SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

サイバー攻撃に対するレジリエントな縮退運転システムの設計と実装
Synthesis and Implementation of Resilient Fallback Control Logic Under Cyberattacks

阪田 恒晟 * 藤田 真太郎 * 澤田 賢治 *
Kousei Sakata Shintaro Fujita Kenji Sawada

遠藤 浩通 † 松本 典剛 †
Hiromichi Endou Noritaka Matsumoto

キーワード 制御システムセキュリティ，縮退運転システム，スーパーバイザ制御

あらまし

産業用制御システムは既にサイバー攻撃を受けることを前提としたシステム設計と運用が必要となっている. すなわち, サイバー攻撃下でもシステムを安全に稼働させる縮退運転が必要になる[1]. 本研究の目的は, 通常運転と縮退運転の遷移が可能な縮退運転システムをシステム論的に設計し, その優位性を検証することにある. 対象は通常用と縮退用の PLC からなる FA システムである. Fig. 1 に FA システムの概要を示す. 通常用 PLC はフィールド機器を制御し, 縮退用 PLC は通常用 PLC が攻撃を受けた後, 制御を引き継ぐ. 制御引き継ぎにはシステムを統合管理するスーパーバイザモデル[2]が必要となるが, PLC の制御プログラムを離散事象システムの枠組みでモデル化する事で当該モデルを導出する方法を与える. 課題の本質は攻撃下におけるスーパーバイザの設計には, 攻撃を含んだ制御仕様の可制御性が必要となることである. 新規性は異常検知の事象を制御仕様に含めることで, 当該課題が解決できる事を明らかにした点である. これにより, 制御システムの運転状態の速やかな切り替えを可能とする. スーパーバイザの実装方法の有効性は, 設計されたスーパーバイザモデルから縮退プログラムを生成し, 縮退用 PLC に実装する事で検証する.

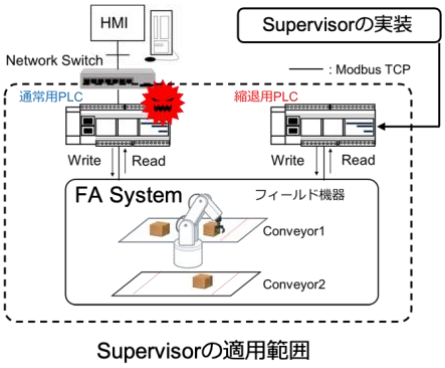

Fig. 1 FA システム

参考文献

[1] T. Sasaki, K. Sawada, S. Shin, and S. Hosokawa: Model Based Fallback Control for Networked Control System via Switched Lyapunov Function, The IEICE Transactions on Fundamentals, Vol.E100-A, No.10, pp 2086-2094, 2017.

[2] 阪田, 藤田, 澤田: サイバー攻撃に対するレジリエントなスーパーバイザの設計, 第 64 回自動制御連合講演会, pp. 252-257, 2021.

* 電気通信大学, 〒182-8585 東京都調布市調布ヶ丘 1-5-1.
The University of Electro-Communications, 1-5-1, Chofugaoka, Chofu, Tokyo, 182-8585, Japan

† (株)日立製作所 研究開発グループ, 茨城県日立市大みか町 7-1-1, Hitachi, Ltd Research & Development Group, 7-1-1, Omika-cho, Hitachi-shi, Ibaraki, Japan