Cyber-Physicalシステムのためのリスク アセスメント手法提案に向けた調査
A survey for proposing a risk assessment method for Cyber-Physical systems

後藤研究室　博士課程前期１年　我妻　敏　Satoshi Agatsuma
E-mail: mgs185501@iisec.ac.jp

情報セキュリティ大学院大学　情報セキュリティ専攻
Graduate School of Information Security, Institute of Information Security

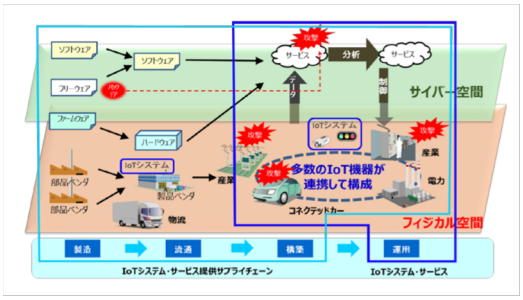
概要

Cyber-Physicalシステム（CPS）を安全なものとするためには、情報システム（IT）のセキュリティと制御システム（OT）のセーフティーを統合的に分析する必要がある。そこで、本研究はCPSを統括的にモデル化し、潜在的リスク分析を行う手法の提案を目標とした。
本稿は、研究の初期段階として既存リスク分析手法を調査した結果をまとめたものである。既存リスク分析手法として、ガイドラインをベースとした手法、FTA/ATA、確率的アプローチ、FMEA、STAMP/STPA、Petri Netを取り上げている。

Abstract

In order to make this Cyber-Physical System (CPS) secure, it is necessary to analyze the security of the information system (IT) and the safety of industrial control system (ICS) in an integrated manner. Therefore, this research aims at proposing a method of conducting latent risk analysis by modeling CPS in a comprehensive manner.
This paper summarizes the results of investigating the existing risk analysis methods as an early stage of research. As an existing risk analysis method, the guideline-based method, FTA / ATA, stochastic approach, FMEA, STAMP / STPA, Petri Net are taken up.

キーワード： Cyber-Physical System(CPS)、Industrial Control System(ICS)、リスク アセスメント、インシデント、セーフティー、FTA、ATA、FMEA、STAMP/STPA、Petri Net
Keyword: Cyber-Physical System(CPS), Industrial Control System(ICS), Risk assessment, Incident, Safety, FTA, ATA,FMEA, STAMP/STPA, Petri Net



戦略的イノベーション創造プログラム（SIP）
IoT 社会に対応したサイバー・フィジカル・セキュリティ 研究開発計画 より

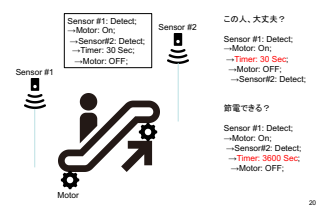
日本が産官学を挙げて推進するIndustry 5.0 に代表されるCyber-Physicalシステム（CPS）とは、実世界（Physical system）のセンシング デバイスをネットワークで繋ぎ、実社会で生み出される膨大なデータを収集・分析することで新たな知識や価値を生み出し（Cyber system）、それを実社会に還元することで様々な社会問題の解決をめざすものである。
ネットワーク化がすすむ制御システム（ICS）は、そのCPSを代表するものの1つとなっており、制御技術と情報技術の融合である。しかし、それはまだ端緒についたばかりであり、重要命題であるネットワーク化された制御システムの安全にはまだ課題が多いのが現状である。これまで制御システム（OT）技術者と情報システム（IT）技術者は互いに交わることなく業務を遂行してきたが、サービスの多様化、高度化、コスト削減などの要請により、制御システムのオープンなネットワーク化の流れは増々強くなることは明らかである。
本研究は、OT/IT技術者が共に対象CPSを理解し、リスク要因抽出 の一助となれる新たなリスク アセスメントの提案を目指すものであるが、本稿は、その初期段階として既存のCPSシステム のモデル化、リスク アセスメント手法を調査しまとめたものである。

ハザード、インシデント対応とその発生契機のマッピング

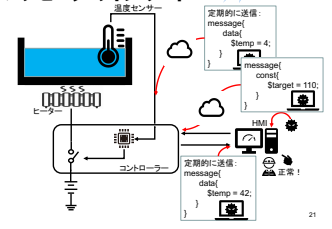
制御システムで発生するハザードやアクシデントに対する対応策などは、これまでもFTA、ETA、FMEA、HAZOPなどのリスク アセスメント手法によりリスクが抽出され、その事前事後対策が策定され、訓練も実施されてきた。
今後起こりえる、情報セキュリティ インシデントを契機として発生したハザードに対する対応としても、これまでに確立されたハザード対応策は有効であると考えられる。しかし、根本原因が悪意の第3者による情報操作である場合には、眼前の事象に対応するだけでは、再度同じハザードを引き起こされてしまう。
したがって、CPSにおいては、発生しうる情報操作と、その帰結として発生するハザードとの対応付けが必須であると考える。
今後のハザード対応では、ハザード対応策の実施とともに、それが情報操作により発生しうるものであるか判断し、もし情報操作で発生しうるものであるのであればその発生原因の究明が必須である。

評価項目	評価内容
視覚的表現	有向グラフなど、メッセージの流れやイベントの発生条件などが表現しやすいか
M_I の表現	なりすまされたメッセージの注入ポイント、流れが判りやすく表現できるか
M_B の表現	正規メッセージのブロック点が検討しやすいか
時間の表現	ホールドタイマーなど、時間条件が表現しやすいか
順序の表現	複数のイベントの順序関係・依存関係が表現しやすいか
階層的な表現	システムの階層的構造を表現しやすいか
形式的検証	客観的表現で、検証可能か（Formalism）
確率の表現	確率的な評価が実行しやすいか

メッセージの順番、設定値



メッセージのインサート



シーケンス制御、PID制御などのインシデントの事例から、情報操作を類型化し、研究目的に適合する手法を決定したい

メッセージのインサート （M_I と表記）
　i.e.) 任意にメッセージ（コマンドやセンサー値）を送信できる
　　偽のアラート情報の送出

メッセージのブロック（M_B と表記）
　i.e.) 開始、停止などのコマンドを妨害
　　緊急アラートを妨害

CPS システムに対するリスク分析手法を調査

通信（メッセージ交換）に着目
　OSI 7階層モデル
システム全体に着目
　Fault Tree Analysis / Attack Tree Analysis (FTA/ATA)
　Event Tree Analysis (ETA)
　Failure Mode and Effect Analysis (FMEA)
　Hazard and Operability Studies (HAZOP)
　Petri net とその拡張
　STRAIDE
　System Theoretical Accident Model and Process (STAMP)

形式	OSI	FTA/ATA	ETA	FMEA	HAZOP	Petri net	STRIDE	STAMP
視覚的表現	○	○	○	×	×	○	○	○
M_I の表現	○	×	×				○	
M_B の表現	○	×	×				○	
時間の表現	×	×	×	×				
順序の表現	×	○		×	×			
階層的な表現					×			○
形式的検証	×	×	×	×	×	○		
確率の表現	×		○				×	×

現時点での利用しやすさの調査結果