IPA Better Life with IT

第2回 STAMPワークショップ

国際安全規格におけるSTAMP/STPA適用可能性の考察

Prospect for availability of STAMP/STPA as safety analysis method in international safety standards

2017年11月28日

IPA/SEC「IoTシステム安全性向上技術WG」委員
JASA「安全性向上委員会」委員
(株)東芝 余宮尚志
(株)ジェーエフピー 中村洋

SEC Software Reliability Enhancement Center

注意：本発表では、国際安全規格における安全分析の概要や考え方について公開情報を整理して説明するが、国際安全規格の詳説やSTAMP/STPAの適用事例は含まない。

この発表の趣旨

- 国際安全規格において、従来の安全分析手法との違いを踏まえて、STAMP/STPAが適する開発工程についてどのように考えられるかを中心に紹介する
  - 国際安全規格の紹介
  - 国際安全規格で参照される従来の安全分析手法の紹介
  - 国際安全規格に対するSTAMP/STPA適用事例からの知見の紹介
  - いくつかの視点での考察
  - まとめ

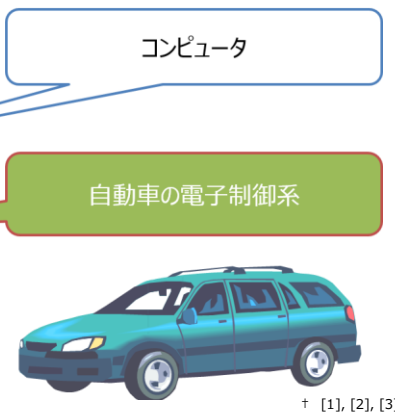
国際安全規格の紹介

ISO/IECのグループ安全規格(機能安全)

規格の種類	ISO/IEC規格
基本安全規格 （タイプA規格）	• ISO 12100 • ISO 14121†
グループ安全規格 （タイプB規格）	• ISO 13849 • IEC 60204 • IEC 61508† など
製品安全規格 （タイプC規格）	• ISO 26262† • ISO 10218 • IEC 60745 など

ISO/IEC Guide 51が定める安全規格の階層構造

ISO 26262 is the adaptation of IEC 61508 to comply with needs specific to the application sector of electrical and/or electronic (E/E) systems within road vehicles.



† [1], [2], [3]

国際安全規格の目的(例)

- 様々な立場によって国際安全規格に準拠する(参照する)目的が異なる
  - 当社では…
    - 安全性確保の手段、説明責任遂行時の根拠とする
      ⇒ 安全性論証
    - 入札条件や、顧客要求である
    - 他社との差別化、営業戦略として用いる

準拠したことは第三者機関が認証することもある

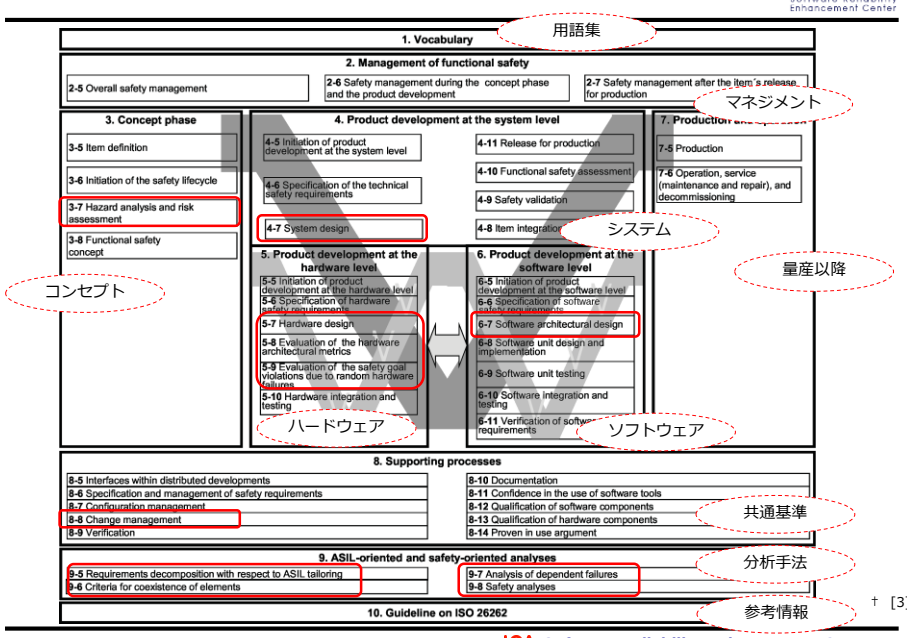
国際安全規格で参照される
従来の安全分析手法の紹介

従来の安全分析手法

- よく知られている安全分析手法
  - FMEA (IEC 60812)†
  - FTA (IEC 61025)†
  - HAZOP (IEC 61882)†
- 国際安全規格では安全分析の実施が求められている
- 安全分析手法は、開発工程、目的に応じて適切なものを選択し、工夫して使用する必要がある

† [4], [5], [6]

ISO 26262†と安全分析(例)



† [3]

国際安全規格における複数回の安全分析

■ IEC 61508では、下記のような記述がある

［フェーズ3の］範囲は、［中略］安全ライフサイクルにかかわるフェーズに依存するであろう（２回以上の潜在危険及びリスク解析を実施する必要があろうから）† [2]

※[フェーズ3の]範囲とは「潜在危険及びリスク解析」

［安全ライフサイクルは、］現実を単純化した図であり、そのため、具体的なフェーズの関わる反復又はフェーズ間の反復の全ては示していない。しかし、反復は、［中略］開発の必須かつ主要な部分である † [2]

複数回の安全分析を示唆

フェーズ3（～5）の反復を行うことが多い

※[フェーズ4]は「すべての安全要求事項」、[フェーズ5]は「安全要求事項の割り当て」

従来の安全分析手法とSTAMP/STPA(第4案)†

手法名	分析方法	特徴
従来手法 FTA,FMEA	● FTAは望ましくない事象をトップ事象として、その要因をツリー状に展開して故障要因を分析する ● FMEAは、構成要素(部品)に起こり得る故障モードを予測し、考えられる原因やシステム全体への影響を分析・評価する ● システムの構成要素(部品)と故障モードが決まる、想定できるアーキテクチャ設計の段階から適用できる	● 構成要素(部品)の故障が事故を引き起こすと考え、その故障を最小化する信頼性工学的手法 ● ドミノモデルやスイスチーズモデルといった故障の一方向への伝搬モデルに基づいて、故障の因果関係を分析する ● 故障要因に故障率を割り当てることで定量的な故障分析ができる ● 人や複雑なソフトウェアの相互作用を伴う複雑システムの故障分析では、全ての故障モードを拾い出すことが難しい ※ HAZOPのガイドワードの考え方で故障モードの網羅性を高めることはできる
STAMP /STPA	● アクシデント、ハザード、安全制約に基づき、安全制御構造図を明示化する(Step-0) ● 4つの非安全制御行動(UCA)に分類してハザードへの影響を分析し、安全制約を詳細化する(Step-1) ● 非安全制御行動を引き起こすハザード誘発要因(HCF)を、制御構造図と経験に基づくガイドワードを用いて分析する(Step-2)	● 故障を低減するという信頼性工学的手法ではなく、事故を回避するための制御行動の乱れを分析する安全制御工学的手法 ● 安全を確保するための制御行動とそのフィードバックという動的システムの中で事故が起こるというモデルに基づく ● 抽象化・階層化したモデルで複雑さを理解するトップダウンのシステム工学的手法で、人・組織や複雑なソフトウェアの相互作用の不具合に伴うハザードを分析する ● 安全制御構造が可視化でき、第三者を含む複数の専門家によるレビューがしやすい。抽象化・階層化したモデルなのでドメイン知識の少ない人でもレビューに参加できる ● 解析する人の能力への依存度が大きい[要議論] ※ モデリング、抽象化の能力が必要

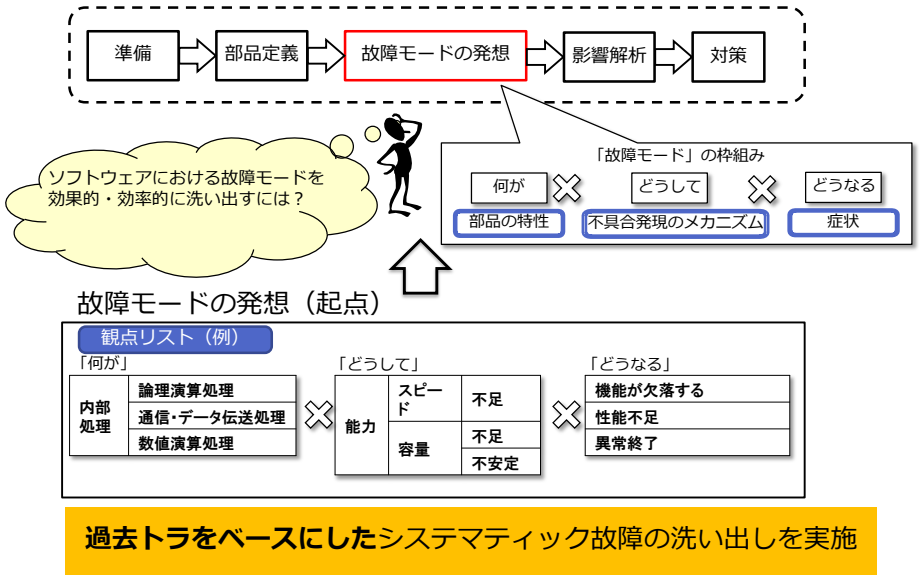
† 会津大学　兼本茂名誉教授作成の資料を一部修正

従来の安全分析手法の使用(当社の事例)

- FMEAでは、(還元的に)各部品・機能の故障モードがどのようにシステムに影響するかを分析する
  - 部品の網羅性
- FTAでは、安全上起きてはいけないことが起きていないことを検証する
  - 全ての安全目標・安全要求を侵害していないこと
- HAZOPは、FMEAやFTAの中で、ガイドワードの考え方を用いる
  - （例えば）故障モードの網羅性

経験知に基づく網羅性によって安全性を論証する

ソフトウェアFMEAとHAZOP(当社の事例) †



過去トラをベースにしたシステマティック故障の洗い出しを実施

† [7], [8]

観点リストの開発手順(当社の事例) †

（0）“組込みソフトウェア一般向け観点リスト”を用意する
(全社で一つ用意)
（1）過去に発現した不具合や制限事項を真因解析し、結果を故障モードにおける3つの属性の組で表現する
（2）手順（1）に対する応用例・類推を考え、列挙する
（3）手順（1）と手順（2）の結果を抽象化する
（4）“製品分野を考慮した観点リスト”に反映すべき結果を選択する
(抽象度の調整やグルーピングも行う)
（5）手順（0）における組込み一般向け観点リストを更新する

■ 経験や実績等をより活かすために以下の内容も手順（1）に含める
- エキスパートの経験や知見

† [7], [8]

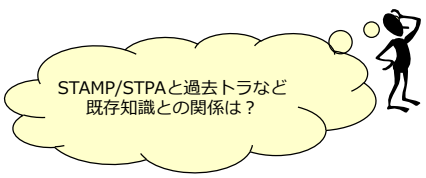
開発現場における従来の安全分析手法

SEC Software Reliability Enhancement Center

■ 現場に浸透している

- 事故が起きたら対策を採るが、FMEAとFTAの分析にはそれらの知見が反映されている

過去トラ、制限事項、既存知識のフル活用



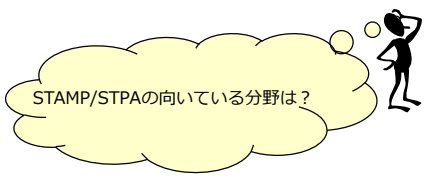
SEC Software Reliability Enhancement Center

国際安全規格に対する
STAMP/STPA適用事例からの知見の紹介

IPA「はじめてのSTAMP/STPA」(2016.3)† 列車の踏切制御装置の事例で分析したときの所感

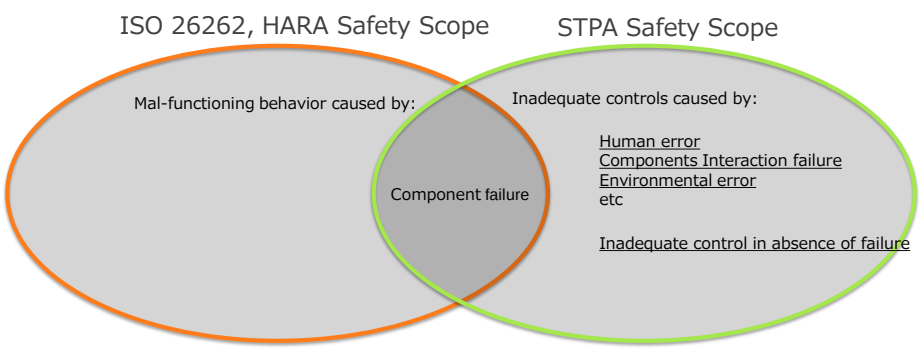
- 十分な過去トラがあるなど、経験知が高い場合にはSTAMP/STPAを行うことによる新しい発見は少ない
- 逆に見れば、経験知の少ない新しいシステム分野や、予見の難しいくらい複雑化したシステムには、向いているのかもしれない

従来手法では洗い出せない、
起きて欲しくないことの発見に対する期待



† [9]

ISO 26262のHARAとSTPAの安全スコープ†



※HARAとはHazard Analysis and Risk assessmentの略(ISO 26262, Part3)
※HARAとSTPAは手法としての基本的な想定が異なっている

STPAをISO 26262の安全スコープを広げた上でISO 26262に
準拠する形で適用している事例～例えば自動運転～

† [11], [12]

ISO 26262†で扱っていないハザード

SEC Software Reliability Enhancement Center

- ISO 26262 addresses possible hazards caused by malfunctioning behaviour of E/E safety-related systems, including interaction of these systems. It does **not** address hazards related to
  - electric shock,
  - fire,
  - smoke,
  - heat,
  - radiation,
  - toxicity,
  - flammability,
  - reactivity,
  - corrosion,
  - release of energy and
  - similar hazards,

unl… of E/E…

Hazard: potential source of harm caused by malfunctioning behaviour of the item

ISO/IECの各規格では要求事項としての範囲を限定している
※規格の要求とは関係なく、製品安全として考慮するのは言うまでもない

STAMP/STPAは広くハザードに対して適用する

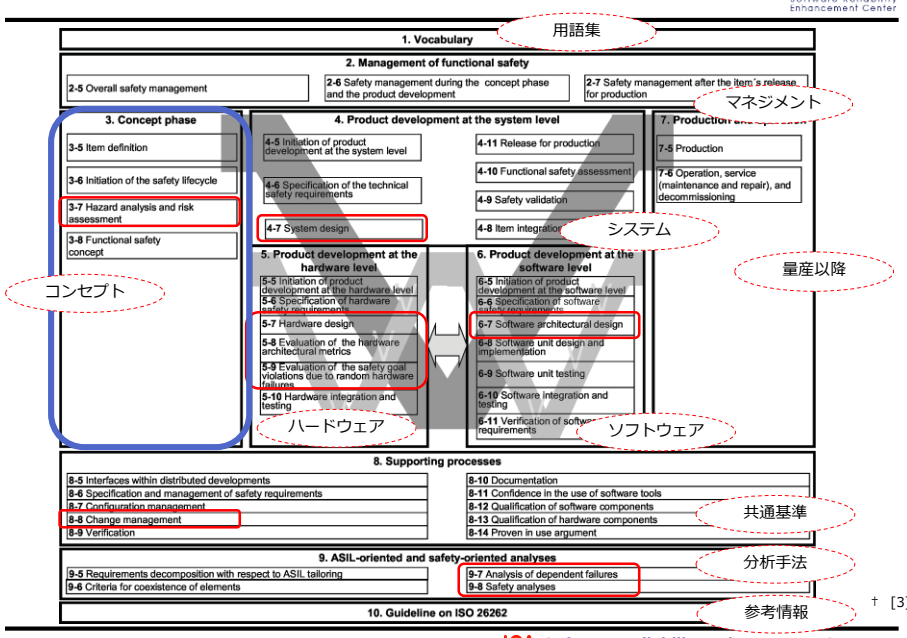
† [3]

(参考)ハザードの違い †

SEC Software Reliability Enhancement Center

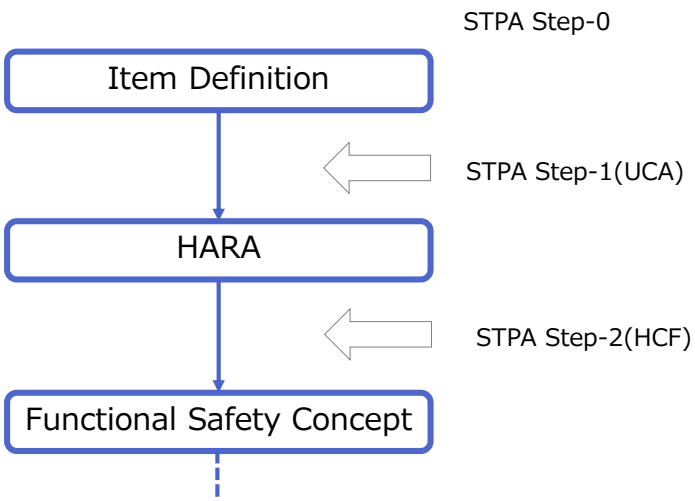
- ハザード(STPA)
  - System states & worst-case environmental conditions which lead to an accident
  - Worst-caseで考えるので、リスク(事象の重大さと発生確率)という概念はない
- ハザード(ISO 26262)
  - Potential source of harm caused by malfunctioning behavior of item(component)
  - リスクは、ハザードのSeverity, Exposure Probability, Controllabilityの組み合わせで評価
    - ハザードを先に定義し危険事象を考える
    - 危険事象にしたがって、それを起こさないための安全目標を決定、安全要求を定義する

ISO 26262†におけるSTPA適用フェーズ(例)



† [3]

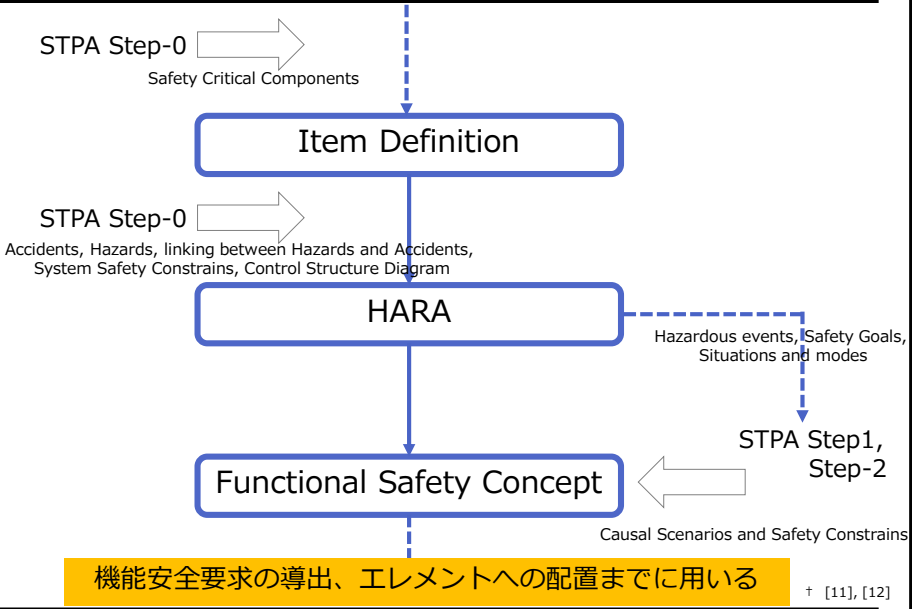
ISO 26262におけるSTPA適用例(1) †



機能安全要求の導出、エレメントへの配置までに用いる

† [13]

ISO 26262におけるSTPA適用例(2)†



† [11], [12]

ISO 26262におけるSTPA適用例(3)

- ハザードや安全制約(安全目標)の精査
- コンセプトフェーズによる安全分析
  - STPAにより、安全制約(安全目標)や、機能安全要求の抜け漏れ、不整合、不完全性を発見することに対する期待
- (正しい)機能安全要求の導出後は従来手法
- 自動運転などの新しい分野、ヒューマンモデル、複雑なシステムに対する利用
  - HCFが特に分からない

いくつかの視点での考察

ISO 26262とSTAMP/STPA適用の考察

- STAMP/STPAの取組みはコンセプトフェーズまでの開発で行っている
- ISO 26262はハザードや状況分析、危険事象について、導出や精査するための明確な手法が定義されていない
- 人、組織、環境を考慮したハザード誘発要因を分析できる(現状の国際安全規格で中心的には扱っていない)
- 事例ではSTAMP/STPAを有効に活用できる可能性を示唆している

国際安全規格の安全論証とSTPAに対する考察

SEC Software Reliability Enhancement Center

- STAMP/STPAは…
  - 全ての部品や機能の故障(故障モード)を洗い出すといった分析に向いているわけではない
  - 例えば、ハザードに対して分析と対策が尽くされたことを説明できないかもしれない

STAMP/STPAの実施だけで安全論証は成立しない

- ISO/IECは…
  - ある特定の制限/条件の下で、ハザードに対して分析と対策が尽くされたことを説明する
  - 新しい、今までに経験のない製品、ステークホルダー全員が素人であるような製品開発には対応しない(ex 自動車の自動運転など)

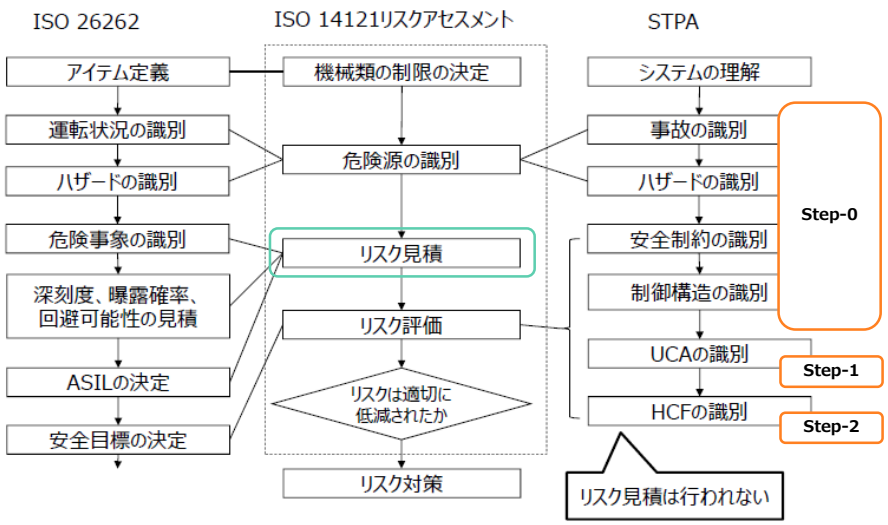
従来の分析手法だけでは難しい

JASPARの試行事例(2016年度版) 他

SEC Software Reliability Enhancement Center

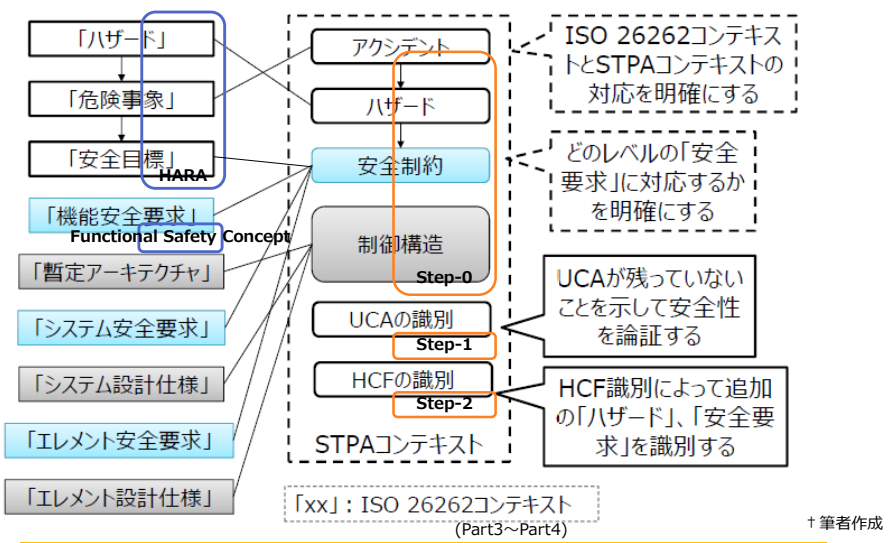
- 自動車のシステム開発(事例)で、ISO 26262における安全論証を考慮しながら、STAMP/STPAを試行
- 安全分析として、使えることは確認している
- この他、各社・各団体同様で効果的な適用プロセスや適用製品、「どこでどう使うのがよいのか？」を検討している

リスクアセスメント標準との関係†



† 筆者作成

ISO 26262とSTPAの関係(別例) †



† 筆者作成

STPAを(粒度の)異なるアーキテクチャレベルで
階層的に複数回用いる例(システム開発の初期段階で用いる例)もある

SEC
Software Reliability Enhancement Center

まとめ

まとめ(1)

SEC
Software Reliability Enhancement Center

- 大前提として、安全分析手法によしあしはない
  - 分析で期待する内容によって使い分ける
  - 製品の各開発工程において適材適所の分析方法を選択する
- 安全分析手法は(使い方次第で)どこでも使える
  - 使用する開発工程によって向き不向きはある
  - STAMP/STPAはISO 26262では、開発の上流工程(コンセプトフェーズ)で用いる例が多く見られる
  - 同じ効果を求めるには実施コストで差が現れるかもしれない

まとめ(2)

- STAMP/STPAは経験知の少ないシステム、複雑なシステム、ヒューマンモデルの分析などに向いている
  - 国際安全規格の安全スコープを広げられる可能性がある
- コンセプトフェーズ以降の工程では従来手法も効率的、効果的に使用できる
  - STAMP/STPAは定量的評価はしない
  - STAMP/STPAは(ボトムアップからの)網羅性を語るのが苦手
- STAMP/STPAだけでは、ISOなどの機能安全規格の準拠性は言いにくい
  - 実施しなければ認証が取れないというものではない
  - 安全の論証性を高めることはできる
  - 使用することそのものは推奨される

参考文献

- 本発表では、以下の文献を元に、IPAなどでの議論をもとに述べました

- [1]ISO 12100：Safety of machinery -- General principles for design -- Risk assessment and risk reduction, ISO, 2010
- [2]IEC 61508 Ed.2.0：Functional Safety of Electrical/Electronic/Programmable Electronic Safety - related Systems, IEC, 2000
- [3]ISO 26262：Road Vehicles – Functional Safety, ISO, 2011
- [4]IEC 60812 Ed.2.0：Analysis techniques for system reliability – Procedure for failure mode and effects analysis, IEC, 2006
- [5]IEC 61025 Ed2.0：Fault tree analysis, IEC, 2006
- [6]IEC 61882：Hazard and operability studies – Application guide, IEC, 2001
- [7]不具合リスク発想のための観点の抽出方法とその効果, ソフトウェア品質シンポジウム, 余宮尚志他, 2016
- [8]観点を用いたソフトウェアにおけるFMEAの効率的・効果的な実施方法とその効果, 先進的な設計・検証技術の適用事例報告書, IPA, 余宮尚志他, 2016
- [9]はじめてのSTAMP/STPA~システム思考に基づく新しい安全性解析手法~, IPA, 2016
- [10]はじめてのSTAMP/STPA~システム思考に基づく新しい安全性解析手法(実践編)~, IPA, 2017
- [11]A systematic approach based on STPA for developing a dependable architecture for fully automated driving, ESW 2016, Daniel Lammering他, 2016
- [12]Using STPA in Compliance with ISO 26262 for developing a Safe Architecture for Fully Automated Vehicles, STAMP Workshop MIT, Asim Abdulkhaleq他, 2017
- [13]Safety Analysis Approaches for Automotive Electronic Control Systems, Qi Van Eikema Hommes, SAE, 2015
- [14]Using STPA in an ISO 26262 Compliant Process, McMaster University, Archana Mallya他,

※番号[*]は本文中で †を用いて引用しています


IPA
Better Life
with IT