Setting the Standard for Automation™

ISA France

Cybersécurité dans l'industrie du futur

IDS (Intrusion Detection System) basé sur ISA95

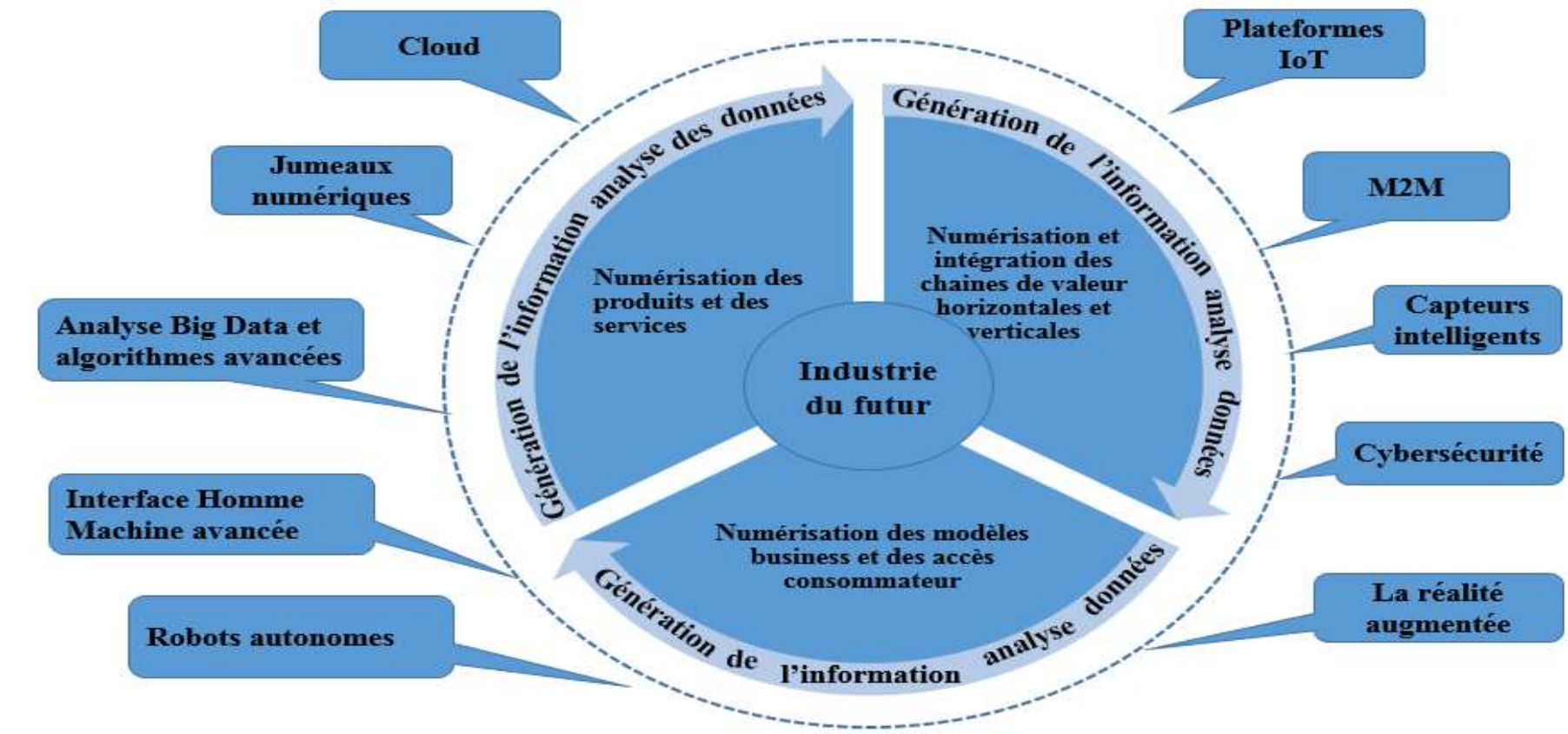
SALWA ALEM LAB-STICC Lorient/Brest

En partenariat avec

Intelligence artificielle et industrie du futur
Grenoble – 5 et 6 février 2019

Contexte des travaux de recherche

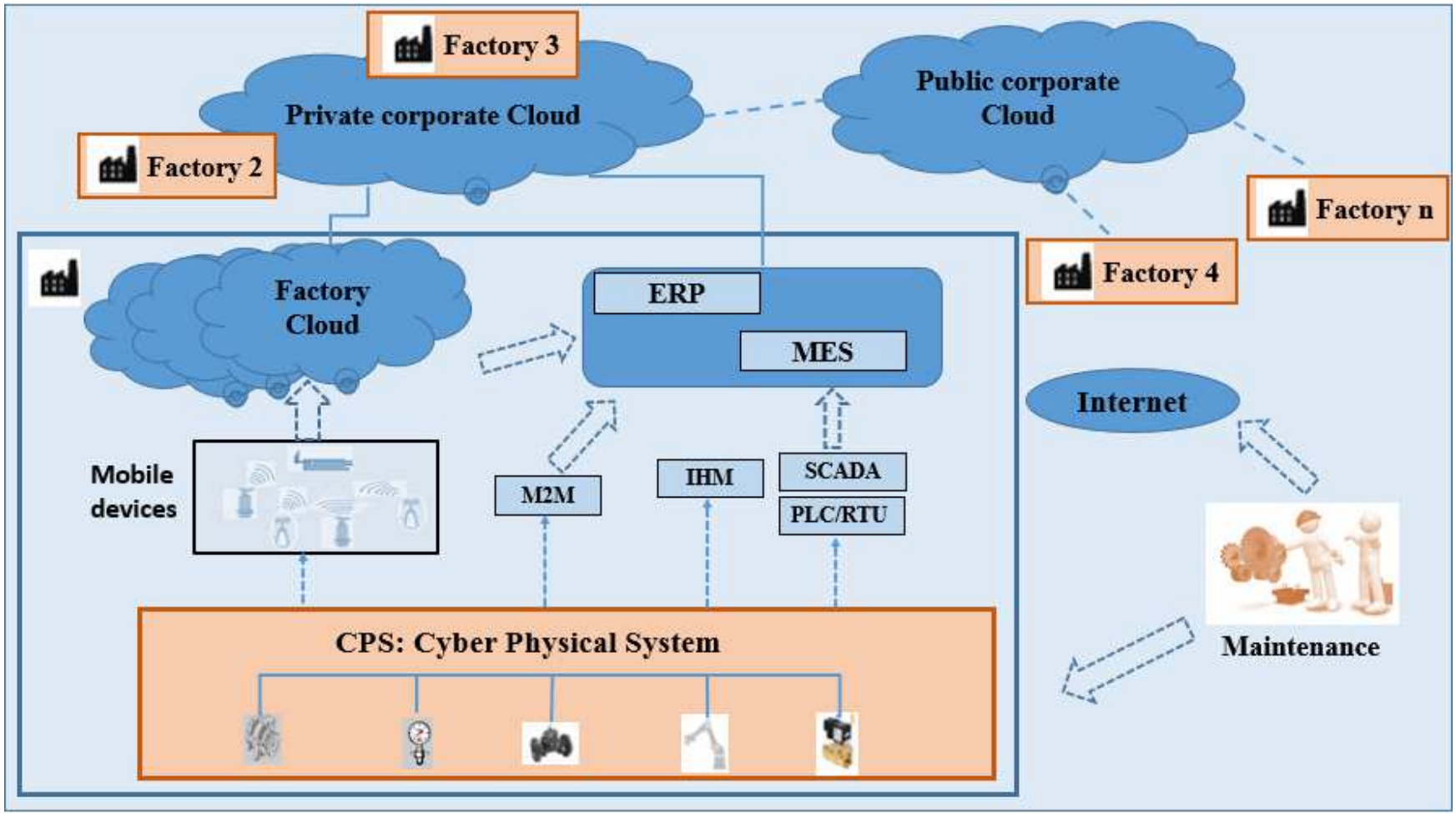
- L'industrie du futur (terminologie française) ou l'industrie 4.0 (terminologie allemande)



Contexte des travaux de recherche

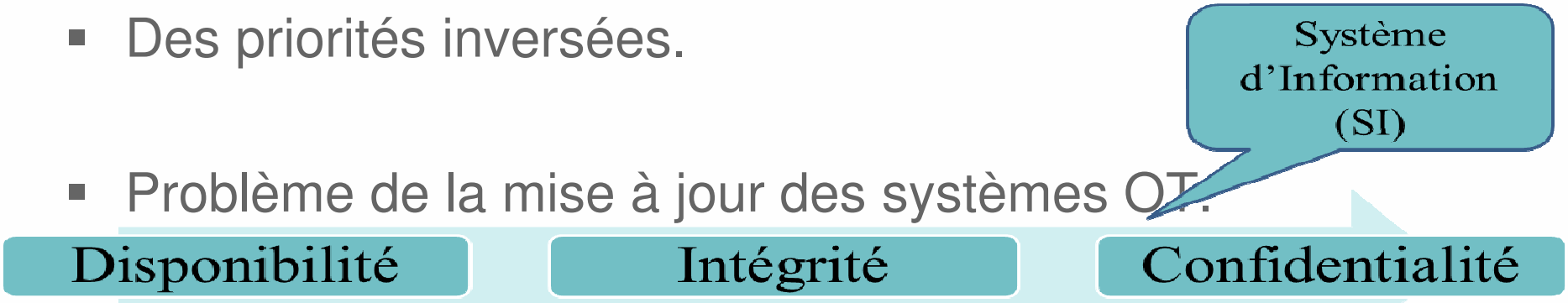
- L'industrie du futur (terminologie française) ou l'industrie 4.0 (terminologie allemande)
- Ouverture sur le monde extérieur et l'apparition de l'internet industriel ➔ Augmentation de la surface de vulnérabilité et le risque d'intrusions dans les ICS (Industrial Cyber Systems).
- La convergence IT/OT: obligation de coexister mais des challenges surgissent.
- Contraintes de temps réel, de disponibilité du matériel et d'intégrité des données.

Contexte des travaux de recherche



Problématique de sécurité dans l'industrie du futur: 1/2

- Des priorités inversées.



- Problème de la mise à jour des systèmes OT.
- Hétérogénéité des composants.
- Verticalité des composants IT/OT à sécuriser➔ Une

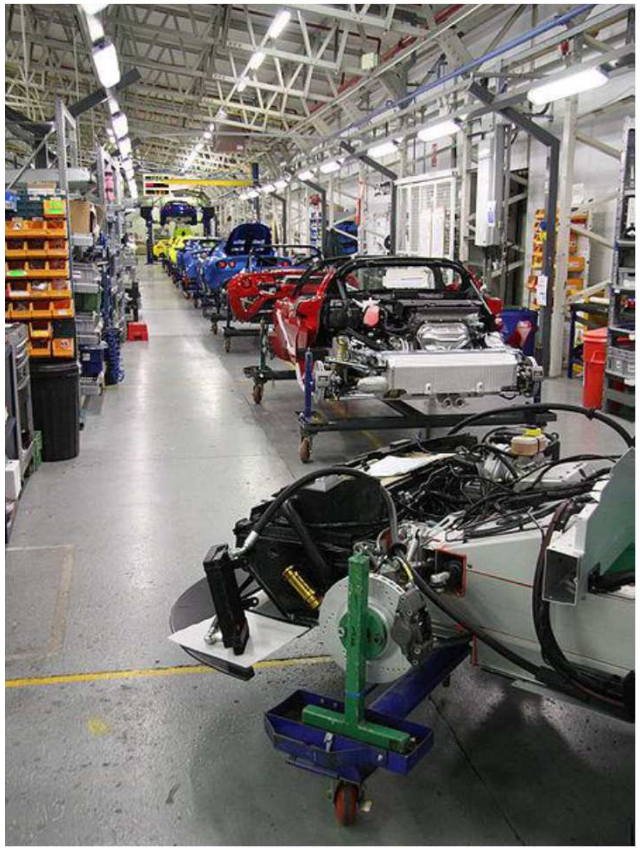
Problématique de sécurité dans l'industrie du futur: 2/2

- Les types d'attaques redoutées:

  - ✓ Des attaques qui visent la chaine de production et son intégrité.
  - ✓ Des attaques qui visent les réseaux sans fil ajoutés.
  - ✓ Des attaques liées au manque de contrôle des données et d'accès au Cloud.

➔ Aujourd'hui, un attaquant peut pénétrer à travers internet le réseau industriel qui est peu sécurisé pour empêcher l'accès au MES (intrusion par un DDoS), modifier ses données (intégrité) et usurper une identité et/ou voler un MdP.

Exemples d'attaques industrielles: DoS usine automobile (Zotob) aux USA



Impact	• 13 usines arrêtées pendant environ 1 heure, 50.000 travailleurs (14 M$ de dommages)
Scénario d'incident	• Propagation d'un ver sur la chaîne de montage
Vulnérabilité	• Manque de filtrage au niveau de l'interconnexion du réseau industriel avec le réseau bureautique

Exemples d'attaques industrielles: Prise de contrôle du système de production d'une aciérie en Allemagne

Impact	• Lourds dégâts matériels causés par la perte de contrôle des logiciels de production
Scénario d'incident	• Prise de contrôle du système de contrôle de l'usine par «spear phishing» via le réseau bureautique
Vulnérabilité	• Passerelle entre le réseau de production et le réseau bureautique

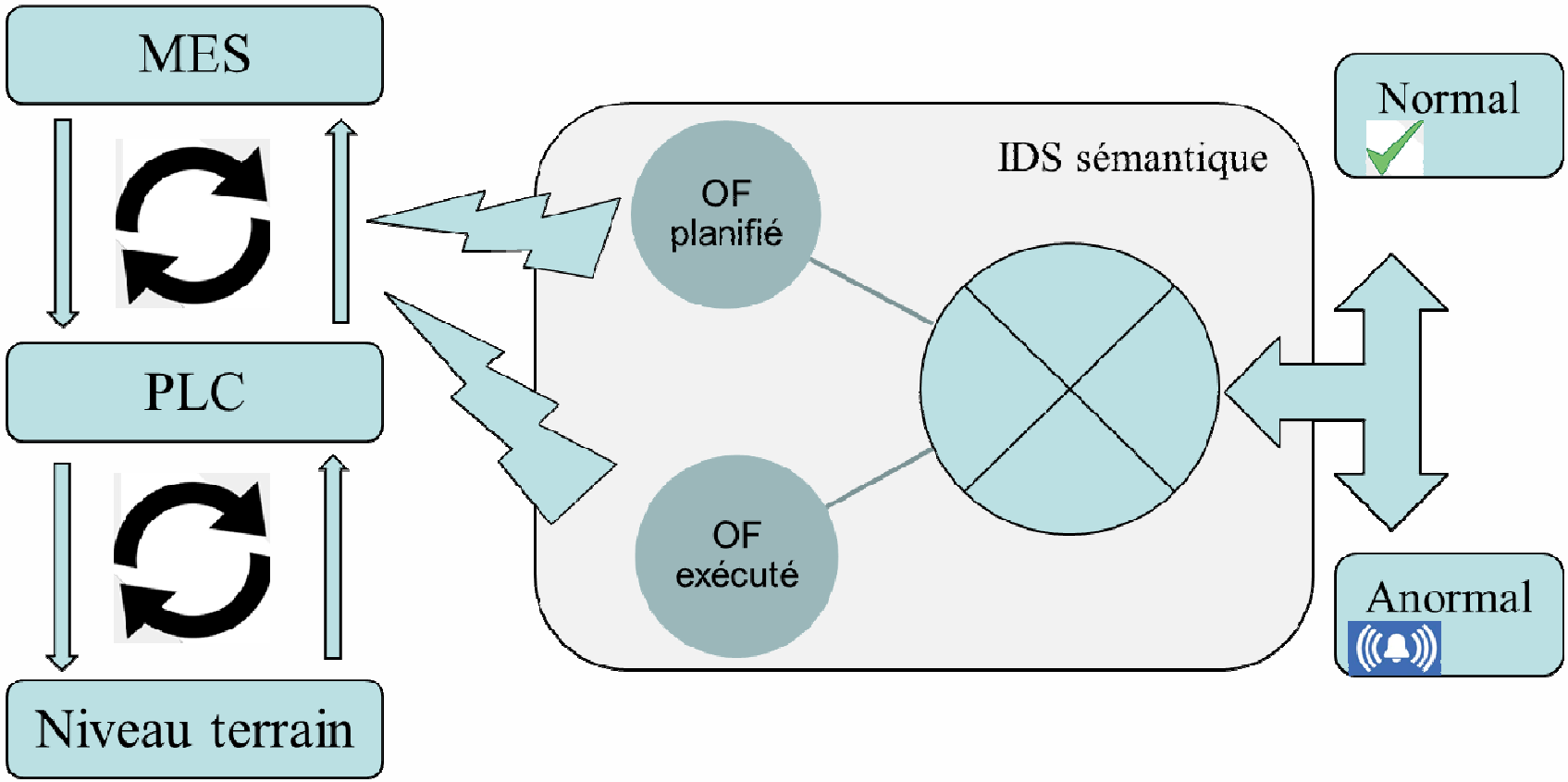
Notre contribution

- Nos travaux de recherche:
  - Se focalisent sur la réalisation d'un **IDS** (système de détection d'intrusion) **passif** dans l'industrie du futur.

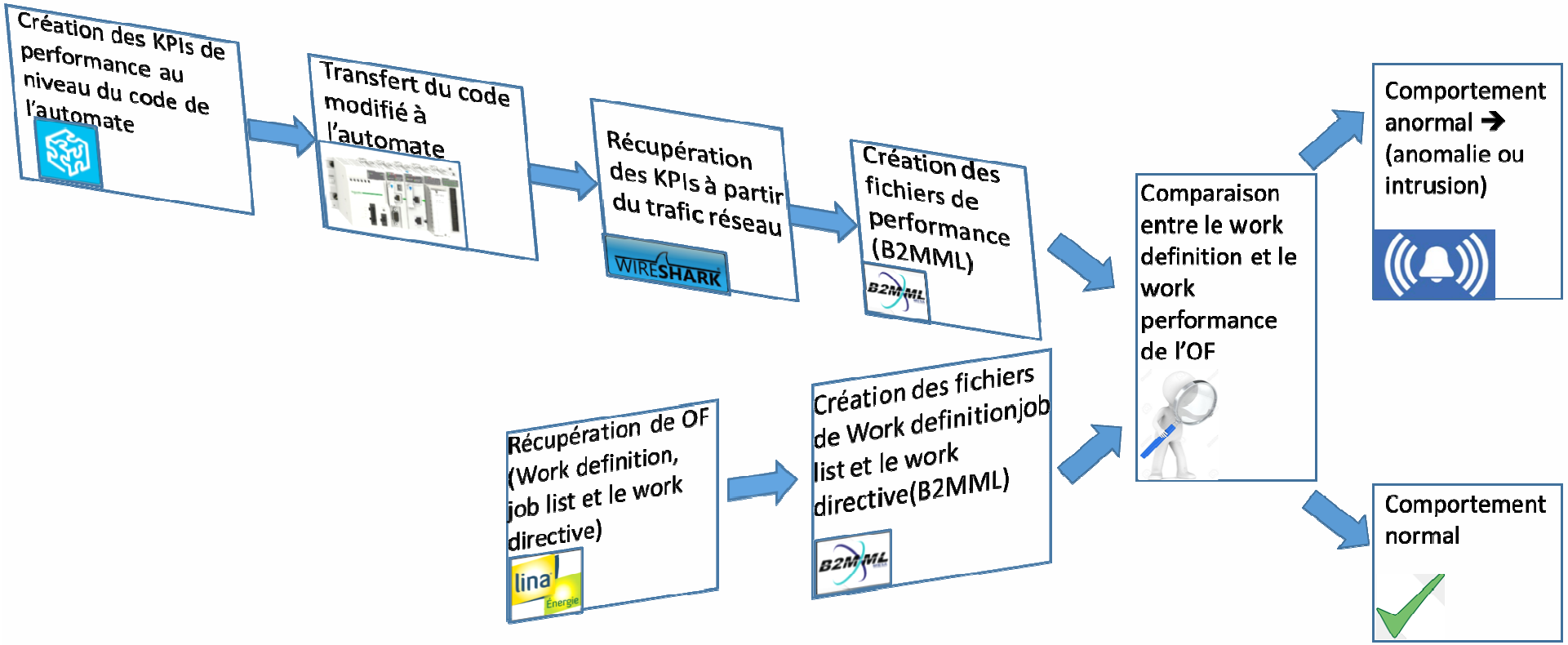
  - Se passent au niveau de l'analyse comportementale d'une chaine de production en complément avec l'analyse des appels systèmes ➔ Un IDS par spécification basé sur une norme (ISA95/IEC 62264) et un IDS comportemental (le deep learning avec le réseau de neurones).

  - Ciblent le niveau industriel MES (Manifacturing Executive System) qui représente un équipement central qui regroupe toute la vie d'un OF y compris la traçabilité.

Notre approche de détection d'intrusions: 1/3

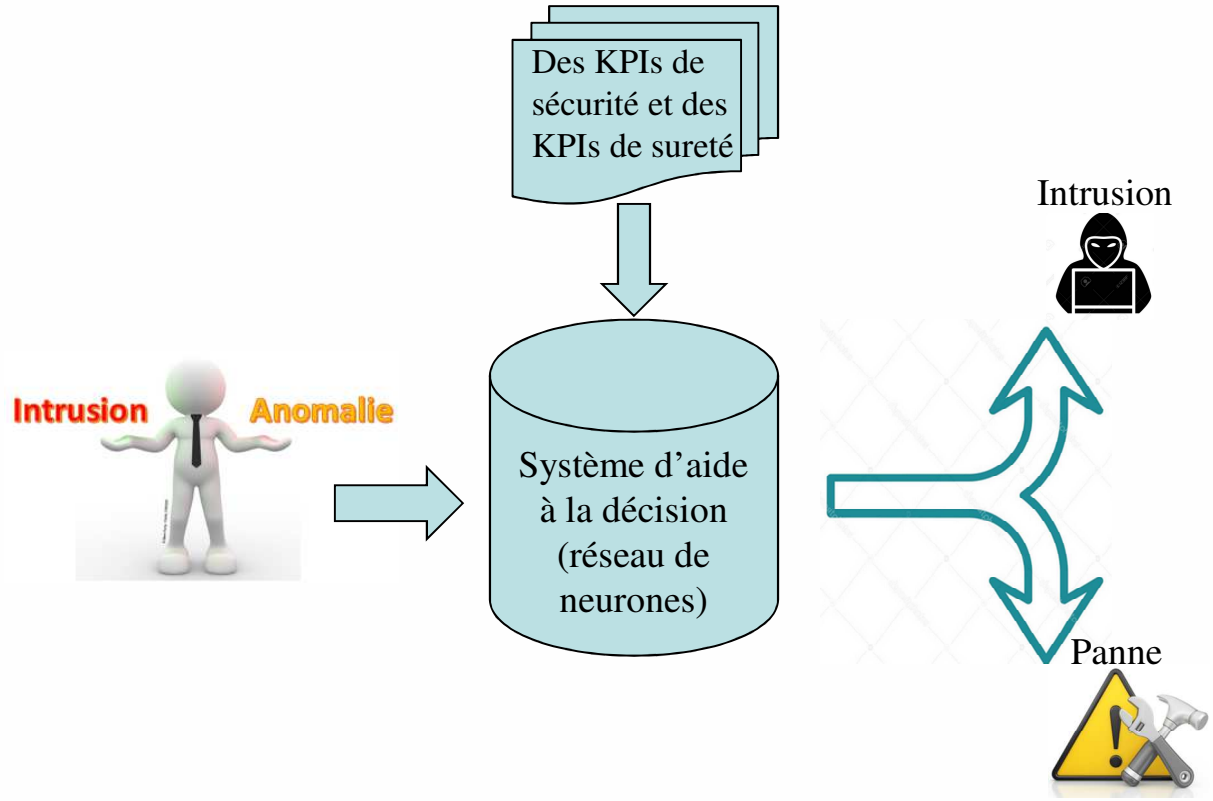


Notre approche de détection d'intrusions: 2/3



Notre approche de détection d'intrusions: 3/3

- Alimenter notre système d'aide à la décision par des KPIs de sécurité et des KPIs de sureté afin de de distinguer le type de l'anomalie



Perspectives et conclusions

- IDS sémantique basé sur le standard ISA95 et son implémentation B2MML

- Expérimentation sur un MES compatible ISA95 acheté en 2018 (COOX ordinal), avec la mise en œuvre d'une attaque typée industrielle.

- Mettre en place un IDS intelligent alimenté par deux natures de KPIs (sureté et sécurité) pour distinguer une intrusion d'une anomalie.