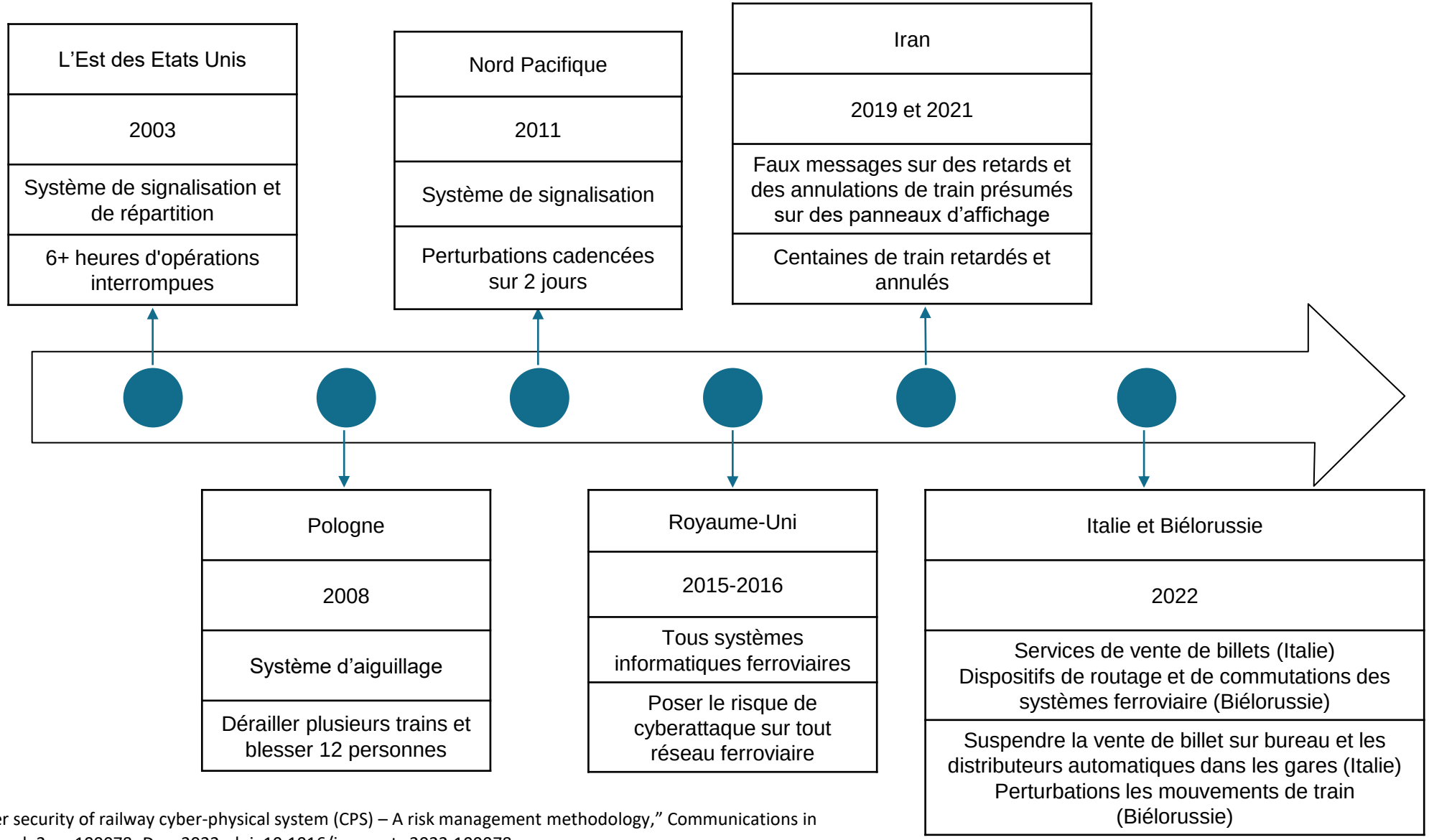
Émulation automatisée d'adversaires pour le système de surveillance ferroviaire via l'Apprentissage par Renforcement

Dinh Duy Kha NGUYEN,[*] *Cédric ESCUDERO*,[*] *Emil DUMITRESCU*,[*] *Eric ZAMAÏ*[*]

dinh-duy-kha.nguyen@insa-lyon.fr

[*] *Laboratoire Ampère CNRS, INSA Lyon, Université de Lyon, 69621 Villeurbanne CEDEX, France*

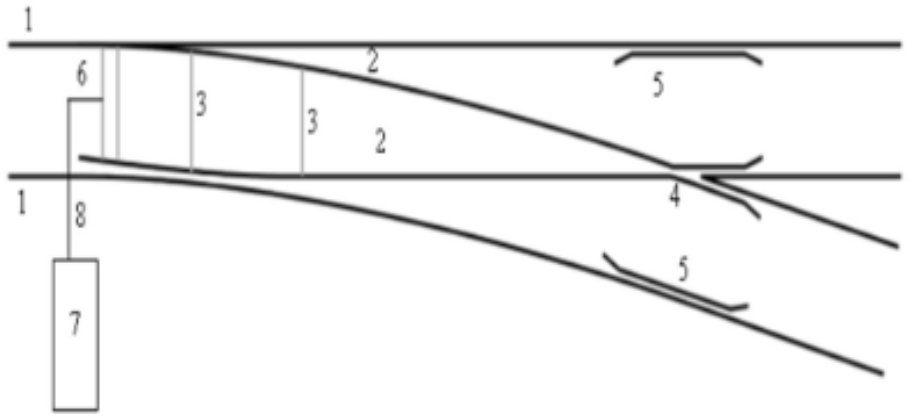
Attaques passées dans le système ferroviaire



Z. Wang and X. Liu, "Cyber security of railway cyber-physical system (CPS) – A risk management methodology," Communications in Transportation Research, vol. 2, p. 100078, Dec. 2022, doi: 10.1016/j.commtr.2022.100078.

Système physique étudié

- ✓ Système d'aiguillage (Switching & Crossing System ou Turnouts) : système mécanique électrique ou hydraulique installé sur la voie, permettant aux véhicules ferroviaires de passer d'un itinéraire à un autre, offrant la flexibilité au réseau ferroviaire.
  - Un système complexe avec grand nombre de composants et différents types de technologies.
  - Vulnérables aux pannes et aux dysfonctionnements entraînées des retards et des accidents mortels.
- ✓ Composants de système: 1. rails de stock, 2. rails d'aiguillage, 3. barres de civière, 4. croisement commun, 5. rails de contrôle, 6. pince, 7. équipement d'exploitation ponctuel (POE), 8. actionneur.



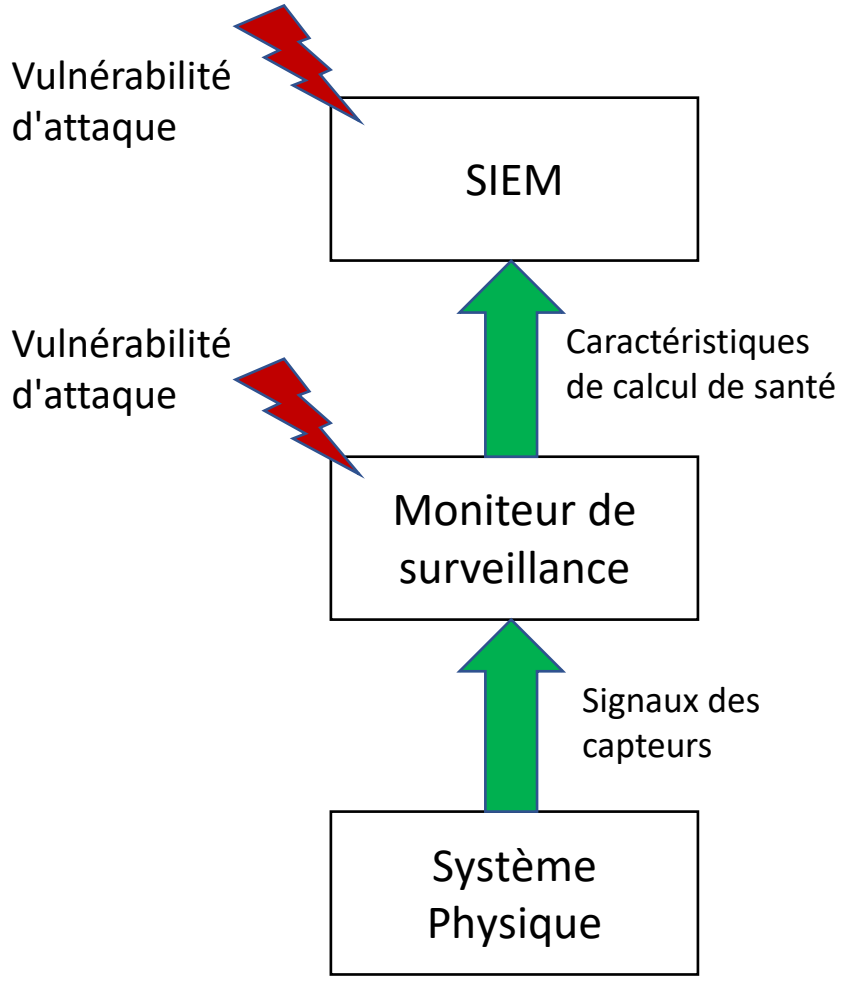
[1] M. Hamadache, S. Dutta, R. Ambur, O. Olaby, E. Stewart, and R. Dixon, "Residual-based Fault Detection Method: Application to Railway Switch & Crossing (S&C) System," in *2019 19th International Conference on Control, Automation and Systems (ICCAS)*, Jeju, Korea (South), Oct. 2019, pp. 1228–1233. doi: 10.23919/ICCAS47443.2019.8971747.

Système de Surveillance

- ✓ Des équipements de surveillance recueillant les signaux de capteurs mesurant les grandeurs physiques du système.
- ✓ Un système de gestion des informations et des événements de sécurité (SIEM) remontant les informations collectées par les équipements de surveillance afin de calculer l'état de santé des composants.

BUT :

- ❑ Planifier les maintenances
- ❑ Garantir la disponibilité de réseau ferroviaire



Type d’attaques

- ✓ Définition 1 (Cacher des maintenances) Les informations contenues dans les équipements de surveillances sont modifiées afin de maintenir l’état de santé dans le SIEM en-dessous des seuils de déclenchement d’alarmes.

- ✓ Définition 2 (Déclencher prématurément des maintenances) Les informations contenues dans les équipements de surveillances sont modifiées afin de maintenir l’état de santé dans le SIEM au-dessus des seuils de déclenchement d’alarmes.

Méthode proposée

- ❑ Entrainer un agent d'attaque pour modifier des valeurs de mesure en fonction de différents types d'attaque à l'aide de l'Apprentissage par Renforcement.

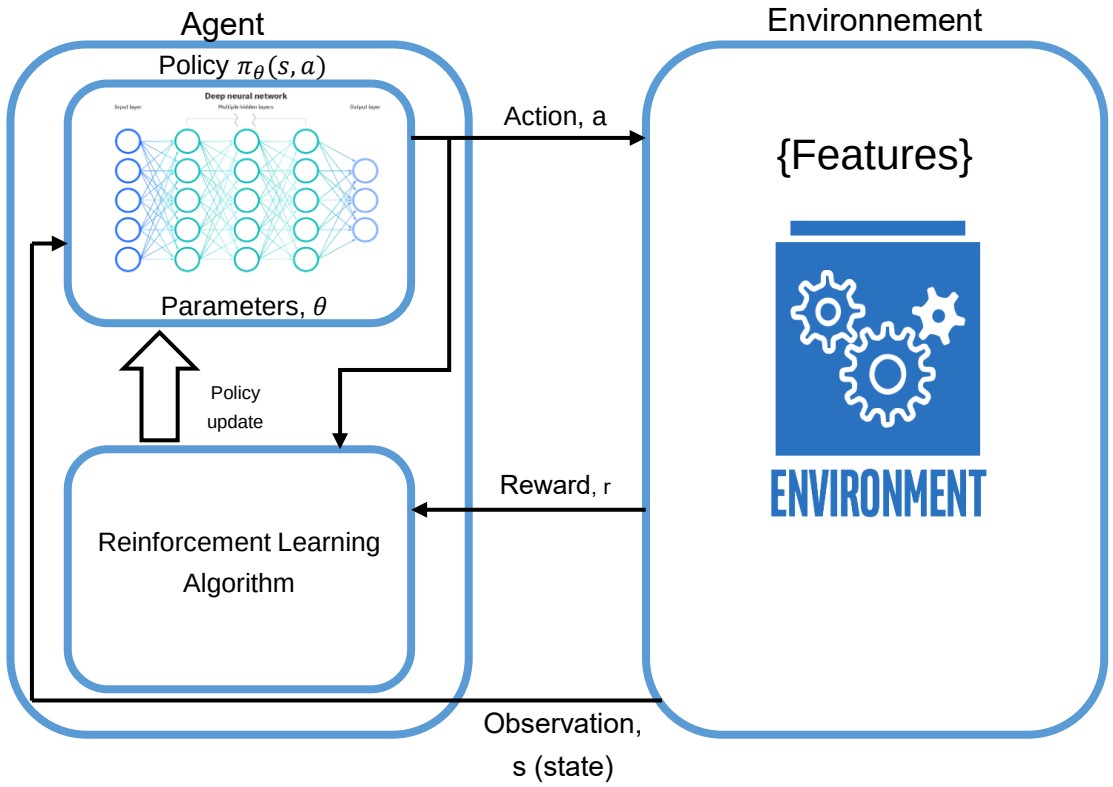
- ❑ Contribuer plusieurs types de la stratégie de l'attaquant basée sur l'émulation d'attaque de l'agent.

- ❑ Comparer la trajectoire suivie par le système de surveillance avec la stratégie de l'agent d'attaque.

- ➢ Comment distinguer chaque type d'attaque?

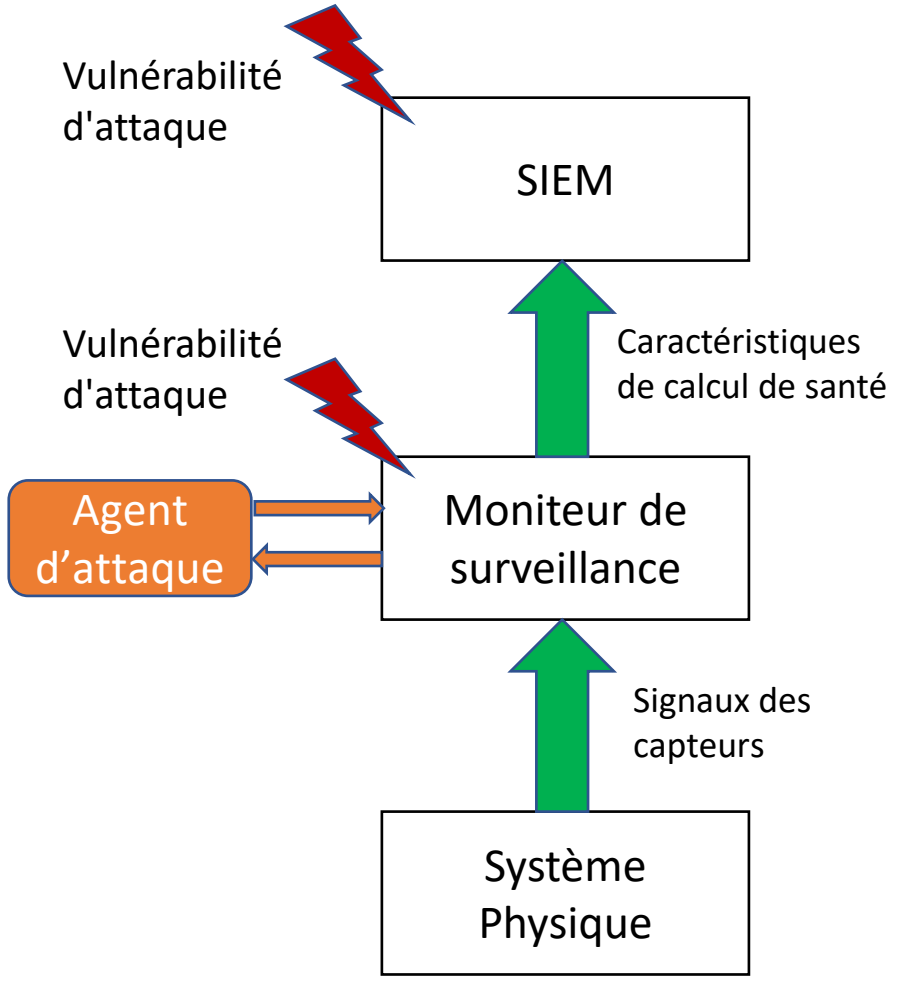
Agent d'attaque

- Méthode : L'Apprentissage par Renforcement.
- Processus de Décision de Markov : $< S, A, P_a, R_a, \gamma >$
  - S : l'ensemble des états du système physique.
  - A : l'ensemble des actions décidé par l'agent.
  - $P_a(s, s')$: la probabilité que l'action a soit effectuée à l'état s et conduise à l'état s'.
  - $R_a(s, s')$: la récompense instantanée reçue par l'agent après avoir effectué l'action a.
  - $\gamma \in [0, 1]$: le facteur de remise.

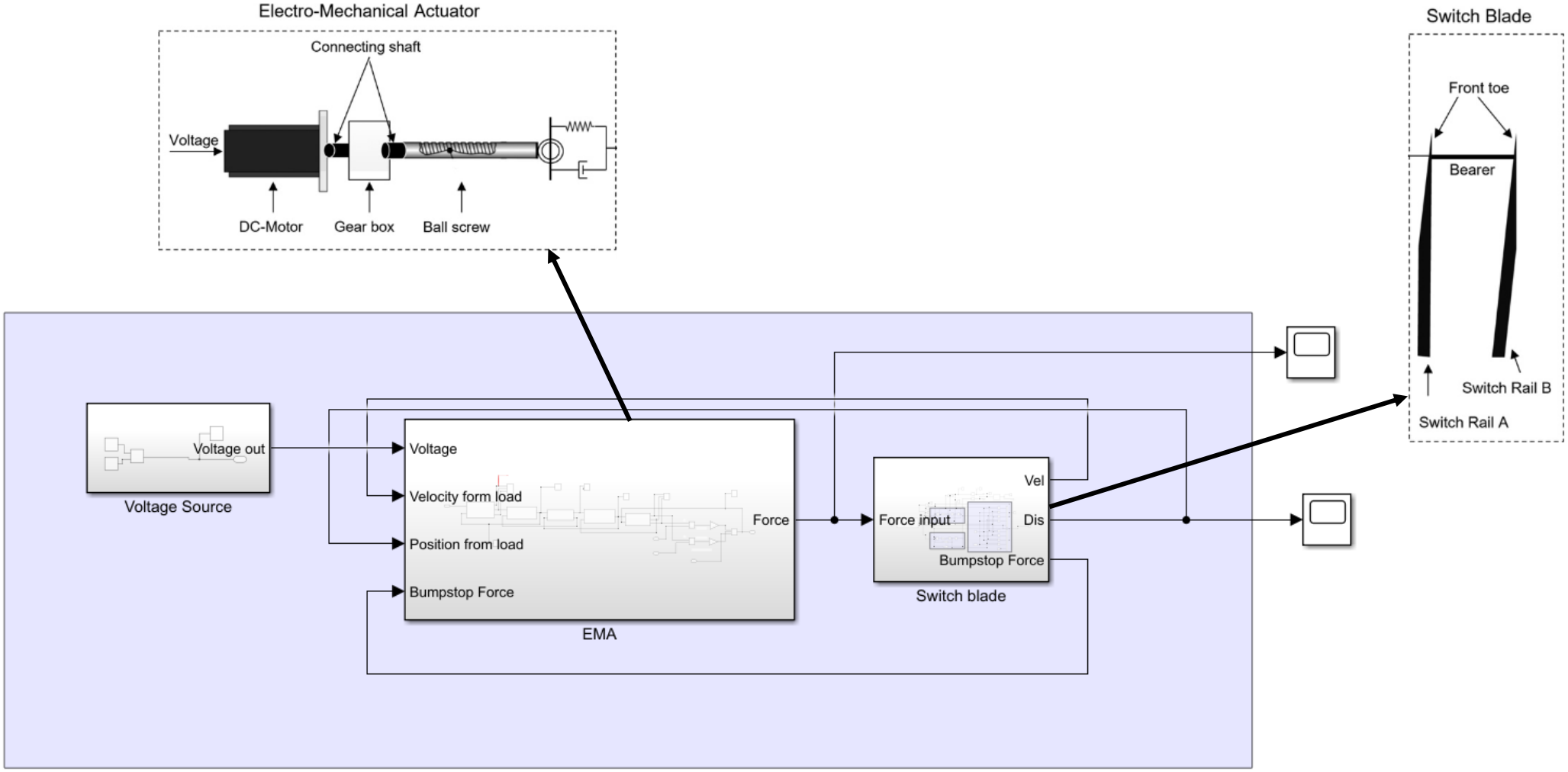


Agent d’attaque

- ✓ A détermineront comment est la stratégie de l’attaque.
- ✓ $R_a(s, s')$
  - Récompense positive pour les attaques exécutées avec succès et non détectées
  - Récompense négative pour les attaques qui échouent ou sont détectées.
- ✓ Une politique $\pi(\mathrm{a} \mid \mathrm{s})$ est une distribution de probabilité qui associe l’état actuel à la possibilité de sélectionner une action spécifique.
- ✓ La fonction de valeur $V_\pi(s) = \mathbb{E}[\sum_t^{T\infty} \gamma^t R_t | s_0 = s]$ représente le retour de récompense attendu à partir de l’état s.
- ✓ Un agent d’attaque vise à apprendre une politique de décision $\pi(\mathrm{a} \mid \mathrm{s})$ qui maximise la récompense future accumulée $\sum_t^{T\infty} \gamma^t R_t$.



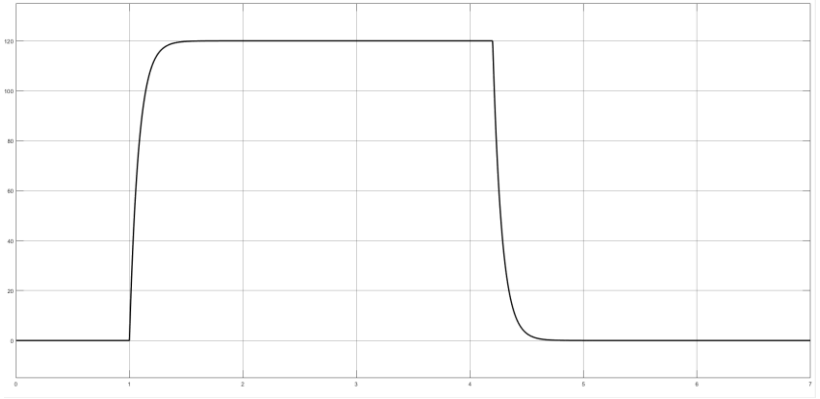
Simulation de système



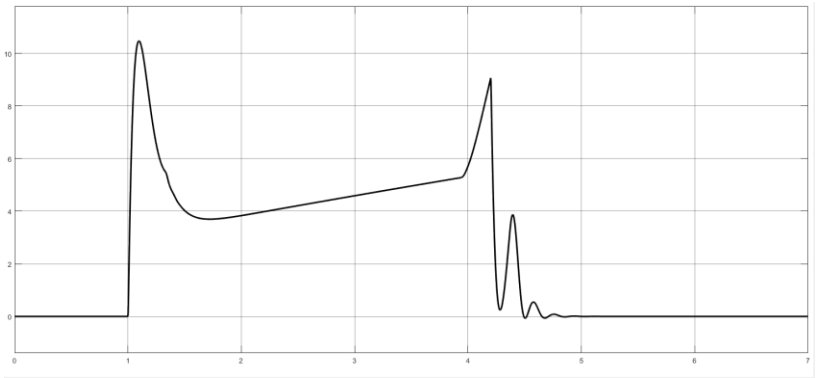
Modèle de système physique en Matlab

Simulation de système

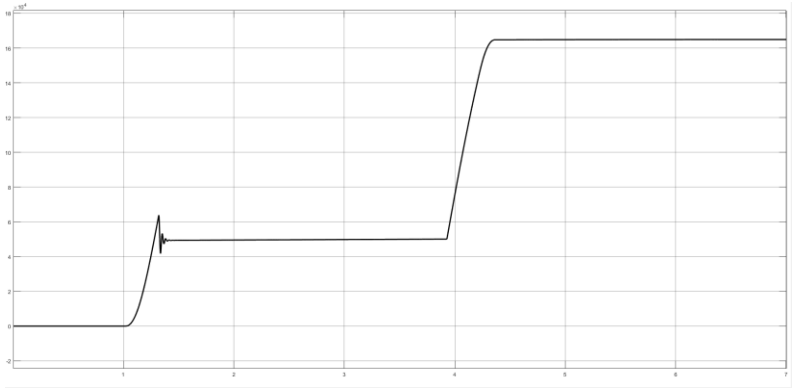
- ✓ Modéliser le modèle de système physique.
  - ➢ Récupéré les courbes des caractéristiques de système.



Tension (Signal de contrôle)



Courant (Valeur de mesure)



Force de l’actionneur (Valeur de mesure)

Conclusion…

- Idée:
  - Modéliser la conception d'agent d'attaques à l'aide de l'Apprentissage par Renforcement, et puis comparer la trajectoire suivie par le système de surveillance avec la stratégie de l'attaquant.
  - Contribuer plusieurs cas d'étude de l'attaquant.

- Travaux dans le futur:
  - Implémentation de l'agent d'attaque au modèle de système d'aiguillage ferroviaire.
  - Simulation des résultats.
  - Développer une conception de détection des cyber-attaques basée sur l'agent d'attaque.