Cybersecurity and resiliency within IIoT context

Co-directeurs de la thèse : Samiha Ayed (UTT ; samiha.ayed@utt.fr)
Lamia Chaari (Université de Sfax ; lamiachaari1@gmail.com)

The Industrial Internet of Things (IIoT) consists on the application of the internet of things in different industrial domains that may include automation like energy distribution, manufacturing, transport industry as well as process industries. To get an optimal use of the IIoT networks, many requirements have to be satisfied such as high reliablity, low latency, high connectivity, etc. Reaching these requirements may be complex mainly because the IIoT systems may be a privileged target for cyber-attacks. Hence, to protect the execution environment of an IIoT system, we have to specify and deploy a security policy. The role of that security policy is to protect the system for potential attacks and detect security incidents. In the literature, many works addressed the security topic in relation with the IIoT systems mainly to detect attacks. Nevertheless, detecting attacks is not enough to ensure the system requirements cited above. Indeed, the chain process of most IIoT systems, the automation aspect as well as the real time criteria make detection attacks not enough efficient for the system operation. For that, in this thesis we aim to deal with the resiliency in relation with the cybersecurity for the IIoT context. The work has to be based on two phases :

1- Definition of a new security detection process that includes a generic security policy describing different attack patterns

2- Specifiiying, modeling and deploying a reaction policy that should be triggered once the detection process is complete. This second phase is describing our resiliency policy. Resiliency is critical for the system operation mainly within the decentralized IIoT context to ensure the system operation stability.

The aim of this thesis is to specify, modelize and deploy a SOC based on the two phases cited above. Actually, there are no solutions that address both detection and reaction phases. The new framework to be proposed should take into account the different requirements of an IIoT environment. The specification of the solution will be based on artificial intelligence approaches. Moreover, the evaluation of the SOC will be based on a set of selected and significant metrics.

Tasks planning :

1) Task 1: To elaborate a state of the art related to the security requirements and proposed solutions to solve security attacks to which the IIoT are exposed.
   This task should be validated at least by one survey paper.
2) Task 2 : To design and validate a secure framework to propose new detection approaches based on artificial intelligence to detect attacks on IIoT environment.
   This task should be validated at least by one journal paper and one conference paper.
3) To propose, specify and validate a new reaction policy approach to contermeasure detected security incidents based on artificial intelligence techniques. The security approach should be dynamic and contextual to take into account the IIoT requirements.
   This task should be validated at least by one journal paper and one conference paper..
4) To propose a SOC and to define its evaluation metrics based on the detection and reaction policies. These metrics have to be applied on a realistic scenarios to be selected.
   This task should be validated at least by one journal paper and one conference paper.