Projet collaboratif ANACONDA : Analyse de Cybersécurité au moyen d'outils non-intrusifs de diagnostique automatique

Ch. Barthélémy
Ponant Technologies,
21 Rue Pierre Mechain
26000 Valence

D. Midroit
120 Rue de St Cyr
69009 Lyon

G. Blanchard, C. Carlotti,
M. Seignobos, A. De Carlo,
Z. Kazemi, S. Jean, A. Mercier,
V. Beroulle, O. Aktouf
Univ. Grenoble Alpes,
Grenoble INP, LCIS, 26000 Valence

- Le nom et l'acronyme du projet : Analyse de Cybersécurité au moyen d'outils non-intrusifs de diagnostique automatique – ANACONDA (https://ponant-technologies.com/projet-anaconda/).
- L'identité et l'affiliation du porteur·euse : Christophe Barthélémy ; Ponant Technologies, Valence (26).
- Le consortium :
  - *Entreprises :* Ponant Technologies (Valence, 26) : Bureau d'étude en informatique industrielle et informatique embarquée et Rtone (Lyon, 69) : Bureau d'étude en développement d'objets intelligents et connectés.
  - *Laboratoire :* LCIS (Valence, 26) : Laboratoire de Conception et d'Intégration des Systèmes.
- L'instrument de financement :
  - R&D Booster, Région Auvergne-Rhône-Alpes, instrument de financement des étapes de validation et de prototypage.
  - Labellisation par le pôle Minalogic : pôle de compétitivité des technologies du numérique en Auvergne-Rhône-Alpes.
- Les dates de début et de fin de projet : Novembre 2020 – Novembre 2023.
- La plage de TRL associée aux innovations : 5 (Validation de composants et/ou de maquettes en environnement représentatif).

Résumé :

A l'instar du grand public, les industriels exploitent de plus en plus l'Internet des Objets pour optimiser l'automatisation et accroître leur productivité. L'industrie du transport, de l'énergie, de la chimie, de l'électronique et de la santé, exploitent des réseaux de capteurs ainsi qu'une multitude d'autres systèmes connectés permettant de collecter des données de production et d'alimenter le cloud, afin d'affiner l'analyse de performance de leurs sites de production.

La démultiplication de l'internet industriel des objets « IIoT » augmente la surface d'attaque des sites industriels. Cet accroissement de la densité et du nombre de points d'accès laisse entrevoir des failles conséquentes en matière de sûreté et de sécurité. Les contraintes de coût auxquelles les constructeurs doivent faire face lors des phases de conception et de fabrication peuvent entraîner des choix de mécanismes de sécurité faibles voire inexistants.

L'IoT dispose de peu de références pour mesurer les impacts de la cybersécurité sur son cycle de développement produit. Par analogie, nous pouvons observer les impacts dans un domaine mature sur ce sujet à savoir les terminaux de paiement qui consacrent de forts investissements pour l'identification des sources d'attaques, pour maintenir une veille et des outils de test à jour des vulnérabilités. Une offre produit simple, adaptable et suivie par des experts peut être déterminante pour les opérateurs d'IoT.

Le projet ANACONDA (ANAlyse de Cybersécurité au moyen d'Outils Non-intrusifs de Diagnostique Automatique) vise à développer le démonstrateur d'un équipement de diagnostique automatique de vulnérabilités pour l'internet des objets dans un contexte d'évaluation et de vérification des exigences de sûreté et de sécurité. Cette solution permettra au concepteur de systèmes connectés d'effectuer des campagnes de tests et d'investigations tout au long des phases de conception pour remplir l'objectif d'une conception sécurisée.

Le consortium intègre l'expertise de Ponant Technologies dans l'automatisation et la robotisation des tests fonctionnels, celle de Rtone pour la conception d'objets connectés sur mesure et le laboratoire LCIS pour son expertise dans le domaine des systèmes embarqués communicants ; enfin Crouzet qui s'associe au projet en tant que premier utilisateur avec comme cible leurs automates industriels programmables.

Les travaux de cadrage, de veille technologique et d'analyse détaillée des normes et directives sont terminés. Ils ont permis de confirmer l'intérêt du positionnement d'ANACONDA et la nécessité de maintenir une veille active sur les évolutions réglementaires. La rédaction des spécifications fonctionnelles et la définition de l'architecture générale sont en cours. La qualification d'outils logiciels et matériels ainsi que la réalisation de proof of concept sont également lancées.