Sujet de stage de M2
Année 2021/2022

Titre : Analyse d'incidence de l'intégration de composants de cybersécurité dans les systèmes de l'industrie 4.0

Contacts :
- Laurent NANA, Professeur des Universités, Université de Bretagne Occidentale, Lab-STICC, Département Informatique, Tél. 02 98 01 71 67, E-mail. Laurent.Nana@univ-brest.fr
- François MONIN, Maître de Conférences, Université de Bretagne Occidentale, Lab-STICC, Département Informatique, Tél. 02 98 01 82 20, E-mail : Francois.Monin@univ-brest.fr

Description :

Contexte :

Contrairement aux systèmes industriels antérieurs qui fonctionnaient principalement en mode local, avec très peu voire quasiment aucune interaction via le réseau Internet et avec une partie logicielle assez réduite et très souvent propriétaire, les systèmes industriels actuels dits 4.0 sont connectés à l'Internet et intègrent une part importante de logiciel. Ils sont ainsi vulnérables aux attaques susceptibles d'intervenir via le réseau Internet et via la partie logicielle qu'ils intègrent et qui devient de plus en plus prédominante.

L'intégration de mécanismes de sécurité dans les systèmes de l'industrie 4.0 est donc essentielle. Cette intégration n'est pas sans conséquence sur le fonctionnement du système initial et peut par exemple induire des latences pouvant entraver le bon fonctionnement du système industriel. Il convient donc de s'assurer que l'ajout de composants de sécurité ne remettra pas en cause le bon fonctionnement du système industriel.

Différents travaux ont été initiés autour de la cybersécurité des systèmes industriels [1, 2]. Différents outils existent pour modéliser, simuler, analyser et vérifier les propriétés de systèmes. Parmi ces derniers, nous pouvons mentionner des outils de simulation, d'analyse et de vérification tels que les Réseaux de Petri [3, 4], les outils de vérification formelle basée sur le model-checking tels que Kronos [5] et UPPAAL [6] et des outils de vérification formelle basée sur la preuve de théorème tels que COQ [7, 8] et PVS [9, 10, 11].

Objectif

Le but du travail proposé dans ce stage est de proposer un modèle de fonctionnement des systèmes industriels de l'industrie 4.0 prenant en compte l'intégration de composants de sécurité, et permettant d'analyser l'incidence de l'ajout de ces composants sur le fonctionnement du système et plus particulièrement sur le respect des contraintes temporelles, puis de modéliser et simuler le modèle à l'aide d'un outil adapté.

Organisation du travail:

Ce travail comportera plusieurs étapes :
- Un état de l'art sur l'industrie 4.0 et les composants de sécurité pour l'industrie 4.0
- Un état de l'art sur les formalismes de modélisation, d'analyse et de vérification de propriétés des systèmes dont les propriétés temporelles
- Le choix d'un système représentatif de l'industrie 4.0 et des composants de sécurité en vue de l'analyse
- Le choix du formalisme de modélisation et d'analyse.
- La modélisation du système et l'analyse des propriétés à l'aide du formalisme retenu.

Références :

[1] ALEM S. Cybersécurité des équipements connectés industriels : systèmes de détection d'intrusions. Thèse de Doctorat, 2021.
[2] ANSSI. Use case of cybersecurity for industrial control systems. Technical report, 2014.
[3] Jensen K. Coloured Petri Nets - Basic Concepts, Analysis Methods and Practical Use. Springer-Verlag Berlin Heidelberg, 1997
[4] Nana L, Legrand J, Singhoff F, Marcé L. Modelling and Testing of PILOT Plans Interpretation Algorithms. In Proceedings of Multi-conference on Computational Engineering in Systems Applications, CESA'03, IEEE, Lille, France, 2003
[5] UPPAAL. http://www.uppaal.com
[6] Kronos. https://www-verimag.imag.fr/DIST-TOOLS/TEMPO/kronos/index-english.html
[7] Development Team, "The Coq proof assistant : Documentation, system Download", contact : http://coq.inria.fr
[8] Huet G, Kahn G, Paulin C. The Coq Proff Assistant : a Tutorial, Version 5.10. INRIA Institut National de Recherche en Informatique et en Automatique, Technical Report, RT-0178
[9] Owre S, Rushby J, Shankarr N, Crow J, Srivas M. A Tutorial Introduction to PVS. http://www.csl.sri.com/papers/wift-tutorial/
[10] Evans N, Schneider S. 2000. Analysing Time Dependent Security Properties in CSP Using PVS. In Proceedings of the 6th European Symposium on Research in Computer Security (ESORICS '00). Springer-Verlag, Berlin, Heidelberg, 222–237.
[11] Nana L, Monin F, Gire S. 2021. Formal Proof of Properties of a Syntax-Oriented Editor of Robotic Missions Plans. ASTESJ, ISSN: 2415-6698, vol. 6 (1), pp. 1049-1057.