Research internship

Petri Nets for Cyber-Physical System Security Analysis – Application to Manufacturing Systems

Location: LIS – Aix-Marseille University (Saint-Jérôme)
Team: MoFED
Duration: 5 months
Supervisors: Rabah Ammour (MdC) and Leonardo Brenner (MdC)
Contact: rabah.ammour@lis-lab.fr
(application should include a CV and transcripts of License, Master 1, 2)

Context:

With the rapid growth and deployment of Cyber-Physical Systems (CPSs), many challenges, not always found in classical or embedded systems, have emerged. One of them is the security issue [1]. Indeed, CPS operate in networked environments as they need to communicate remotely with monitoring and management systems. This feature makes them more vulnerable to various threats and cyber-attacks with major potential consequences for users. More specifically, cyber-attacks could manipulate the system in order to induce a catastrophic event. For instance, malicious adversaries can arbitrarily corrupt the measurements of remote sensors in the CPS. The corrupted measurements data will lead to corrupted controls since sensor measurement data are used to generate the control inputs. This leads the physical system to possibly reach undesirable and critical operational conditions.

For the modelling and analysis of dynamical systems, discrete event systems (DESs) theory provides mathematical abstractions and formalisms that can be exploited. It proposes techniques and formalisms including Petri nets (PNs) [2] with different extensions. Recently, a new formalism called Output Synchronized Petri Nets (OutSynPNs) [3] was developed to model CPSs. This formalism was exploited in [4] to evaluate the cost of an attack that aims to drive a CPS from its current state to a forbidden or dangerous one.

The objectives of the research internship are the following:

1) Literature review on the modelling of cyber-attacks in discrete event systems framework.
2) Review of the Output Synchronized Petri Nets [3] formalism.
3) Extend the work developed in [4] to the case where the attacker does not know the current state of the system.
4) Implement and validate the developed method on an experimental manufacturing system.

References:

[1] Alur, R., 2015 *Principles of cyber-physical systems*. MIT Press.
[2] David, R., & Alla, H., 2010. *Discrete, continuous, and hybrid Petri nets* (Vol. 1, pp. 17-130). Berlin: Springer.
[3] Ammour, R., Amari, S., Brenner, L., Demongodin, I., Lefebvre, D., 2021. Observer design for output synchronized Petri nets. *European Control Conference.*
[4] Ammour, R., Amari, S., Brenner, L., Demongodin, I., and Lefebvre, D. (2021). Costs analysis of stealthy attacks with bounded output synchronized Petri nets. *IEEE Int. Conference on Automation Science and Engineering (CASE)*, 799-804.

Keywords: Cyber-physical systems, Cyber-attacks, Petri nets, Manufacturing systems, Matlab programming.