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

シーケンス制御システムに対するホワイトリスト式異常検知のための正常状態遷移のモデル化

Normal State Transition Modeling for Whitelisting Function of Sequential Control System

藤田 真太郎 * 澤田 賢治 *
Shintaro Fujita Sawada Kenji

キーワード 制御システムセキュリティ，ホワイトリスト

あらまし

産業用制御システムに対するサイバー攻撃は増加しており，2021 年の 5 月にアメリカのパイプラインで発生したランサムウェアによる攻撃は，経済に大きな損失を生んだ[1]．この攻撃は，DarkSide と呼ばれる組織による犯行とされており，今後もこのような組織的かつ計画的な犯行が増加していくと考えられる．そのため，ICS を保護するためにさまざまなセキュリティ対策手法が検討されている．

制御システムの異常を検知する方法として，システムの正常な状態遷移をリストとして登録し，リストに登録されていない状態遷移を異常として検知するホワイトリスト式異常検知がある．このホワイトリスト式異常検知のためのリストにあたる正常状態遷移モデルの生成手法を提案する．特に制御システムの中でも，離散事象システムとしてモデル化が可能なシーケンス制御システムを対象とする．

シーケンス制御システムの多くは，リレー回路を模擬したラダー言語で制御されている．ラダー言語の離散事象モデル化手法[2]は多く研究されているが，プラントの動作モデルは設計者が与える必要がある．更新などによりシステムの構成が変更した場合，従来手法ではモデルの再生成が困難である．そこで，動作ログからプラントの動作モデルを生成し状態遷移モデルの生成する手法の検討をシミュレーションプラントを用いて行った．プラントシミュレータは Factory I/O[3]を用いて，図 1 に示すロボットアームによる荷物仕分プラントを対象とした.．本手法によって，ホワイトリストの生成に設計者の情報が不要となる．将来的には制御器がプログラムの解析とログ収集を行いホワイトリストの自動更新が可能となるとを目指す．

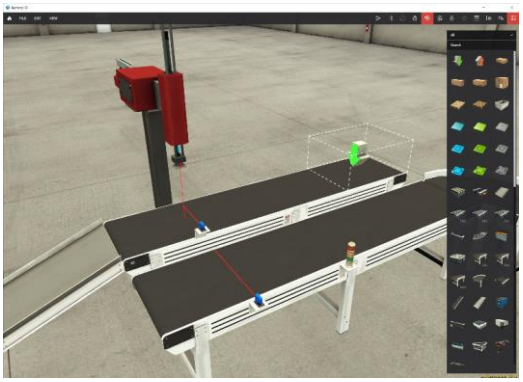

図 1 Factory I/O により作成したシミュレーションプラント

参考文献

[1] Colonial Pipeline Paid Hackers Nearly 5 Million in Ransom:https://www.bloomberg.com/news/articles/2021-05-13/colonial-pipeline-paid-hackers-nearly-5-million-in-ransom

[2] S. Nakamura, Y. Fujii and T. Sekiguchi, "Study on a transformation method of ladder diagram into se-quential function chart on the basis of linear pro-gramming technique," 1997 IEEE 6th International Conference on Emerging Technologies and Factory Automation Proceedings, EFTA'97, 1997, pp. 473-478

[3] Factory I/O, https://factoryio.com

* 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.