Cybersécurité des Systèmes de Surveillance des Appareils de Voie Ferroviaires

Sara Abdellaoui, Dinh Duy Kha Nguyen, Emil Dumitrescu, Cédric Escudero, Eric Zamaï

Cybersécurité des Systèmes de Surveillance des Appareils de Voie Ferroviaires

Sara Abdellaoui, Dinh Duy Kha Nguyen, Emil Dumitrescu, Cédric Escudero, and Eric Zamai

Univ Lyon, INSA Lyon, Université Claude Bernard Lyon 1, Ecole Centrale de Lyon, CNRS, Ampère, UMR5005, 69621 Villeurbanne, France
prénom.nom@insa-lyon.fr

Abstract

Bien qu'ils soient de plus en plus performants, les systèmes cyberphysiques demeurent sensibles aux cyberattaques. Cet article porte sur les appareils de voie de l'infrastructure de transport ferroviaire. Pour de tels systèmes, les données surveillées sont géographiquement dispersées, ce qui les rend particulièrement vulnérables : les attaquants peuvent soit masquer des pannes, soit déclencher des décisions de maintenance inutiles. Pour répondre à ce problème, un paradigme d'évaluation des menaces cybernétiques est proposé afin de mettre à la disposition des opérateurs de maintenance un indicateur de menace basé sur des données de terrain. L'approche est développée et validée à partir d'un ensemble de données simulées relatives aux appareils de voie ferroviaires.

1 Introduction

La plupart des secteurs industriels sont aujourd'hui vulnérables face aux cyberattaques : la santé, le réseau électrique, le militaire, les transports, etc [26]. Quant aux infrastructures de transport, le secteur ferroviaire a révélé des vulnérabilités qui ont des conséquences sur la sécurité des biens et des personnes, ainsi que sur sa disponibilité. En 2017, la cyberattaque WannaCry contre la gare allemande Deutsche Bahn a affecté les distributeurs de billets et les systèmes d'information des passagers [25]. En 2022, l'attaque contre le train danois a bloqué la circulation des trains pendant des heures [23] ; ou encore, la perturbation des mouvements des forces russes sur le territoire biélorusse en début 2022 qui a paralysé le réseau ferroviaire [24].

Dans le contexte des menaces diversifiées, l'objectif de ce travail est de mettre à la disposition des opérateurs de maintenance d'infrastructures ferroviaires des informations supplémentaires concernant l'authenticité des signaux télésurveillés. La décision de maintenance repose sur des informations recueillies par le système de surveillance central CMS (Central Monitoring System). Or, ce système présente des vulnérabilités que les attaquants peuvent exploiter, ce qui provoque des imprécisions telles que des Faux Positifs (FP) ou des Faux Négatifs (FN). Dans le cas des Appareils de Voie (AdV), un FP signifie la détection de pannes en réalité inexistante, ce qui peut mener à des décisions de maintenance inutiles entraînant des surcoûts. En revanche, un FN signifie la non-détection de pannes existantes, ce qui peut conduire à des conséquences catastrophiques à la fois sur la vie des personnes et sur les équipements. Les types d'attaques considérés dans ce travail sont ceux qui visent à intercepter la communication entre les capteurs et le CMS ou à injecter directement de fausses données dans les relevés des capteurs afin de dégrader le système de surveillance et de limiter la disponibilité de l'AdV en déclenchant des faux négatifs ou des faux positifs. La détection de ces attaques peut se faire sur deux niveaux :

- **Détection locale** : le niveau de détection locale permet de détecter les attaques visant à modifier les données stockées dans les concentrateurs de données. Les mesures des

capteurs sont exploitées ainsi qu'un modèle mathématique précis du système physique (AdV) pour reconstruire l'entrée de ce système qui est la tension du moteur responsable du mouvement d'aiguillage. Pour rechercher en détail le fonctionnement normal et aussi les défaillances de l'AdV, un simulateur a été construit basé sur les équations fondamentales de la physique considérée. Sur la base de cette connaissance, une méthode optimisée de détection des attaques est développée.

- **Détection globale** : le niveau de détection globale porte sur les attaques furtives ayant réussi à contourner la détection locale. Ces attaques se manifestent sous la forme d'un mode de fonctionnement normal de l'AdV (avec ou sans défaut) visant à masquer des pannes ou à initier des décisions de maintenance inutiles. Pour ce faire, deux blocs de fonctions complémentaires ont été intégrés au CMS, tel que l'illustre la Figure 1.

Le reste de l'article est organisé comme suit. La section 2 présente un état de l'art des méthodes de détection des cyberattaques. La section 3 met en avant une vue d'ensemble de l'architecture de l'AdV, ainsi que les hypothèses requises pour le développement de la méthode proposée. La section 4 détaille la procédure de développement du modèle de détection globale. La section 5 présente le simulateur d'un AdV pour générer des courbes de fonctionnement. La section 6 propose une application de l'approche proposée et enfin, la dernière 7 conclut l'article et donne les perspectives de recherche.

2 État de l'art

Pour faire face aux cyberattaques et éviter les pertes humaines et économiques, des mesures de sécurité sont nécessaires pour assurer la sécurité des CPS. Deux paradigmes de détection des intrusions sont préconisés dans la littérature [2] :

- *Misuse Intrusion Detection (MID) systèmes* : La détection des intrusions est basée sur une liste d'attaques connues stockées dans une base de données. Les systèmes MID sont capables de détecter les attaques connues et non les nouvelles.

- *Anomaly Intrusion Detection (AID) systèmes* : La détection des intrusions est basée sur des modèles caractérisant les comportements licites du système.

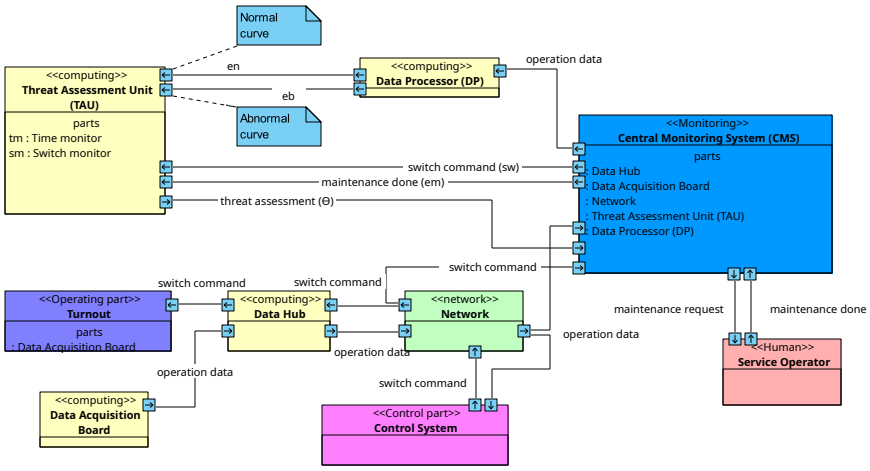


Figure 1: Procédure d'acquisition des données de l'AdV.

Selon [10], la détection d'attaques est possible en s'appuyant sur des méthodes AID qui font appel à des techniques fondées sur la statistique, la connaissance et l'apprentissage automatique.

En utilisant une technique statistique, les auteurs dans [1] proposent des modèles de Markov cachés pour détecter et distinguer les données défaillantes des données malveillantes dans un réseau de capteurs. Les modèles de défaillance et d'attaque sont définis à l'avance de manière à ne prendre en compte que les attaques qui modifient le comportement du système différemment des changements provoqués par les défaillances. En revanche, l'objectif de cette approche est de détecter et de distinguer les attaques des défaillances qui affectent le système de la même manière. Quant à [12], les auteurs proposent un algorithme de détection en ligne des cyberattaques pour un processus de décision de Markov partiellement observable en utilisant l'apprentissage par renforcement. L'avantage de la méthode est la rapidité de détecter les changements dans les conditions normales de fonctionnement. Néanmoins, elle ne permet pas de distinguer les défaillances des cyberattaques, et plus encore, si l'attaquant imite les conditions normales de fonctionnement, cette méthode ne permet pas de détecter l'attaque.

Les techniques basées sur la connaissance définissent des modèles fondés sur les spécifications du système et la définition de son comportement légitime fournies par les experts [8].

Concernant les techniques d'apprentissage automatique, elles ont été largement utilisées dans la détection des attaques. Citons notamment Isolation Forest IF [15, 7], Random Forest RF [4, 19], Support Vector Machine SVM [16, 4], K-Nearest Neighbor KNN [27], classification Bayésienne [3, 11]. Ces approches de détection présentent des limites, particulièrement le fait que la détection ne repose que sur la modélisation du comportement normal du système pour détecter tout comportement différent de celui-ci [15, 7, 19, 16], il convient également de noter que ces méthodes sont incapables de distinguer les modes de défaillance des cyberattaques et sont facilement manipulables si l'objectif de l'attaquant est de faire croire aux opérateurs que le système a un comportement normal. Ou encore [4, 27] où les auteurs développent des modèles basés soit sur des données fiables résultant d'une communication sécurisée entre les capteurs de terrain et les niveaux supérieurs, soit sur des ensembles de données étiquetées, contrairement aux types d'attaques considérés dans le présent article.

Bien que des travaux de recherche aient été consacrés à l'évaluation du risque de cyber-attaque visant les systèmes ferroviaires [18, 5, 22], peu de travaux traitent de la détection des cyberattaques en considérant le réseau ferroviaire comme un système cyberphysique. La référence [28] propose une méthode pour détecter les attaques contre les capteurs de vitesse des trains. Elle est basée sur la prévision du bruit des capteurs à l'aide des informations topographiques de la voie ferrée et la comparer à l'estimation du bruit. Dans [13], le système de détection proposé est destiné à détecter l'injection de fausses données de tension, de courant et de position dans les bornes de train. Pour ce faire, les auteurs commencent par construire des vecteurs d'attaque, puis développent un détecteur en deux étapes pour révéler des attaques en définissant des seuils sur les données des capteurs. Et pour éviter les fausses alarmes, [13] prévoit de ne déclencher une alarme qu'en cas de détection successive d'alarmes. La référence [6] présente la détection des attaques contre le réseau Ethernet dans le ferroviaire en utilisant et en comparant des techniques d'apprentissage automatique. Pour valider l'approche proposée, une expérience a été menée sur un ensemble de données étiquetées.

Selon nos connaissances, aucun des travaux existants sur la détection des attaques contre les CPS n'a abordé la détection des attaques furtives visant à dissimuler des pannes ou à déclencher des décisions de maintenance inutiles.

3 Contexte et Problématique

Dans cet article, nous nous intéressons à la détection d'attaques portant sur la télésurveillance des appareils de voie. Dans un premier temps, nous présenterons le fonctionnement de l'architecture de télésurveillance puis nous développerons les hypothèses de travail et la problématique de recherche que nous cherchons à résoudre.

3.1 Appareil de voie

Un AdV, communément appelé système d'aiguillage, est un dispositif électromécanique installé sur les rails permettant aux trains de changer de voies. Ce dispositif est dit critique puisqu'une panne ou une mauvaise commande peut entraîner un mauvais aiguillage, voire un déraillement du train. Chaque AdV se retrouve ainsi équipé de capteurs mesurant la commande de l'actionneur électromécanique, le courant et la vitesse de rotation du moteur, et la force exercée par l'actionneur sur le rail. Les données capteurs sont ensuite transmises au concentrateur de données (CD) via un bus CAN. Un CMS reçoit et traite ensuite l'ensemble des données provenant de chaque CD installé sur le réseau ferroviaire afin de l'informer sur l'état de santé de chaque AdV (Figure 2).

3.2 Hypothèses et Problématique

La vulnérabilité du système de surveillance est basée sur la répartition géographique des AdV sur l'ensemble du territoire national, ce qui permet aux attaquants de s'introduire facilement dans le système à n'importe quel niveau, comme le montre la Figure 2.

Les opérateurs de maintenance s'appuient sur l'analyse des données de terrain pour déterminer si le système d'aiguillage fonctionne correctement ou nécessite une maintenance. La problématique traitée par cet article consiste à fournir aux opérateurs un indicateur de menace associé à chaque donnée de terrain. Ces données représentent la quantité de courant consommée pendant la manœuvre d'aiguillage.

Le scénario malveillant considéré est un scénario de manipulation des données de terrain par des attaquants. Le but est de modifier la forme de la courbe de courant pour corrompre les informations acquises par le CMS concernant l'état de santé de l'AdV.

Étant donné que la forme d'une courbe de courant peut varier en fonction de plusieurs conditions (obstacles, lubrification, cyberattaques...), plusieurs travaux de recherche proposent des modèles pour diagnostiquer les pannes d'AdV à partir des courbes de courant [9, 20]. Mais le

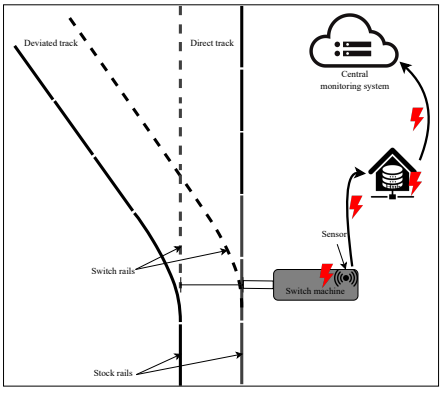


Figure 2: Appareil de Voie.

principal défi à relever reste de déterminer dans quelle mesure l'état de santé de l'AdV annoncé par le système classique de diagnostic des pannes reflète son état réel.

On considère un attaquant avec des connaissances approfondies de l'infrastructure ferroviaire, mais sans avoir la visibilité sur les plannings de maintenance donc sur le cycle de vie de l'AdV. Pour être furtif, il manipule les données pour les rendre similaires à celles associées à un fonctionnement normal ou à des pannes. Dorénavant, deux types d'attaques sont considérés :

- Attaque par masquage de pannes : l'attaquant dissimule une panne existante en faisant croire au CMS que l'AdV fonctionne normalement en diffusant une courbe de courant de comportement normal;
- Attaque par injection de pannes : l'attaquant simule une panne inexistante en faisant croire au CMS qu'il y a une défaillance dans l'AdV qui nécessite une maintenance par la diffusion d'une courbe de courant indiquant une panne.

4 Méthode proposée

La méthode proposée est illustrée par la Figure 3. Les données d'entrée sont celles que le CMS reçoit de chaque AdV pendant chaque manœuvre d'aiguillage. La méthode s'appuie sur les connaissances des opérateurs ferroviaires concernant le vieillissement et l'usure de chaque AdV dans le cadre du planning de maintenance. L'approche adoptée suit deux phases :

- La *phase de développement* démarre avec une grande quantité de données de surveillance. Le principal défi consiste à déterminer comment utiliser ces données et comprendre leur pertinence. Cela se fait par une première étape d'analyse sémantique en utilisant une technique de clustering (regrouper automatiquement les données en clusters). Ensuite, une signification doit être associée à chaque groupe de courbes de courant (cluster) en se basant sur les connaissances des experts. Pour valoriser cette opération d'apprentissage et généraliser le processus de prédiction pour des nouvelles données de terrain, une étape de modélisation des données basée sur une méthode d'apprentissage supervisé a été effectuée, conduisant à la création de la fonction *Data Processor* DP qui donne une étiquette à chaque donnée de terrain : normale e_n ou anormale e_b.
- La *phase d'exploitation* représente un processus récurrent basé sur les résultats du DP : e_n ou e_b. Cette phase est déclenchée par la réception d'une courbe de données de terrain et conduit une évaluation de la menace menée par le *Threat Assessment Unit* TAU dans le but de produire une estimation de menace. Dans le cadre de cet article, seule la phase d'exploitation sera présentée.

4.1 Évaluation des cyberattaques

En dehors du fonctionnement normal, il existe autant de typologies de courbes que de dysfonctionnements : adaptation, lubrification, usure, etc. Sans perte de généralité, le périmètre de cette étude se réduit à deux classes : les courbes normales e_n et les courbes de panne e_b. Soit $E = \{e_n, e_b\}$ les deux étiquettes associées. La phase précédente de développement a permis de classifier le comportement relatif à une courbe de courant acquise comme étant "normal" ou "panne". Désormais, indépendamment de la forme exacte d'une courbe de courant, seule son étiquette, fournie par le processeur de données (DP), est prise en considération. Il convient de noter que l'apparition d'une étiquette peut être considérée comme un événement. Le type et le contexte d'apparition de chaque événement sont traduits en une estimation de menace Θ par le TAU selon les modalités suivantes :

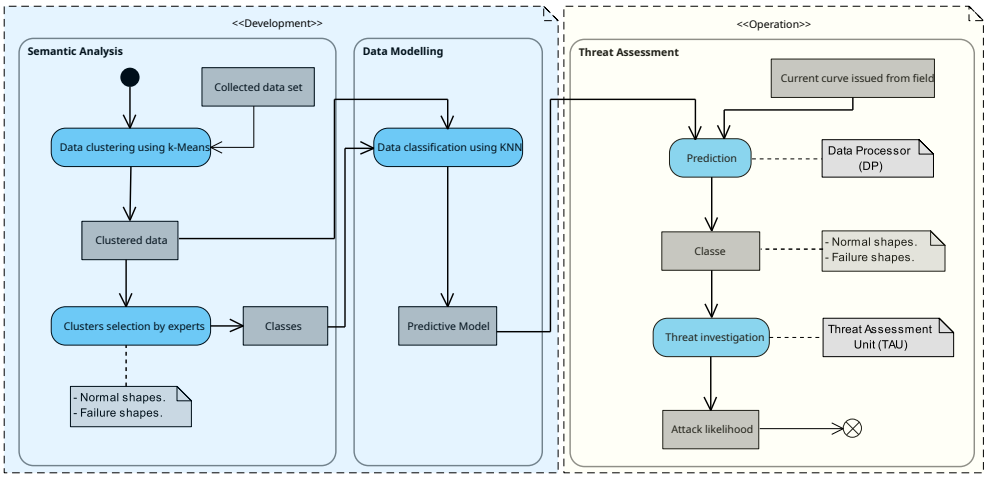


Figure 3: Méthodologie proposée.

- Θ fournit une probabilité. Il est considéré que $\Theta \in]0, 1[$, ce qui signifie que la menace ne peut jamais être jugée impossible (proche de 0) ni totalement certaine (proche de 1);
- chaque occurrence de e_n ou e_b conduit à une estimation de Θ;
- après une opération de maintenance, l'apparition de e_b éveille davantage de soupçons, alors qu'avant une maintenance prévue, les soupçons sont moindres;
- après une opération de maintenance, l'occurrence de e_n suscite une suspicion faible et, avant une maintenance planifiée, une suspicion plus élevée.

Les opérations de maintenance sont considérées comme consécutives à la détérioration de l'AdV, qui se produit soit au fil du temps, soit à la suite d'un certain nombre de manœuvres d'aiguillage [21]. Dans la réalité, les pannes sont liées à l'usure. Et aussi peuvent être fréquentes juste après les opérations de maintenance. En effet, les experts évaluent le comportement dysfonctionnel d'un ensemble des AdV (et de la plupart des systèmes en général) selon la courbe de *Baignoire* [21], illustrée à la Figure 4. Il est désormais établi que le comportement dysfonctionnel d'une collection de pièces identiques se déroule en trois étapes [21] :

- *période de rodage* : la phase initiale après la maintenance (ou l'installation) du système, dans laquelle le taux de panne est élevé du fait de défauts de matériaux et de problèmes dans l'installation de l'AdV;
- *période de vie utile* : la période d'exploitation où le taux de défaillance se stabilise au niveau le plus bas;
- *période d'usure* : la dernière période de la durée de vie de l'AdV où le taux de défaillance augmente en raison du vieillissement, de la détérioration des matériaux, d'un entretien médiocre de l'AdV, etc.

D'après ce qui précède, la détection des attaques visant le masquage ou l'injection de pannes est basée sur la surveillance du temps de vieillissement et du nombre de manœuvres d'aiguillage

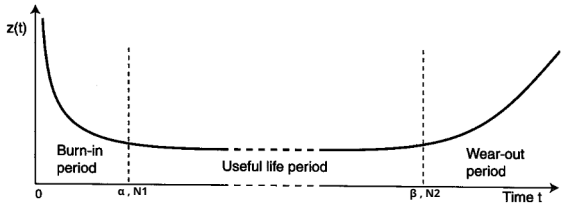


Figure 4: Courbe en Baignoire [21].

effectuées depuis l'installation ou la maintenance de l'AdV. Il est supposé qu'après chaque opération de maintenance, le système d'aiguillage se comporte comme après son installation.

En fonction de l'usure de l'AdV, le TAU surveille les événements survenant en considérant à la fois la durée et le nombre d'opérations d'aiguillage. Selon l'expertise et les connaissances des opérateurs ferroviaire, quatre jalons peuvent être définis pour s'y référer : α et β pour le facteur temporel; N_1 et N_2 pour le facteur nombre de manœuvres d'aiguillage. Ces facteurs sont liés à la période de vie utile de l'AdV, où les pannes "naturelles" sont peu fréquentes, comme le montre la Figure 4. Ainsi, pendant la période de rodage, le TAU ne peut pas estimer le degré de menace associé à une courbe normale ou de panne. Cela est dû au risque élevé de défaillances pendant cette période, alors qu'un comportement normal est également attendu.

La surveillance des menaces est donc assurée par deux blocs, chacun modélisé par un modèle dynamique basé sur des états/événements. Les états $\{0, 1, 2\}$ représentent les trois intervalles de la courbe de "baignoire". Les transitions sont déclenchées par les mêmes événements $E = \{e_m, e_n, e_b, sw\}$:

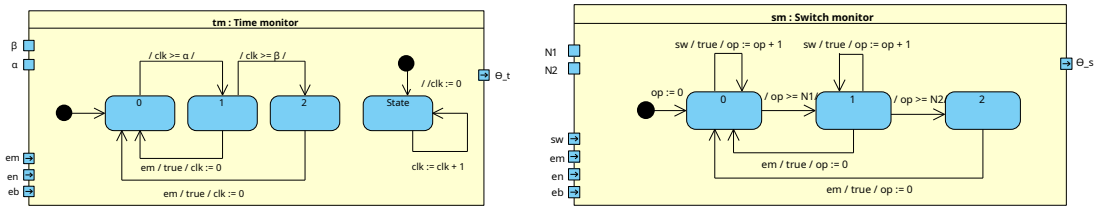
- Le moniteur de temps Tm (Time Monitor) est représenté dans la Figure 5a et défini comme $Tm = \langle Q_t, q_t^0, E, \delta_t, \Theta_t \rangle$ où Q_t et E représentent les ensembles d'états et d'événements, q_t^0 est l'état initial et δ_t la fonction de transition de Tm. Soit ϵ un nombre réel positif infiniment petit. $\Theta_t : Q_t \times \{e_n, e_b\} \times \mathbb{R}^+ \to]0, 1[$ est la fonction de sortie de Tm définie comme suit :

$$\Theta_t(s_t, e, t) = \begin{cases} 0.5 & \text{if } s_t = 0 \\ \frac{\beta - t - \epsilon}{\beta - \alpha} & \text{if } s_t = 1 \ \& \ e = e_b \\ \frac{t - \alpha + \epsilon}{\beta - \alpha} & \text{if } s_t = 1 \ \& \ e = e_n \\ \epsilon & \text{if } s_t = 2 \ \& \ e = e_b \\ 1 - \epsilon & \text{if } s_t = 2 \ \& \ e = e_n \end{cases} \tag{1}$$

  L'état du moniteur de temps Tm évolue en fonction d'une horloge interne clk qui est réinitialisée à chaque action de maintenance e_m.

- Le moniteur de manœuvre d'aiguillage Sm (Switch Monitor) est représenté dans la Figure 5b et défini comme $Sm = \langle Q_s, q_s^0, E, \delta_s, \Theta_s \rangle$ où Q_s, q_s^0, δ_s et E sont similaires à ce qui précède et $\Theta_s : Q_s \times \{e_n, e_b\} \times \mathbb{N}^+ \to]0, 1[$ est la fonction de sortie de Sm définie comme suit :

$$\Theta_s(s_s, e, op) = \begin{cases} 0.5 & \text{if } s_s = 0 \\ \frac{N_2 - op - \epsilon}{N_2 - N_1} & \text{if } s_s = 1 \ \& \ e = e_b \\ \frac{op - N_1 + \epsilon}{N_2 - N_1} & \text{if } s_s = 1 \ \& \ e = e_n \\ \epsilon & \text{if } s_s = 2 \ \& \ e = e_b \\ 1 - \epsilon & \text{if } s_s = 2 \ \& \ e = e_n \end{cases} \tag{2}$$



(a) Moniteur de temps. (b) Moniteur de manœuvre d'aiguillage.

Figure 5: Estimation de la menace.

L'état du moniteur de manœuvre d'aiguillage Sm évolue en fonction du nombre d'opérations d'aiguillage op, qui est incrémenté à chaque commande de commutation sw et réinitialisé à chaque action de maintenance e_m.

L'indicateur global de menace Θ de l'aiguillage prend en compte à la fois le temps d'occurrence et le nombre d'opérations d'aiguillage. Pour obtenir Θ, une estimation de Θ_t et de Θ_s est d'abord effectuée. Ensuite, pour garantir la prise en compte du scénario le plus défavorable et éviter les éventuelles attaques, la valeur maximale des valeurs Θ_t et Θ_s est attribuée à Θ en tant qu'indicateur global de la menace.

Après avoir présenté la méthode de détection globale, nous présentons le simulateur développé afin de tester la méthode proposée.

5 Simulateur d'un appareil de voie

5.1 Modélisation du système

La modélisation d'un AdV peut être décomposée en deux sous-modèles inter-connectés : le modèle de l'actionneur électromécanique (EMA) et de la lame d'aiguilles. Tout d'abord, nous modélisons le comportement dynamique de l'EMA puis celui de la lame d'aiguilles. Enfin, nous présenterons plusieurs défaillances qui ont été reportées dans la littérature.

5.1.1 EMA

L'EMA se compose d'un moteur à courant continu, d'un réducteur, d'une vis à billes et d'une pince appliquant la force générée par l'EMA sur la lame d'aiguilles. Le comportement dynamique de l'EMA peut être décrit par la représentation d'états suivante [14] :

$$\begin{aligned} \dot{x}_a(t) &= A_a x_a(t) + B_a u_a(t) \\ y_a(t) &= C_a x_a(t) + B_a u_a(t) \end{aligned} \tag{3}$$

avec $x_a(t) = [i_m(t), \theta_m(t), \dot{\theta}_m(t), \theta_{gs}(t), \dot{\theta}_{gs}(t), \theta_{bs}(t), \dot{\theta}_{bs}(t)]^\top$ ($x_a \in \mathbb{R}^7$) où $\dot{\theta}_m(t)$ [rad.s^{-1}], $\theta_m(t)$ [rad], $i_m(t)$ [A] sont respectivement l'accélération angulaire, la position angulaire et le courant du moteur; $\dot{\theta}_{gs}(t)$ [rad.s^{-1}], $\theta_{gs}(t)$ [rad] sont respectivement la vitesse et la position angulaires du réducteur; et $\dot{\theta}_{bs}(t)$ [rad.s^{-1}], $\theta_{bs}(t)$ [rad] la vitesse et la position de la vis à billes; $u_a(t) = [v(t), x_l(t), \dot{x}_l(t), f_s(t)]^\top$ ($u_a \in \mathbb{R}^4$) avec $v(t)$ [V] la tension appliquée au moteur, $\dot{x}_l(t)$ [m.s^{-1}], $x_l(t)$ [m] la vitesse et le déplacement de la lame d'aiguilles, $f_s(t)$ [N] la force de contact entre la lame d'aiguilles et le rail fixe; et $y_a(t) = [f_a(t), i_m(t)]^\top$ ($y_a \in \mathbb{R}^2$) où $f_a(t)$ [N] est la force délivrée par l'actionneur et $i_m(t)$ [A] le courant mesuré et transmis au concentrateur de données (CD). Les matrices du système (3) sont définies en (5).

$$A_a = \begin{bmatrix} -\frac{R_m}{L_m} & 0 & -\frac{K_e}{L_m} & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ \frac{K_t}{J_m} & -\frac{K_s}{J_m} & -\frac{(D_m+C_s)}{J_m} & \frac{K_s}{C_s} & \frac{C_s}{J_m} & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & \frac{K_s}{J_g} & \frac{C_s}{J_g} & (-\frac{K_s}{J_g} - \frac{K_s}{J_g n_g n_b}) & -\frac{D_g-C_s}{J_g} - \frac{C_s}{J_g n_g n_b} & \frac{K_s}{J_g n_g} & \frac{C_s}{J_g n_g} \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & \frac{K_s}{J_b n_b} & \frac{C_s}{J_b n_b} & -\frac{l_b^2 \times K_b}{4\pi^2 J_b} - \frac{K_s}{J_b} & -\frac{l_b^2 C_b}{4\pi^2 J_b} - \frac{D_b+C_s}{J_b} \end{bmatrix}, \tag{4}$$

$$B_a = \begin{bmatrix} \frac{1}{L_m} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & \frac{l_b K_b}{2\pi J_b} & \frac{l_b C_b}{2\pi J_b} & \frac{l_b}{2\pi J_b} \end{bmatrix}, C_a = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & \frac{l_b k_b}{2\pi} & \frac{l_b C_b}{2\pi} \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, D_a = \begin{bmatrix} 0 & K_b & -C_b & -1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \tag{5}$$

La vitesse de rotation de la vis à billes $\dot{\theta}_{bs}$ sature :

$$\dot{\theta}_{bs}(t) = \begin{cases} \dot{\theta}_{bs}(t) & \text{si } \dot{\theta}_{bs}(t) \geq 0, \\ 0 & \text{sinon.} \end{cases} \tag{6}$$

Les paramètres du modèle EMA sont les suivants : résistance R_m (2.6 Ω), inductance L_m (0.0108 H), constante de la force électromagnétique K_e (0.2865 Vrms/(rad.s^{-1})), constante de couple du moteur K_t (0.75 N.mA^{-1}), inertie J_m (7.5×10^{-3} kg.m^2), constante d'amortissement D_m (4.01×10^{-4} Nm(rads^{-1})) (moteur); inertie J_g (2.1×10^{-3} kg.m^2), constante d'amortissement D_g (3×10^{-4} N.m(rads^{-1})), rapport de réduction n_g (15) (réducteur); inertie J_b (0.2 kg.m^2), constante d'amortissement D_b (0.1×10^{-4} N.m(rads^{-1})), rapport de réduction n_b (15), pas de vis l_b (0.008 m) (vis à billes); raideur K_s (10 N.m^{-1}), constante d'amortissement C_s (1500 kg.s^{-1}) (arbre de transmission moteur-réducteur et réducteur-vis à billes); constante de raideur K_b (10 N.m^{-1}), constante d'amortissement C_b (10^7 kg.s^{-1}) (connexion vis à billes-pince).

5.1.2 Lame d'aiguilles

La lame d'aiguilles est composée de deux rails inter-connectés. Selon [14], la lame d'aiguilles peut être ainsi divisée en segments, chacun modélisé comme un élément de poutre avec des paramètres de masse, de raideur et d'amortissement spécifiques. Chaque élément est constitué d'une paire de nœuds, correspondant au jonction avec les aiguilles. Dans notre simulation, la lame d'aiguilles est composée de N segments et de N paires de nœuds. Cependant, la force de l'actionneur applique seulement au $c^{ème}$ emplacement de nœuds. Le comportement dynamique de la lame d'aiguilles peut être décrit par la représentation d'états suivante :

$$\begin{aligned} \dot{x}_s(t) &= A_s x_s(t) + B_s u_s(t) \\ y_s(t) &= C_s x_s(t) \end{aligned} \tag{7}$$

avec $x_s(t) = [x_1(t), \dot{x}_1(t), x_2(t), \dot{x}_2(t)]^\top$ ($x_1 \in \mathbb{R}^{N\times 1}, \dot{x}_1(t) \in \mathbb{R}^{N\times 1}, x_2(t) \in \mathbb{R}^{N\times 1}, \dot{x}_2(t) \in \mathbb{R}^{N\times 1}$) où $\dot{x}_1(t)$ [m.s^{-1}], $x_1(t)$ [m] sont respectivement le vecteur de vitesse et de déplacement

pour chaque segment de l'aiguille 1 de la lame; $\dot{x}_2(t)$ [m.s^{-1}], $x_2(t)$ [m] sont respectivement le vecteur de vitesse et de déplacement pour chaque segment de l'aiguille 2 de la lame; $u_s(t) = [f(t), f_r(t)]^\top$ ($f(t) \in \mathbb{R}^{N\times 1}, f_r(t) \in \mathbb{R}^{N\times 1}$) avec $f(t)$ [N] la force de déplacement de lame d'aiguilles, $f_r(t)$ [N] la force de friction de la lame; et $y_s(t) = [x_1(t), \dot{x}_1(t)]^\top$. Les matrices du système (7) sont définies en (9).

$$A_s = \begin{bmatrix} \mathbf{0} & I & \mathbf{0} & \mathbf{0} \\ -M^{-1}K - M^{-1}k & M^{-1}C - M^{-1}b & M^{-1}k & M^{-1}b \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ M^{-1}k & M^{-1}b & -M^{-1}K - M^{-1}k & -M^{-1}C - M^{-1}b \end{bmatrix}, \quad (8)$$

$$B_s = \begin{bmatrix} \mathbf{0} & \mathbf{0} \\ -M^{-1} & M^{-1} \\ \mathbf{0} & \mathbf{0} \\ -M^{-1} & \mathbf{0} \end{bmatrix}, \qquad C_s = \begin{bmatrix} I & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & I & \mathbf{0} & \mathbf{0} \end{bmatrix} \quad (9)$$

A la fin du déplacement, la lame d'aiguilles entre en contact avec le rail ce qui se traduit par une saturation des déplacements des aiguilles :

$$x_1(t) = \begin{cases} 0 & \text{si } x_1(t) < 0, \\ x_1(t) & \text{si } 0 \le x_1(t) \le \bar{x}_1, \\ \bar{x}_1 & \text{si } x_1(t) > \bar{x}_1. \end{cases} \qquad x_2(t) = \begin{cases} 0 & \text{si } x_2(t) < 0, \\ x_2(t) & \text{si } 0 \le x_2(t) \le \bar{x}_1, \\ \bar{x}_1 & \text{si } x_2(t) > \bar{x}_1. \end{cases} \quad (10)$$

avec $\bar{x}_1$ le déplacement maximal de l'aiguille ($0.1m$)
Les paramètres du modèle lame d'aiguilles sont les suivants : matrice de masses M ($M \in \mathbb{R}^{N\times N}$), matrice de raideur K ($K \in \mathbb{R}^{N\times N}$), matrice d'amortissement C ($C \in \mathbb{R}^{N\times N}$), coefficient d'amortissement de ressort b (10^6 kg.s^{-1}), raideur de ressort k (10^4 N.m^{-1}). Les valeurs des matrices M, K, et C sont données dans [14].

5.1.3 Appareil de voie (AdV)

Après avoir établit le comportement dynamique de l'EMA et de la lame d'aiguilles, le modèle de l'AdV peut être établit en inter-connectant les deux modèles. La tension $v(t)$ appliquée au moteur de l'EMA est reçu d'un contrôleur lorsque le déplacement de la lame d'aiguilles est demandé. La force de friction appliquée à la lame d'aiguilles $f(t)$ dépend de la force délivrée par l'actionneur $f_a(t)$. Lorsque cette dernière est supérieure à la constante de force de friction F_f (2.3996×10^3 N), la lame est alors soumise à la force de friction $f(t)$.

$$f(t) = \begin{cases} 0 & \text{si } F_f - f_a(t) \ge 0, \\ F_f & \text{sinon.} \end{cases} \quad (11)$$

Similairement, la force de déplacement de la lame $f_r(t)$ dépend de la force délivrée par l'actionneur $f_a(t)$. Lorsque cette dernière est supérieure à la constante de force de friction F_f, la lame est alors soumise à la force délivrée par l'actionneur $f_a(t)$. Pour rappel, la lame d'aiguilles est composé de N segments et donc de N paires de noeuds (un noeud sur chaque aiguille).

$$f_r(t) = \begin{cases} 0 & \text{si } F_f - f_a(t) \ge 0, \\ Sf_a(t) & \text{sinon.} \end{cases} \quad (12)$$

avec S ($S \in \mathbb{R}^{N\times 1}$) un vecteur de sélection pour sélectionner le noeud sur lequel est appliqué la force de l'actionneur.
Lorsque les aiguilles entrent en contact avec le rail (correspondant au déplacement maximal $\bar{x}_1$), une force de contact $f_s(t)$ apparaît:

$$f_s(t) = \begin{cases} 0 & \text{si } x_1(t) - \bar{x}_1 < 0, \\ K_r(x_1(t) - \bar{x}_1) + C_r\dot{x}_1(t) & \text{sinon.} \end{cases} \tag{13}$$

Dernièrement, la vitesse et le déplacement du noeud où la force de l'actionneur est appliquée sont définies ci-après:

$$x_l(t) = S^\top x_1(t), \qquad \dot{x}_l(t) = S^\top \dot{x}_1(t) \tag{14}$$

Après avoir décrit le comportement dynamique de l'AdV, le reste de la section s'intéressent à plusieurs défaillances présentes dans les AdVs.

5.2 Modèle des défaillances

Afin de compléter notre simulateur, nous introduisons différentes défaillances présentes dans la littérature [17].

- (D1) Défaillance de moteur : la dégradation du commutateur peut se modéliser par une augmentation de la résistance du moteur ($R_m = 12,5$),
- (D2) Défaillance de la lame d'aiguilles : la rupture de la pince peut se modéliser par la non connexion entre le modèle de l'EMA et de la lame d'aiguilles ($f_a(t) = 0 \,\forall\, t$),
- (D3) Présence d'un obstacle : le déplacement de la lame d'aiguilles est bloqué par un obstacle ($\bar{x}_1 = 0.05m$).
- (D4) Bruit dans la mesure : présence de bruit blanc dans les mesures du courant $i_m(t)$.

6 Application

Une application de la méthode proposée a été réalisée sur des données de courant issue du simulateur développé de l'AdV. La première étape d'analyse sémantique a été effectuée pour identifier les similitudes entre toutes les données afin de distinguer les différentes formes de courbes de courant. Pour ce faire, la méthode de clustering k-Means a été employée en utilisant l'environnement Scikit-learn 5 clusters sont identifiés qui représentent 5 classes de profils de courbes de courant. Ces résultats correspondent parfaitement avec ce qui était généré par le simulateur, à savoir trois types de pannes de l'AdV, un comportement parfaitement normal et un comportement qui représente une dégradation du système. Pour cette étape, seuls les comportements normaux ou de panne sont considérés. Nous avons donc considéré le comportement de dégradation comme type de défaillance.

Les résultats de l'analyse sémantique servent à entraîner un modèle de classification basé sur l'algorithme KNN. Avec ce modèle, toute nouvelle donnée de courant est classée en événement, qu'il s'agisse d'un fonctionnement normal ou d'une panne.

Après avoir déterminé l'événement selon le profil de la courbe de courant, l'évaluation de la menace est menée à l'aide de TAU : d'abord, l'estimation du niveau de menace Θ_t en se basant sur la surveillance du temps de l'apparition de la manœuvre d'aiguillage et Θ_s selon le nombre

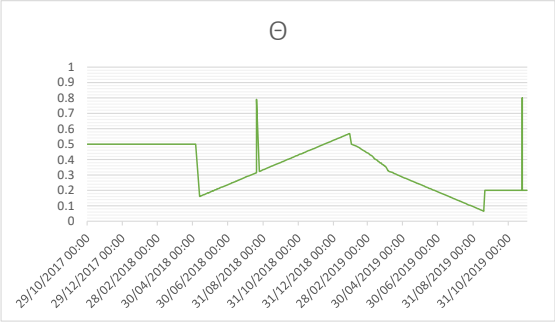


Figure 6: L'estimation globale de la menace.

des manœuvres effectuées depuis l'installation de l'AdV, ensuite définir l'indicateur global de menace Θ qui est représenté dans la Figure 6.

Juste après le début de la période de vie utile, le TAU a détecté des courbes de comportement normales, ce qui a entraîné une faible estimation de la menace. Au fil du temps, une forte estimation de menace est soudainement détectée en raison de la présence de courbe de défaillance pendant la période utile de l'AdV. À l'approche de la période d'usure, l'évaluation de la menace diminue progressivement, car le TAU identifie des courbes de défaillances, ce qui est probable en raison de l'usure de l'AdV. Cependant, une estimation élevée est observée vers la fin de cette période, en raison de la détection d'un comportement normal de l'AdV, qui se rapproche de la fin de sa durée de vie.

Afin d'évaluer les résultats, il faut d'abord souligner que l'approche proposée n'est pas en mesure de fournir une estimation de menace pendant la période de rodage. Néanmoins, si l'attaquant envoie une courbe de défaillance au début de la période de vie utile, le TAU fournira une estimation de menace élevée, et pour améliorer la fiabilité de cette estimation, des études supplémentaires doivent être menées afin de déterminer le type de défaillance détectée et ses conséquences sur le comportement de l'appareil ainsi que sa fréquence d'apparition. Au fur et à mesure que le temps passe, les courbes de défaillance sont plus en plus probables, donc le TAU pourrait détecter uniquement des attaques qui imitent un comportement parfait de l'AdV et non pas un comportement lié au vieillissement. Cela est dû au fait que, dans cette étude, nous n'avons pas pris en considération le vieillissement normal de l'AdV qui, dans notre cas, a été considéré comme une défaillance.

7 Conclusion

L'article propose un nouveau paradigme pour l'évaluation des cyberattaques pesant sur les données de surveillance des AdV. L'objectif est de détecter les cyberattaques qui visent soit à rendre difficile les décisions de maintenance en dissimulant une panne, soit à déclencher des actions de maintenance inutiles en reproduisant le comportement d'une panne. L'approche est fondée sur l'analyse des profils de courbes de courant générés pendant les manœuvres d'aiguillage et projeter ces informations dans le cycle de vie d'un AdV, compte tenu des critères de vieillissement temporel et opérationnel afin de contextualiser la probabilité de cyberattaque.

Le paradigme proposé constitue une preuve de concept, reposant sur les techniques de traitement des données les plus courantes et les plus faciles à appliquer, ainsi que sur une logique simple d'estimation du niveau de menace. Les perspectives seront de proposer des améliorations en ce sens : l'analyse sémantique peut être améliorée ou consolidée par une étude approfondie des méthodes de clustering les plus performantes; la même chose peut être faite pour l'étape de modélisation des données. Quant à l'estimation du niveau de menace, l'analyse de séquences de courbes dans le temps semble prometteuse.

8 Acknowledgments

Le projet RailMon est financé par le gouvernement Français et BPI France dans le cadre du Programme d'Investissements d'Avenir.

References

[1] C. Basile, M. Gupta, Z. Kalbarczyk, and R.K. Iyer. An Approach for Detecting and Distinguishing Errors versus Attacks in Sensor Networks. In *International Conference on Dependable Systems and Networks (DSN'06)*, pages 473–484, Philadelphia, PA, USA, 2006. IEEE.

[2] Amaury Beaudet, Cédric Escudero, and Éric Zamaï. Malicious Anomaly Detection Approaches Robustness in Manufacturing ICSs. *IFAC-PapersOnLine*, 54(1):146–151, 2021.

[3] Anatolij Bezemskij, George Loukas, Diane Gan, and Richard J. Anthony. Detecting Cyber-Physical Threats in an Autonomous Robotic Vehicle Using Bayesian Networks. In *2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pages 98–103, Exeter, June 2017. IEEE.

[4] Raymond C. Borges Hink, Justin M. Beaver, Mark A. Buckner, Tommy Morris, Uttam Adhikari, and Shengyi Pan. Machine learning for power system disturbance and cyber-attack discrimination. In *2014 7th International Symposium on Resilient Control Systems (ISRCS)*, pages 1–8, Denver, CO, USA, August 2014. IEEE.

[5] Binbin Chen, Christoph Schmittner, Zhendong Ma, William G. Temple, Xinshu Dong, Douglas L. Jones, and William H. Sanders. Security Analysis of Urban Railway Systems: The Need for a Cyber-Physical Perspective. In *Computer Safety, Reliability, and Security*, volume 9338, pages 277–290. Springer International Publishing, Cham, 2015. Series Title: Lecture Notes in Computer Science.

[6] Ruifeng Duo, Xiaobo Nie, Ning Yang, Chuan Yue, and Yongxiang Wang. Anomaly Detection and Attack Classification for Train Real-Time Ethernet. *IEEE Access*, 9:22528–22541, 2021.

[7] Mariam Elnour, Nader Meskin, Khaled Khan, and Raj Jain. A Dual-Isolation-Forests-Based Attack Detection Framework for Industrial Control Systems. *IEEE Access*, 8:36639–36651, 2020. Conference Name: IEEE Access.

[8] Cedric Escudero, Franck Sicard, and Eric Zamai. Process-Aware Model based IDSs for Industrial Control Systems Cybersecurity: Approaches, Limits and Further Research. *23rd International Conference on Emerging Technologies and Factory Automation, ETFA - Torino, Italy (2018.9.4-2018.9.7)*, pages 605–612, 2018. Publisher: IEEE ISBN: 9781538671085.

[9] Shize Huang, Fan Zhang, Rongjie Yu, Wei Chen, Fei Hu, and Decun Dong. Turnout Fault Diagnosis through Dynamic Time Warping and Signal Normalization. *Journal of Advanced Transportation*, 2017:1–8, 2017.

[10] Mohamad Kaouk, Jean-Marie Flaus, Marie-Laure Potet, and Roland Groz. A Review of Intrusion Detection Systems for Industrial Control Systems. In *2019 6th International Conference on Control, Decision and Information Technologies (CoDIT)*, pages 1699–1704, Paris, France, April 2019. IEEE.

[11] Mojtaba Kordestani and Mehrdad Saif. Observer-Based Attack Detection and Mitigation for Cyberphysical Systems: A Review. *IEEE Systems, Man, and Cybernetics Magazine*, 7(2):35–60, April 2021.

[12] Mehmet Necip Kurt, Oyetunji Ogundijo, Chong Li, and Xiaodong Wang. Online Cyber-Attack Detection in Smart Grid: A Reinforcement Learning Approach. *IEEE Transactions on Smart Grid*, 10(5):5174–5185, September 2019.

[13] Subhash Lakshminarayana, Teo Zhan Teng, Rui Tan, and David K. Y. Yau. Modeling and Detecting False Data Injection Attacks against Railway Traction Power Systems. *ACM Transactions on Cyber-Physical Systems*, 2(4):1–29, September 2018.

[14] Linxiao Li, Saikat Dutta, Roger Dixon, and Edward Stewart. Railway track switch simulation: a new dynamic model for studying actuator and switch blade dynamics. *Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit*, page 095440972211417, November 2022.

[15] Fei Tony Liu, Kai Ming Ting, and Zhi-Hua Zhou. Isolation-Based Anomaly Detection. *ACM Transactions on Knowledge Discovery from Data*, 6(1):1–39, March 2012.

[16] Leandros A. Maglaras and Jianmin Jiang. Intrusion detection in SCADA systems using machine learning techniques. In *2014 Science and Information Conference*, pages 626–631, London, UK, August 2014. IEEE.

[17] Fausto Pedro Garcia Marquez, Paul Weston, and Clive Roberts. Failure analysis and diagnostics for railway trackside equipment. *Engineering Failure Analysis*, 14(8):1411–1426, December 2007.

[18] Stefano Marrone, Ricardo J. Rodríguez, Roberto Nardone, Francesco Flammini, and Valeria Vittorini. On synergies of cyber and physical security modelling in vulnerability assessment of railway systems. *Computers & Electrical Engineering*, 47:275–285, October 2015.

[19] Sohrab Mokhtari, Alireza Abbaspour, Kang K. Yen, and Arman Sargolzaei. A Machine Learning Approach for Anomaly Detection in Industrial Control Systems Based on Measurement Data. *Electronics*, 10(4):407, February 2021.

[20] Dongxiu Ou, Rui Xue, and Ke Cui. A Data-Driven Fault Diagnosis Method for Railway Turnouts. *Transportation Research Record: Journal of the Transportation Research Board*, 2673(4):448–457, April 2019.

[21] Marvin Rausand and Arnljot Høyland. *System reliability theory: models, statistical methods, and applications*. Wiley series in probability and statistics. Wiley-Interscience, Hoboken, NJ, 2nd ed edition, 2004.

[22] Mouna Rekik, Christophe Gransart, and Marion Berbineau. Cyber-Physical Security Risk Assessment for Train Control and Monitoring Systems. In *2018 IEEE Conference on Communications and Network Security (CNS)*, pages 1–9, Beijing, May 2018. IEEE.

[23] Reuters. Danish train standstill on Saturday caused by cyber attack. https://www.reuters.com/technology/danish-train-standstill-saturday-caused-by-cyber-attack-2022-11-03/, November 2022.

[24] Andrew Roth. 'Cyberpartisans' hack Belarusian railway to disrupt Russian buildup. https://www.theguardian.com/world/2022/jan/25/cyberpartisans-hack-belarusian-railway-to-disrupt-russian-buildup, January 2022.

[25] Josephine Cordero Sapién. Global Cyber Attack Hits Deutsche Bahn. https://railway-news.com/global-cyber-attack-hits-deutsche-bahn/, May 2017.

[26] Franck Sicard, Cédric Escudero, Éric Zamaï, and Jean-Marie Flaus. From ICS Attacks' Analysis to the S.A.F.E. Approach: Implementation of Filters based on Behavioral Models and Critical State Distance for ICS Cybersecurity. In *2nd Cyber Security In Networking Conference*, 2nd Cyber Security In Networking Conference (CSNet'18) Proceedings, page 8, Paris, France, October 2018. IEEE.

[27] Denis Ulybyshev, Ibrahim Yilmaz, Bradley Northern, Vadim Kholodilo, and Michael Rogers. Trustworthy Data Analysis and Sensor Data Protection in Cyber-Physical Systems. In *Proceedings of the 2021 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems*, pages 13–22, Virtual Event USA, April 2021. ACM.

[28] Buyeon Yu and Yongsoon Eun. Sensor attack detection for railway vehicles using topographic information. In *2017 17th International Conference on Control, Automation and Systems (ICCAS)*, pages 149–154, Jeju, October 2017. IEEE.