第 3 回 STAMP ワークショップ発表概要

タイトル

STPA を用いたリスク分析・対策選定手法の提案と適用

Proposal and application of risk analysis / countermeasure selection method using STPA

著者・発表者

東京電機大学　早川 拓郎

Tokyo Denki University　Takuo Hayakawa

概要

IoT の普及が進んでいる．IoT の対象は家電から医療機器まで多岐に渡り，これらはもともとスタンドアロンでの動作を前提とした機器である．したがって，IoT は新たな機能や価値を実現すると同時に，サイバー攻撃などの想定されなかったセキュリティ上の脅威をもたらす．また，従来の IT 機器と異なり，セキュリティ上の脅威により誤作動や停止など、セーフティ上の脅威が発生する可能性もある．したがって、メーカーは設計段階からセキュリティ・バイ・デザインと機能安全の両面を考慮しなければならない。

セキュリティ・バイ・デザイン実現のためにはリスクコミュニケーションが不可欠である．設計段階であらかじめ関係者同士でリスクについて合意形成しておくことで効果的な対策を選定できる．通常、リスクコミュニケーションはツリー分析等によるリスク分析手順を含む．従来，リスク分析にはフォールトツリー解析やアタックツリー解析が用いられてきた．これらの手法を用いることでリスクの値に基づく合意形成と対策の選定が可能となる。一方で、現状ではセーフティとセキュリティの分野間では乖離があり，両分野は別の領域として議論される。このような現状はセーフティとセキュリティを統合的に扱う必要のある IoT には不適切である．また，IoT は多数の構成要素と制御を含んでおり，従来の木構造解析だけでなく，システムのモデルを含んだ分析を行うことが望ましい．

本研究では IoT のセーフティとセキュリティの統合的なリスクコミュニケーションを実現するための新たなリスク分析・脅威選定手法提案する．この手法には安全解析手法 STPA とツリー分析手法の一つである EFT(Extended Fault Tree)によるリスク分析手順、ディフェンスツリーによる対策選定手順が含まれる．提案手法の全体図を以下の図 1 に、手順を以下の表 1 に示す．また，提案手法を実際に糖尿病患者向け IoT 機器であるインスリンポンプに適用した例を示す．

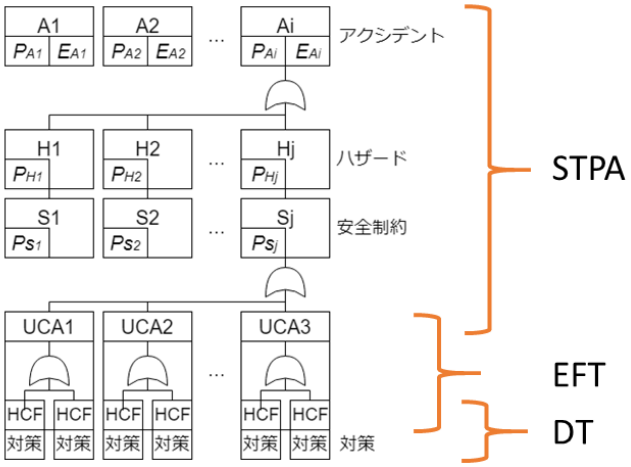

図 1. 提案手法の全体図

手順	内容
1	アクシデント，ハザード，安全制約の識別
2	コントロールストラクチャの構築
3	UCAの識別
4	ハザード誘発要因の特定
5	アクシデントの確率分析
6	対策選定

表 1. 提案手法の手順

キーワード

(1) リスク分析

(2) 対策選定

(3) ツリー分析

(4) セキュリティ・バイ・デザイン