le nom et l'acronyme du projet : **Tiaki**
l'identité et l'affiliation du porteur : **Sentryo**
le consortium : **Sentryo et CEA Cadarache**
l'instrument de financement : **DGA Rapid**
les dates de début et de fin de projet : **01/10/2015 - 31/12/2018**
la plage de TRL associée aux innovations : **4 à 7**

La cybersécurité des systèmes industriels représente un enjeu majeur alors que les usines deviennent de plus en plus connectées et donc plus vulnérables à des attaques informatiques. L'impact peut être encore plus important que dans un environnement IT classique car les conséquences peuvent se répercuter dans le monde physique si le processus industriel est altéré (imaginons les conséquences catastrophique d'une attaque informatique dans une centrale électrique). Les outils actuels de détection d'intrusion sont couramment utilisés mais ont le défaut de devoir être configurés manuellement et présentent un taux de faux positifs élevé. Afin de remédier à ces limitations, le projet TIAKI s'est porté à développer des outils de Machine Learning afin d'être plus efficace dans les détections d'attaques.

Pour ce faire, un projet de recherche en collaboration avec le CEA (les sociétés ESI et Rtone sont intervenues en support) a été financé par la DGA. Sentryo a ainsi eu accès à des lots de données contenant du trafic réseau dans les installations du CEA, en condition nominale et avec différents scénarios d'attaque, sur différents types de réseaux et équipements ciblés (principalement des automates industriels).

Différents scénarios d'attaques ont été étudiés puis catégorisés, et des algorithmes de Machine Learning ont été développés afin de détecter les étapes successives survenant lors d'une attaque. L'enseignement principal de ces études est qu'il est difficile de faire l'apprentissage d'un algorithme de manière binaire à partir de comportements prédéfinis (nominal ou attaques). Nous avons donc opté pour une approche de détection d'anomalie, avec un apprentissage du modèle fait sur le terrain, spécifique à chaque installation qui sera surveillée. Cet apprentissage se base sur les variables d'automates observées en phase de fonctionnement nominale. La tâche du modèle est de prédire le comportement futur du processus industriel, étant donné les observations faites auparavant sur les mêmes variables. Si une différence significative est observée entre la prédiction du modèle et l'observation faite sur le terrain, une alerte est émise afin d'alerter l'opérateur.

Un retour sur les travaux effectués ainsi que les perspectives de développement pour un système de détection d'anomalie dans un environnement contraint seront présentés plus en détail.