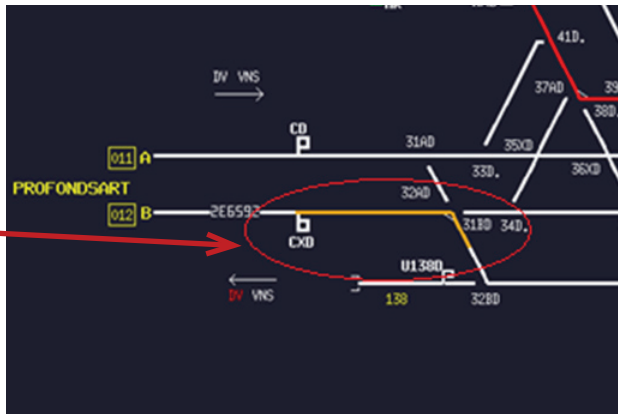
A 21h22'45", un itinéraire est tracé automatiquement par le système *Automatic Route Setting* (ARS) pour le train E6592 de la voie 111 vers la voie 012. Le système ARS ouvre le signal D1-D.29 et le train E6592 commence à parcourir cet itinéraire.



Alors qu'il en a parcouru une première partie, la seconde partie de cet itinéraire est détruite.

L'opérateur du poste de signalisation voit alors sur son écran le train E6592 coloré de bistre, signalant ainsi une occupation sans enclenchement. Sur la voie, rien ne matérialise cette occupation sans enclenchement pour le conducteur et il poursuit son trajet : le train sort du gril d'Ottignies.





Cet incident, sans conséquence sur le trafic des trains impliqués, résulte de la succession de plusieurs éléments :

- la pédale associée au signal D10-R.29 du début de l'itinéraire du premier train dysfonctionne : l'information du passage du premier train n'est pas transmise à l'enclenchement dans l'intervalle de temps prévu;
- l'itinéraire tracé pour ce train est composé d'une série de 10 sous-routes, chaînées les unes aux autres;
- le dysfonctionnement de la pédale ne permet pas de libérer la première sous-route, ce qui, par le chaînage, ne libère pas les sous-routes suivantes : l'itinéraire, bien que parcouru entièrement par le train, n'est pas libéré;
- la fonction NT de secours, initiée par le desservant suivant la réglementation, envoie une série de commandes depuis le système EBP vers l'enclenchement de type SmartLock :
    - une commande SDG pour les signaux encadrant la route
    - des commandes d'annulation de route (NIR) : chaque fraction (sous-route) composant l'itinéraire doit être libérée dans l'ordre par une commande NIR;
- lorsque la commande NIR de l'avant dernière sous-route est appliquée, et avant même l'envoi de la commande NIR pour la dernière sous-route, l'enclenchement libère l'itinéraire: la dernière sous-route se libère avec la libération de l'avant-dernière sous-route, étant donné que les 4 autres conditions de libération de cette sous-route avaient été remplies lors du passage du train;
- l'itinéraire libéré, les conditions sont réunies pour que le système *Automatic Route Settings* trace l'itinéraire du train E6592: les commandes de tracé de cet itinéraire sont envoyées par le système EBP vers l'enclenchement;
- au tracé de l'itinéraire, le signal, devant lequel le second train est à l'arrêt, est ouvert et le second train commence à parcourir son itinéraire;
- le système EBP envoie les commandes NIR (34D, 31BD, CXD) relatives à la dernière sous-routes de l'itinéraire du premier train (34D-CXD); vu les 2 zones d'immobilisation communes avec la dernière sous-route de l'itinéraire du train E6592, les commandes NIR sont inopérantes (cette sous-route (D1D-34D) est chaînée avec la première sous-route de l'itinéraire du train E6592);
- lorsque le train E6592 a terminé de parcourir la première sous-route de son itinéraire, cette fraction de son itinéraire est libérée, ce qui rend opérante les commandes NIR lancées (voir point précédent);
- au moment où le train aborde la seconde sous-route de son itinéraire, celui-ci se détruit, entraînant l'apparition du DOBMI (détection d'un mouvement sur un itinéraire non enclenché) sur l'écran EBP du desservant.

Le système EBP et l'enclenchement informatisé PLP enregistrent dans des logs les commandes et les états du système, ce qui permet, entre autre, des analyses. Les procédures du gestionnaire de l'infrastructure prévoient ainsi que les enregistrements des DOBMI soient analysés afin d'en déterminer la cause (SPAD, défaillance d'un organe de détection dans la voie,…) : l'analyse a mis en évidence les conditions particulières ayant entraîné la libération d'un itinéraire alors qu'il était parcouru par un train, ainsi que la nécessité de très rapidement apporter une correction à ce fonctionnement non sécurisé.
La collaboration d'Infrabel et de Siemens a permis à Siemens d'adapter la programmation de l'EBP en tenant compte de l'ordre dans lequel les commandes de sécurité doivent être envoyées à l'enclenchement SmartLock.

4.2. CONCLUSION

L'analyse des *logs* a mis en évidence la condition "primaire" pour la survenance du DOBMI :

- la destruction de l'itinéraire du train E6592 alors que le train le parcourait.

Cette destruction était elle-même la résultante de diverses causes indirectes :

- une commande NT avait dû être lancée par l'opérateur suite au souci de la pédale D10R qui, avec le chaînage des sous-routes, n'a pas permis la libération de l'itinéraire une fois que le train 2E2020 l'avait parcouru,
- les diverses commandes NIR qui découlaient de la commande NT se sont intercalées dans les commandes de tracé de route,
- le retard entre la commande et son action effective, qui a été rendu possible par le mode de gestion de l'interface entre l'EBP et l'enclenchement de type SmartLock. L'EBP communique avec le SmartLock 400 selon un protocole qui permet l'envoi de commandes normales et de secours de manière concomitante.

Enfin, les causes sous-jacentes de cet incident sont à rechercher dans les analyses systèmes réalisées lors de l'introduction des enclenchements SmartLock en remplacement des enclenchements Solid State Interlocking (SSI) : elles n'ont pas mis en évidence l'existence de ce problème potentiel. La gestion de l'interface EBP/SSI n'autorise pas l'envoi de commandes normales tant que les commandes de secours n'ont pas toutes été exécutées, ce qui n'était pas le cas pour l'interface EBP/SmartLock.
L'imbrication de commandes de différents types pouvait entraîner un fonctionnement non désiré, qui s'est produit lors de l'incident d'Ottignies.
Le problème survenu à Ottignies a révélé une faiblesse de l'analyse.

La présence de boucle de récupération (ou boucle de rattrapage) a permis d'identifier le dysfonctionnement, qui n'apparait que dans de très rares cas et dans des circonstances particulières.
L'apparition à l'écran du signaleur d'une occupation intempestive (DOBMI) et l'analyse a posteriori de cet événement constituent un indicateur pour les équipes techniques d'Infrabel.

L'analyse des mesures prises (détaillées au chapitre 5), du système de gestion des incidents et du système de gestion des actions correctives conclut que l'incident a été géré de façon professionnelle, argumentée et reproductible et n'amène pas à de recommandation.

5. MESURES PRISES

5.1. MESURES IMMÉDIATES

Avant qu'un correctif ne soit développé, il était important d'éviter qu'un incident similaire ne se reproduise. Infrabel a donc communiqués les 2 actions temporaires suivantes :

- avant de lancer une commande NT dans un gril, il fallait que l'opérateur du poste de signalisation désactive les automatismes de tracés de routes (ARS);
- avant de forcer une ligne de mouvement pour laquelle un "V"[9] est affiché sur l'écran EBP, il est nécessaire de vérifier l'état du gril.

5.2. CORRECTIF

L'analyse du DOBMI enregistré le jour de l'incident a permis de déceler une anomalie dans le système EBP/SmartLock. Cette analyse devait permettre de :

- comprendre les conditions d'occurrence de cette anomalie;
- s'assurer de la bonne compréhension du problème en le reproduisant sur simulateur;
- initier la mise en place d'un correctif.

Une fois le problème identifié, une phase de développement d'un correctif pour le système EBP s'est mise en place. Elle a associé Infrabel et Siemens, développeur de l'EBP.

Afin de structurer, enregistrer et faciliter les échanges entre les parties prenantes lors de la résolution du problème, il est fait usage de l'outil eBugp. Il s'agit d'une plateforme d'encodage des change requests et des problem reports, où chaque personne impliquée dans la résolution du problème est enregistrée et reçoit les communications relatives. Divers services du gestionnaire sont impliqués. Chacun reçoit un rôle (assigned, développeur, testeur, contrôleur,…), rôle qui peut évoluer au cours de la résolution du bug.
Le délai de correction du problème est également défini lors de cet encodage dans l'eBugp : un délai très court a été imposé.

Se constitue enfin un CCB, Committee Change Board, qui implique les 2 sociétés Infrabel et Siemens. C'est ce board qui a analysé le problème, ses impacts, le scope des tests et qui a déterminé quelles personnes seraient impliquées dans la gestion de la correction.

Siemens a imaginé plusieurs solutions. Au sein du board, Infrabel et Siemens ont évalué ces solutions et une seule a été sélectionnée.

9 *Un V dans la ligne de mouvement signifie que le tracé de la ligne de mouvement rencontre une incompatibilité : le dispositif de contrôle de libération de la voie signale une occupation dans le gril, sur un aiguillage parcouru, de protection et/ou d'incompatibilité.*

La solution adoptée consiste, lorsqu'une commande de sécurité a été initiée au sein de la zone EBP, à "empiler" les commandes normales (c-à-d de tracé de route) après les commandes de sécurité. Le système EBP doit envoyer les commandes une à une dans l'ordre de la pile et, de ce fait, les commandes de sécurité seront exécutées entièrement avant toute autre commande normale, qu'elle soit issue d'un opérateur ou du système ARS.
Cette solution consiste à l'adaptation de la gestion de l'interface entre l'EBP et le SmartLock lors de l'envoi de commandes (normales et de sécurité).
Le changement à programmer a été décrit dans un document de spécifications pour être ensuite transmis à Siemens.

S'en est suivi du développement par Siemens, au terme duquel Siemens a effectué ses propres tests et contrôles. Ces derniers avaient été décrits au sein de la plateforme eBugp pour assurer une traçabilité optimale et y ont été annexés les résultats des tests effectués.

Infrabel a réalisé ensuite divers tests sur 2 plateformes différentes, durant lesquels divers scénarios ont été envisagés, de même que la simulation de l'incident d'Ottignies.

Les tests et contrôles étant concluant, la nouvelle version (release) développée a été installée sur tous les postes de signalisation présents sur le réseau Infrabel.

Organisme d'Enquête sur les Accidents et Incidents Ferroviaires

http://www.mobilit.belgium.be