第 3 回 STAMP ワークショップ発表概要

タイトル

ICS におけるセーフティとセキュリティのための STAMP モデル適用

An Application of STAMP to Safety and Cyber Security for ICS

著者・発表者

名古屋工業大学大学院　近藤　駿、佐藤　草太、濵口　孝司、橋本　芳宏

Nagoya Institute of Technology　Shun KONDO, Souta SATO, Takashi HAMAGUCHI, Yoshihiro HASHIMOTO

概要

近年、産業制御システム（ICS）に対するサイバー攻撃が現実のものとなり、被害も深刻化している。情報システムに対するサイバー攻撃と異なり、ICS に対するサイバー攻撃は現実世界に直接的な影響を与えることが可能であり、人命に影響を与える事故や災害につながる危険性がある。サイバー攻撃の手口は無数に存在し、すべてを想定することは困難であることから、サイバーインシデントが発生してしまったらという観点で、ICS や制御対象における異常が事故に繋がらないように対策の強化、および、速やかに復旧して事業を継続できるようにレジリエンシーの強化が必要である。

重要な ICS には異常や事故を未然に防ぐ、あるいは被害を抑えるといった観点から、独立防護層（IPL）に基づく安全設計が行われている。しかし、同時多重に発生しうるサイバー攻撃によって引き起こされた異常によって、基本プロセス制御システムとは独立して設置された安全対策としての自動安全計装システムのプログラムが書き換えられて異常発生時に動作しない場合や、監視画面の隠蔽工作により、オペレータが適切な緊急時対応をとれなかい場合が発生しうる。すなわち、IPL の多重性はサイバー攻撃下では無効化される危険性があるため、従来の観点に加え、「サイバー攻撃に対しても安全対策の多重性を維持する」といった観点から対策や緊急時対応を設計する必要がでてきた。

本発表では、設置された複数の対策および緊急時対応における機能連動の構造を STAMP モデルで表現した上で、ICS のネットワーク構成情報と組み合わせる事によって、「サイバー攻撃に対しても多重性を維持できる安全対策の設計」、および「サイバーインシデント時における有効な対策の選択」を議論する方法を発表する。

キーワード

(1)　セーフティ

(2)　サイバーセキュリティ

(3)　インシデントレスポンス

(4)　多重防護の設計