La vulnérabilité des systèmes de contrôle industriels à des attaques informatiques a été largement mise en évidence en 2010 par l'affaire StuxNet. Les conséquences de telles attaques sur des infrastructures critiques, dans des domaines comme l'énergie, le transport ou la défense, peuvent être extrêmement graves. Il est donc fondamental de proposer des composants capables de mieux résister à ces attaques.

Dans ce contexte, le projet FUI INGOPCS propose de développer une implantation du protocole OPC-UA (norme EN/IEC 62541) pour la communication entre systèmes industriels, en suivant une approche robuste, qui permettra à terme de viser une certification Critères Communs (ISO 15408) de niveau EAL4.

Le standard OPC-UA définit des objectifs de sécurité pour garantir l'authentification, l'autorisation, la confidentialité, l'intégrité, l'auditabilité et la disponibilité. Il définit également des menaces, comme le flooding, le profilage et le débordement de capacité. Ces menaces doivent être contrées au niveau du protocole lui-même par la mise en place de certificats et de communications chiffrées. Cependant, il faut également vérifier que l'implantation, tant au niveau de l'architecture matérielle qu'au niveau du code, respecte les scénarios établis au niveau du protocole.

Afin de fournir une implantation sécurisée, nous proposons de produire une version libre de la pile de communication basée sur la norme OPC-UA, qui sera vérifiée avec des outils d'analyse statique pour s'assurer qu'elle répond bien aux objectifs de sécurité. La plate-forme Frama-C, disponible en open-source, et ses contreparties industrielles TrustInSoft Analyzer et TrustInSoft Interpreter (lui aussi open-source) seront utilisées pour l'analyse du code de la pile. Ces outils proposent des analyses basées sur les méthodes formelles pour détecter exhaustivement les erreurs potentielles à l'exécution dans du code C ou C++. Cela garantit par exemple que le code ne contient pas de vulnérabilité comme des débordements de buffer (CWE-120), des fuites de mémoire (CWE-125), ou des divisions par zéro (CWE-369).

En outre, afin d'assurer la certifiabilité de la pile au sens des critères communs, INGOPCS s'attache à définir clairement son contexte d'utilisation, les exigences fonctionnelles de sécurité, et les exigences d'assurance de sécurité attachées à la pile. Ces aspects ont été pris en compte dès le début du projet afin d'assurer l'adéquation du processus de développement avec ces exigences.

Enfin, le projet comporte différents démonstrateurs industriels, incluant des systèmes d'acquisition de données (SCADA), des systèmes de contrôle distribués, des contrôleurs programmables (PLC) et des capteurs intelligents, afin de valider l'utilisabilité de la pile. Ces démonstrateurs seront réalisés par les partenaires du projet, qui représentent la plupart des domaines industriels concernés. INGOPCS est par ailleurs soutenu par l'ANSSI.