ETロボコン走行体システムへのSTAMP/STPA適用事例の紹介

仙台高等専門学校
大友楓雅,菊池雄太郎,力武克彰,岡本圭史

目次

背景

背景

STAMP/STPAとは

- システム理論に基づくアクシデントモデル
- 構成要素の相互作用がもたらす障害の分析に有効

STPAの手順

Step0準備1　アクシデント、ハザード、安全制約の識別
Step0準備2　コントロールストラクチャの構築
Step1　UCA(Unsafe Control Action)の抽出
Step2　HCF(Hazard Causal Factor)の特定

背景

STAMP/STPAの課題

- 比較的公開された適用事例少ない

  (IPAの直近5年の報告書では7件)

- 補助ツールの利用事例さらに少ない

- 「はじめてのSTAMP/STPA」の事例　→　人間系を含まず

目的

目的

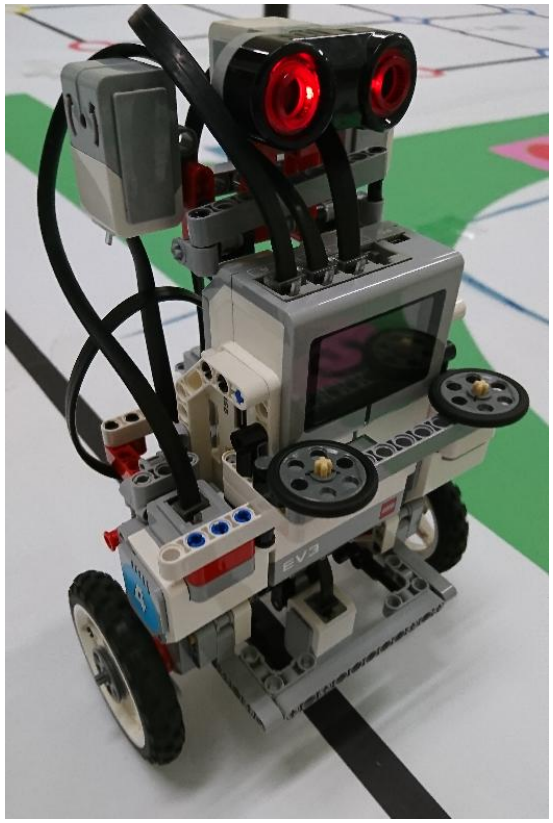
STAMP/STPA分析を志す人への事例提供

その際、以下の３点に留意

1. 運用部分(人間系)を含めた分析の実施
2. 入手が容易な補助ツール(XSTAMPP)の利用
3. 分析用資料の入手容易さ

ETロボコンの概要

ETロボコンの概要



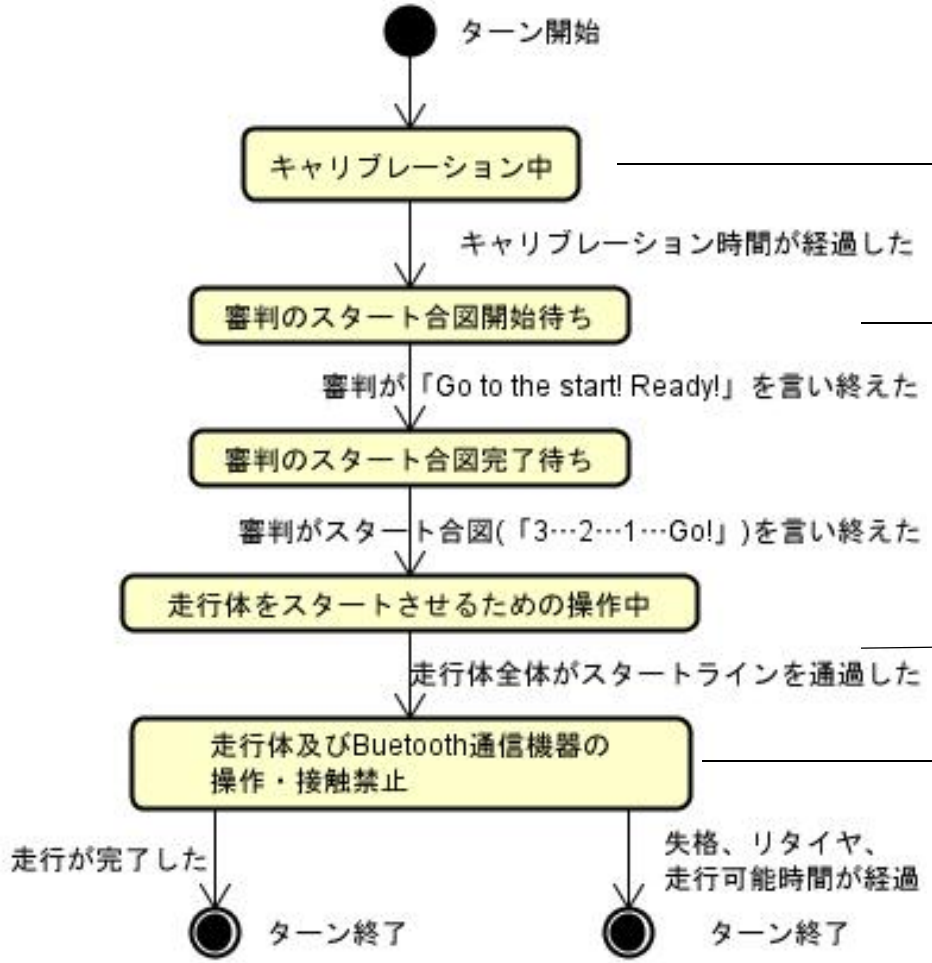
ETロボコン

：共通のロボット（走行体）を用いて
コースを走破するタイムを競う競技

デベロッパー部門プライマリクラスとは

- ジャイロセンサを用いて傾き制御
- 輝度値センサを用いてライントレース
- ゴール後に難所に挑戦可能
  - ➢今回は競技開始からゴールまでを分析対象とした

ETロボコンの概要



キャリブレーション中
輝度値サンプリングと
スタートへの設置

スタートまで
走行体は完全停止状態

スタート後
外部から操作不可

図.ターンでの振る舞い　ETロボコン2016 競技規約から抜粋

XSTAMPPを用いたSTPA

分析手順と利用ツール

• IPAの「はじめてのSTAMP/STPA」を参考に以下の手順で行った

Step0準備1	アクシデント、ハザード、安全制約の識別
Step0準備2	コントロールストラクチャの構築
Step1	UCA(Unsafe Control Action)の抽出
Step2	HCF(Hazard Causal Factor)の特定
最終Step	対策のまとめ

XSTAMPPを利用

Excel,Wordを利用

STPAに用いた情報

- ETロボコン競技規約
- シーケンス図
- プログラムソース
- 前年度の経験

アクシデント・ハザード・安全制約の識別

アクシデント

：望んでもいないし計画もしていない、損失につながるようなイベント

→競技リタイヤとなるイベントをアクシデントに設定

No.	アクシデント	ハザード	安全制約
1	走行体が転倒する	走行体が限度を超えて傾く	走行体の傾きが限度を超えてはならない
2	走行体がコースを外れて復帰不可能になる	コースラインをトレースしない	走行体はライン上に存在しなければならない

元にした情報

- ETロボコン競技規約
- 前年度の経験

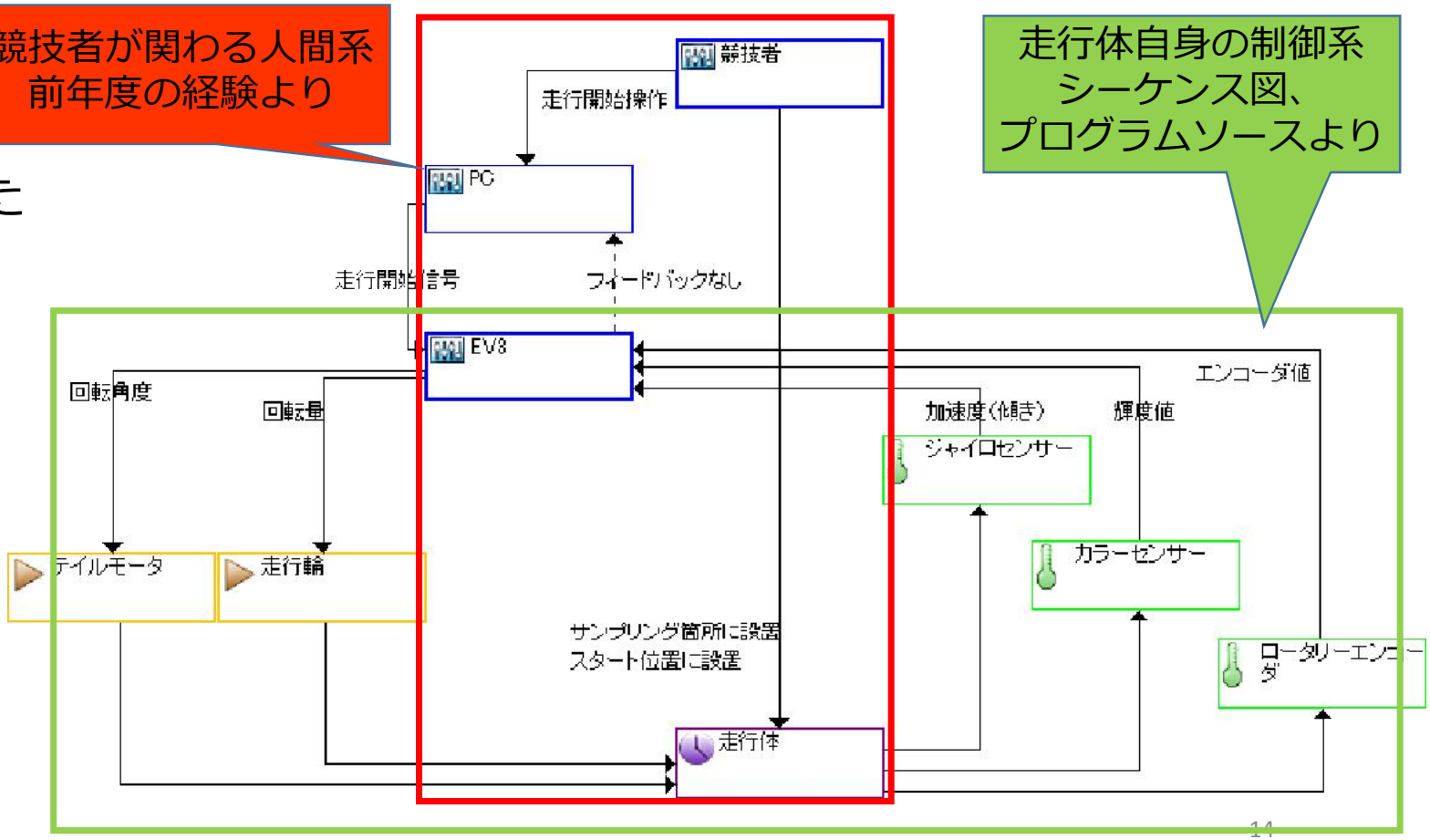
コントロールストラクチャの構築

構築の観点

- 走行体への
  コントロールを探した
- 走行体のパーツは
  別のコンポーネント

試行の結果得た知見

- XSTAMPP利用で
  作図が容易
- 包含関係は示せない



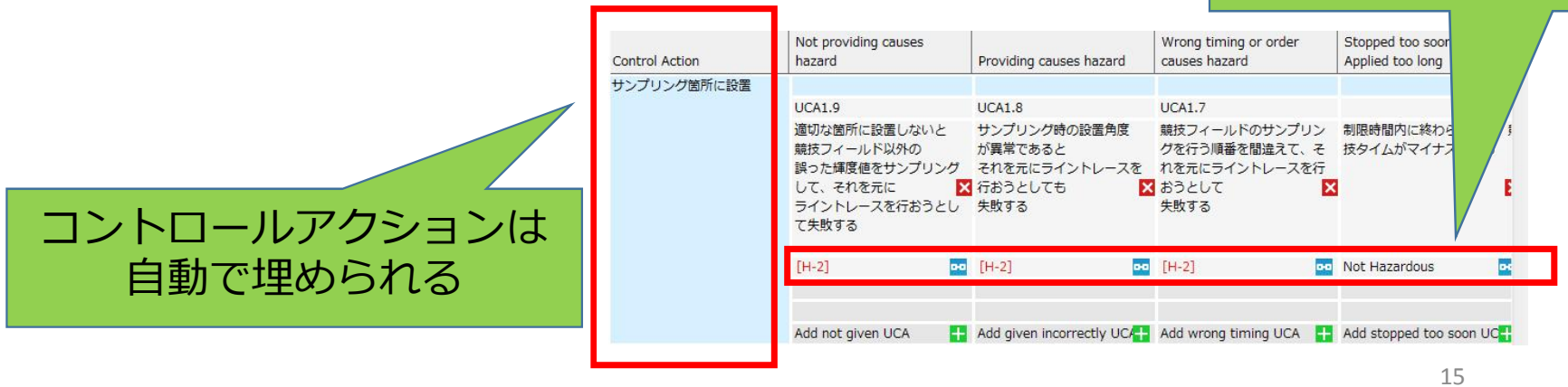
UCAの抽出

抽出の観点

- 前年度、競技スタート時にアクシデント多く経験
  →UCAの発想の手助け

抽出の結果

- 13件のUCAを抽出 (競技スタートに関するUCAは9件)
- XSTAMPPではUCAテーブル作成の手間が減る



抽出したUCAの例

経験から予想できたものと出来ないものがあった

コントロール アクション	どこから	どこへ	XSTAMPPの ガイドワード	UCA	予想
走行開始操作	競技者	PC	Wrong timing/order (Wrong timing)	スタート位置へ設置完了前に走行開始すると、スタート姿勢ではない状態で走り出す	○
スタート位置へ設置	競技者	走行体	Providing	走行体を傾けて設置してスタートすると傾きを立て直せないまま走り出す	○
輝度値サンプリング箇所に設置	競技者	走行体	Wrong timing/order (Wrong order)	複数箇所サンプリングする場合、設置順番を間違えると誤った基準でライントレースすることになる	×
回転量	EV3	テイルモータ	Not providing	テイルが安全な位置に固定されず、走行中に競技フィールドと接触	×

HCFの特定

特定作業の手順

1. UCAとHCF特定用ガイドワードのテーブルのテンプレートを作成

   （ Excel使用。はじめてのSTAMP/STPAの形式を参考）
2. コントロールループとガイドワードの対応を見ながら考える
3. HCF+ハザードシナリオをテーブルに入力

HCFの特定

試行の結果得た知見

- 分析対象の知識が必要

  →今回は前年度の同競技への出場経験から必要知識を得た

- どこにHCF特定用のガイドワードが対応しているか分かり辛い

  →コントロールストラクチャに直接ガイドワードを配置すると良い

対策のまとめ

対策の考案

- 人間系と非人間系どちらにHCFがあるかで大別

人間系HCF

- 「競技者の動きの想定」ヒアリング
- 競技者の認識の変更で対策
  防げない場合　→　プログラム側で対策

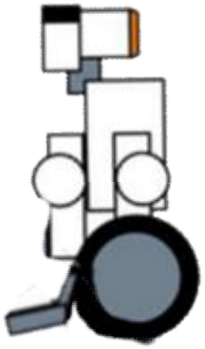
非人間系HCF

- プログラムソースを参考
- プログラム側で対策

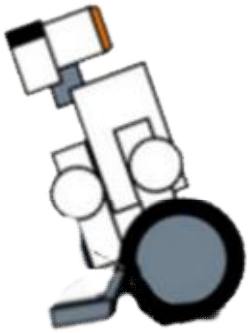
- 結果はHCFのテーブルに追記し、重複するものをまとめた

対策シナリオの例

ControlAction	(走行体を)スタート位置へ設置
UCA	走行体を傾けて設置した状態で、 そのままスタートさせたため走行体が転倒
HCF	競技者の感覚に任せた不正確な操作
ハザード シナリオ	競技者が、機体角度を自身の感覚で決めて、 設置する。スタート後2輪走行を開始するが、 設置角度が不適切な場合立て直しきれず転倒
対策	スタートまで、機体角度が不適切なことを 検知し競技者に通知



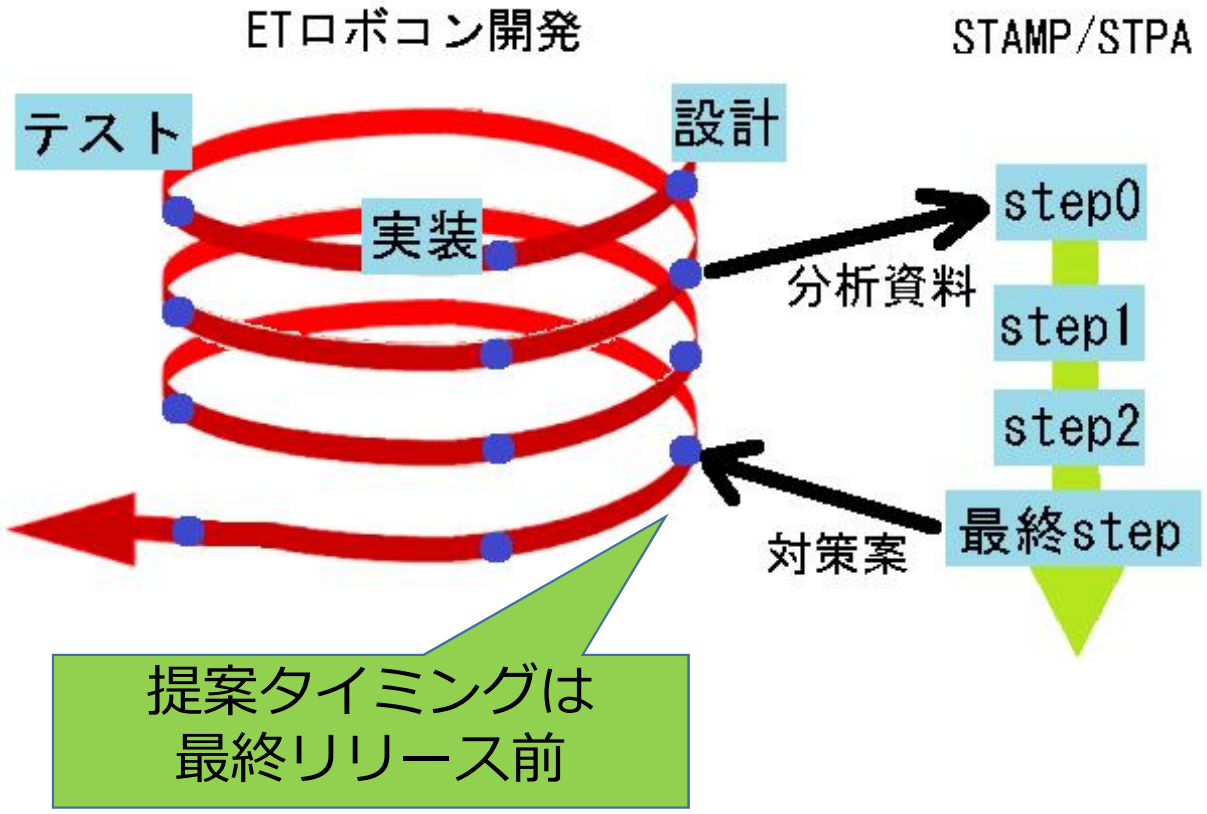
適切なスタート姿勢



傾いたスタート姿勢

感覚に頼らず定量的基準を作る

今回の開発と分析の関係



分析資料
- ETロボコン競技規約
- UML図
- プログラムソース

対策案(Word形式)
- ハザードシナリオ
- 対策

対策の採用・非採用

- 考案した対策のうち一部のみ採用された

採用された対策の例

- 競技者の競技中における行動手順書の作成
- 輝度値サンプリングが終了するまでスタート姿勢にならないようにする

採用されなかった対策の例

- 輝度値サンプリングのやり直し機能をとりいれる
- サンプリングした輝度値が想定の範囲外の場合通知する

微修正でOK

採用されなかった理由：コスト

新機能必要

対策の採用・非採用

別な形で採用された対策

- ハザードシナリオ

  競技者が走行体角度を自身の感覚で決めて、設置する。
  スタート後2輪走行を開始するが、設置角度が不適切な場合
  立て直しきれず転倒

- 対策　：スタートまでの間、機体角度が不適切なことを
  ロータリーエンコーダから検知し競技者に通知

要機能追加
コスト高

低コストでの対策

ほぼ直立状態をスタート姿勢として設定し、
不適切な角度では設置が行えないように、テイルを制御

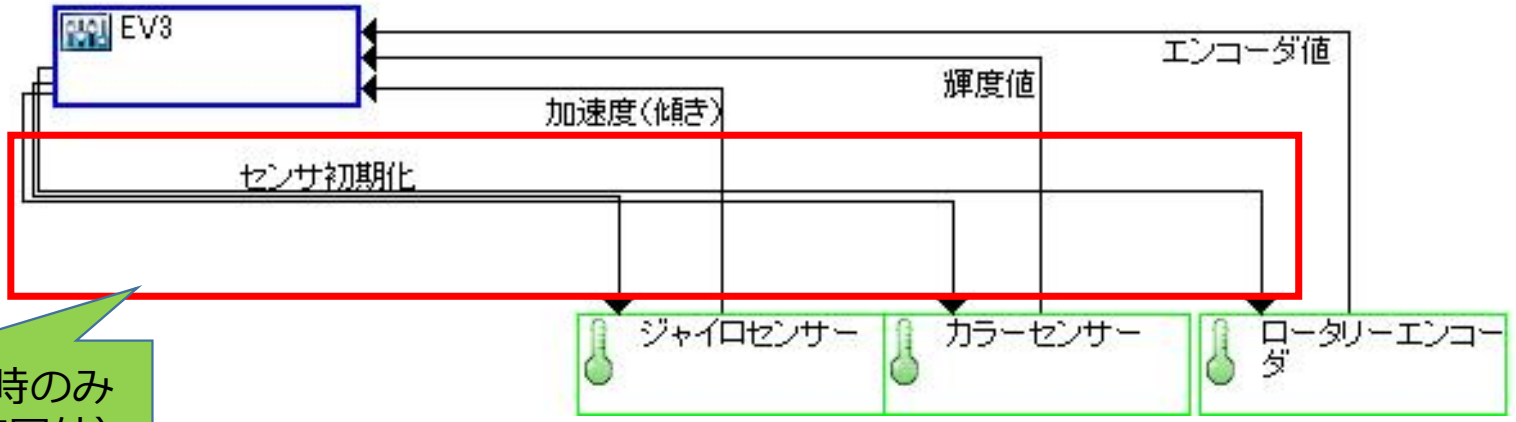
微修正でOK
コスト低

競技の結果

結果　競技中にアクシデント「走行体が転倒する」が発生

STPAを再度試行

- センサに対するコントロールアクションが抜けを発見



システム起動時のみ
（前回は分析範囲外）

2度目のSTPAの結果

新たに抽出できたUCA

- 走行体が静止していない時にセンサ初期化されると、
  ジャイロセンサが正しく働かなくなり傾きを誤認識する

対応するHCF

- センサ初期化や輝度値サンプリングを開始するタイミングが
  不明確であるため、想定した順序で行われない

追加対策案

1. センサ初期化は競技前に開始し、静止状態で行う
2. センサ初期化が終わるまで、輝度値サンプリング位置へ設置は行わない

採用を想定し
運用面で対策

まとめ

まとめ

ETロボコンを運用部分も含めSTAMP/STPAを実施

- UCAの抽出まではXSTAMPPを利用
- ガイドワード適用により、既知ではないUCAも抽出

対策案を開発者へ提案

- 実装コストの低いものは採用
- ハザードシナリオと併せて提案することで開発者は代替案を提案可能

競技本番ではアクシデント発生防げず

- 再度STPA実施、コントロールストラクチャ構築の不備が原因？