Démonstrateur ASSecIN: ligne industrielle virtuelle permettant l'évaluation de passerelle intelligente *

Thomas Toublanc, Sébastien Guillet, Florent de Lamotte, Pascal Berruet

Démonstrateur ASSecIN: ligne industrielle virtuelle permettant l'évaluation de passerelle intelligente *

Thomas Toublanc[1], Sébastien Guillet[1], Florent de Lamotte[1], and Pascal Berruet[1]

Université Bretagne Sud, Lorient, Bretagne, France
Prénom.Nom@univ-ubs.fr

Résumé

Nos industries sont confrontées à leur 4ème révolution. De nos jours, les menaces sur les systèmes de production industrielle ne sont plus seulement théoriques. L'attaque sur les fours d'aciérie allemande ciblant le système à travers l'intelligence du processus industriel (PI) en est le parfait exemple. ASSecIN est né de cette problématique, ce projet envisage comme solution une passerelle entre PI et les acteurs du processus industriel (PA). Cet équipement réseau intelligent met en œuvre des mécanismes de détection et de réaction aux attaques. Pour tester cette solution nous avons mis au point un démonstrateur présenté en section.1 et un cas d'usage décrit en section.2 qui relate aussi nos premiers résultats. La section.3 donne les perspectives de notre travail.

1 l'outil

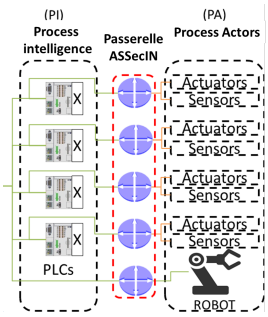

FIGURE 1 – placement de la passerelle

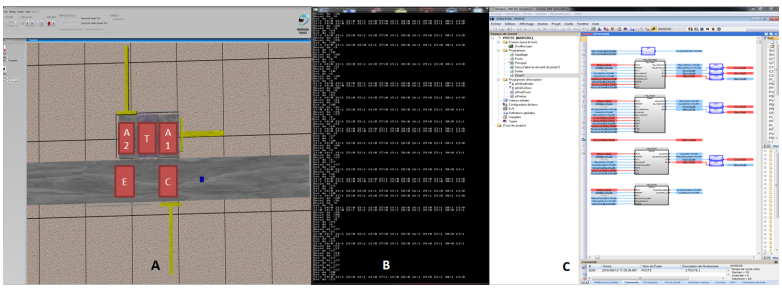

FIGURE 2 – description du démonstrateur

Le démonstrateur présenté dans ce papier a pour but d'évaluer des mécanismes de détection et de réaction, à bas niveau dans le système de contrôle commande (CC) comme schématisé dans la figure.1 en termes d'efficacité et de latence induite. Il est composé de trois parties (A,B,C) montrées dans la figue.2 : SimSED (A), un simulateur physique de partie opérative et Straton Runtime (C), qui émule un automate physique. Ces deux outils dont notre passerelle(B) est cliente communiquent à travers le protocole T5 de type client-serveur. Une chaine de transmission a donc été développée, ainsi qu'un algorithme de filtrage décrit dans [3]. Ce filtrage permet l'isolation des trames intéressantes en termes de sécurité afin d'optimiser le temps de

*d'autres personnes ont contribué à ces travaux: Romain Bévan (laboratoire Lab-STICC) et l'équipe technique de la Syleps.

communication. La passerelle permet la mise en œuvre de gardiens, qui par analyse des trames CC détectent des attaques et y réagissent en satisfaisant des objectifs de sécurité. Pour cette première version (pratiquement trois outils sont implantés sur 2 ou 3 ordinateurs), l'objectif est la sûreté de fonctionnement. On souhaite garantir que le système n'a pas d'impact néfaste sur son environnement et/ou sur lui même. Des mécanismes de réaction comme le filtrage d'ordre ou la mise en repli du système peuvent alors être sollicités. Ils interviennent après la détection instantanée de violation des contraintes logiques. D'autres travaux comme [2] font eux confiance à PI dans une certaine mesure et traitent les mêmes objectifs de sécurité, cependant ils les mettent en œuvre différemment.

2 Le cas d'usage

Notre cas d'étude test est constitué d'un poste de tri avec vérins orthogonaux commandé par PI cf. figure.2.C. Le comportement de PI est défini par trois tâches : l'interception, le transfert, et l'éjection, ainsi que des zones opérationnelles : capture (C), attente1 (A1), travail (T), attente2 (A2), éjection (E), sont présentées en figure.2.A. Quand un produit est détecté en zone C, la tâche d'interception fait une requête pour l'état de la zone A1 et elle intercepte le produit, quand la zone est libre. La tâche de transfert déplace le produit de la zone A1 à T puis A2. Enfin la tâche d'éjection demande la disponibilité de la zone E et y transfère le produit. Pour la démonstration l'ajout d'un programme malveillant permettant de simuler une attaque par corruption d'automate a été choisi. Celui-ci est compilé avec le code initial du système et permet à la mise à jour d'une variable globale, d'activer la sortie de deux vérins simultanément. Durant l'expérimentation les temps de simulation et de communication suivant ont été mesurés : 57ms sans la passerelle, 59ms avec, le temps de cycle automate est de 18ms et celui de la simulation était de 20ms. Ces résultats nous permettent de déduire une latence induite par notre premier mécanisme de 2ms. La détection a bien fonctionné tout comme les différents mécanismes de réaction. Notre démonstrateur utilisant des interfaces réseau physiques, cela permet son monitorage à travers un analyseur réseau. Aussi il autorise l'exploitation de failles de sécurité semblable au système réel.

3 Travaux futurs

La prochaine étape de notre travail est la génération automatique de modèle de détection interprétable et utilisable par notre passerelle. Ce travail se fera par transformation et enrichissement du modèle existant et décrit dans la thèse de Romain Bévan [1]. Nous souhaitons aussi tester de nouveaux mécanismes de détection et de réaction, faisant appel à d'autres modèles permettant le profilage d'information/composant ou la mise en replis du système.

Références

[1] Romain Bévan. *Approche composant pour la commande multi-version des système transitiques reconfigurables.* PhD thesis, Universitée de Bretagne Sud, 2013.

[2] Romain Pichard, Alesandre Philippot, and Bernard Riera. Consistency checking of safety constraints for manufacturing systems with graph analysis. In *{IFAC} Proceedings Volumes*, Toulouse, France, juillet 2017.

[3] Thomas Toublanc, sebastien Guillet, Florent Delamotte, and Pascal Berruet. Using virtual plant to support the development of intelligent gateway to sensors/actuators. In *{IFAC} Proceedings Volumes*, Toulouse, France, juillet 2017.