倒立二輪車の人間・機械協調システムのSTAMP解析

STPA analysis for human-machine interaction system using two-wheel-pendulum

2016. 12. 6

IPA/SEC　佐々木 千春

Agenda

- 背景 Background
- ロボットの紹介 What's Robot?
- STPAの実施 Using STPA
- 実施結果を基にした対策の適応 Implementation of measures
- まとめ Summary

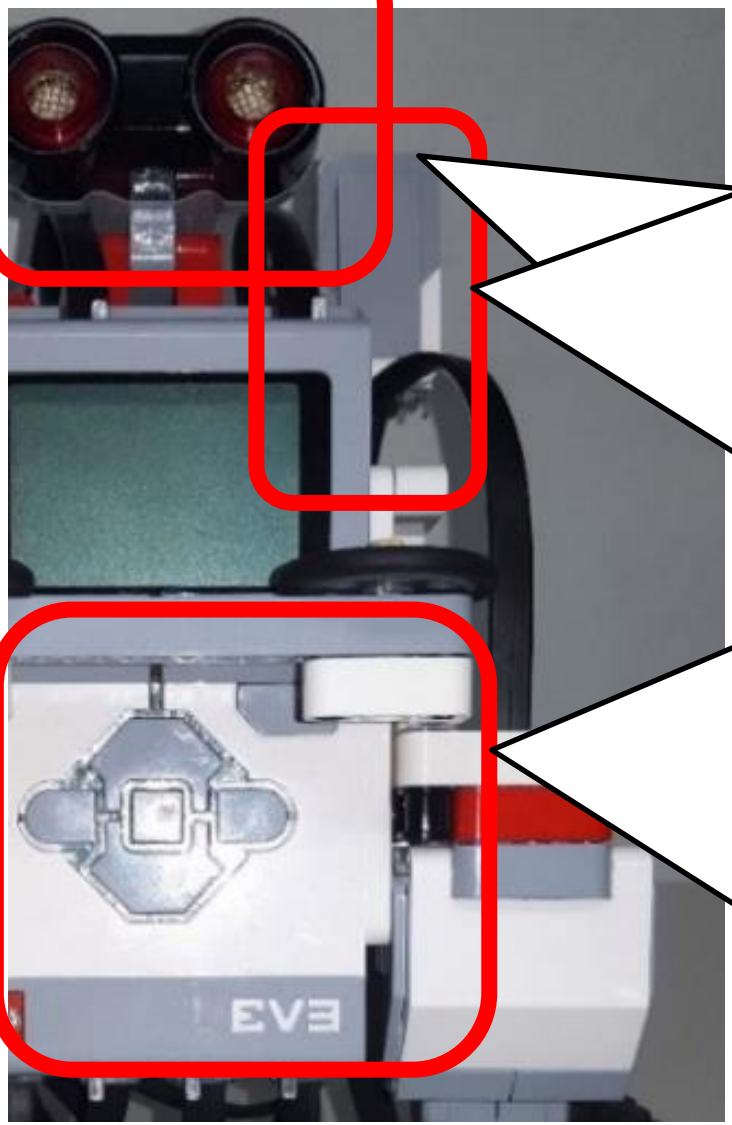
背景 Background

- ソフトウェアが高機能化するに伴い、航空機・自動車・ロボットをはじめとした、人間と機械が協調したシステムが広く登場している。
- 一方でソフトウェアの不具合によって人間に危害を与えたり、大きな経済損失を与える危険性が高まっている。システムが安全であることを担保することも重要になってきている。
- 如何にして、人間と機械が協調するシステムの安全を担保するかが重要となる。
- 人間と機械が協調するモデルとして、二輪倒立ロボットをベースにユーザーの操作機能を追加したシステムを構築し、STPAを実施する。

ロボットの紹介

- **名称**
  LEGO Mindstorms EV3
  ロボコン(JASA ET**ロボコン**)**等で使用される、主に教育用とに利用されるロボット**
- **性能**
  CPU: ARM9
  MEM:16Mb(Flash)+64Mb(RAM)
  10年前の携帯/ゲーム機と同じぐらいの性能
- OS:BrickOS
- I/O
  Sensor Input(4 port)
  Motor Output(4 port)
  Wifi/Bluetooth
- **ロボットの最大速度**(MAX Speed)
  約44cm/s

ロボットの紹介



[Function] Manipulate Robot

ロボット操作

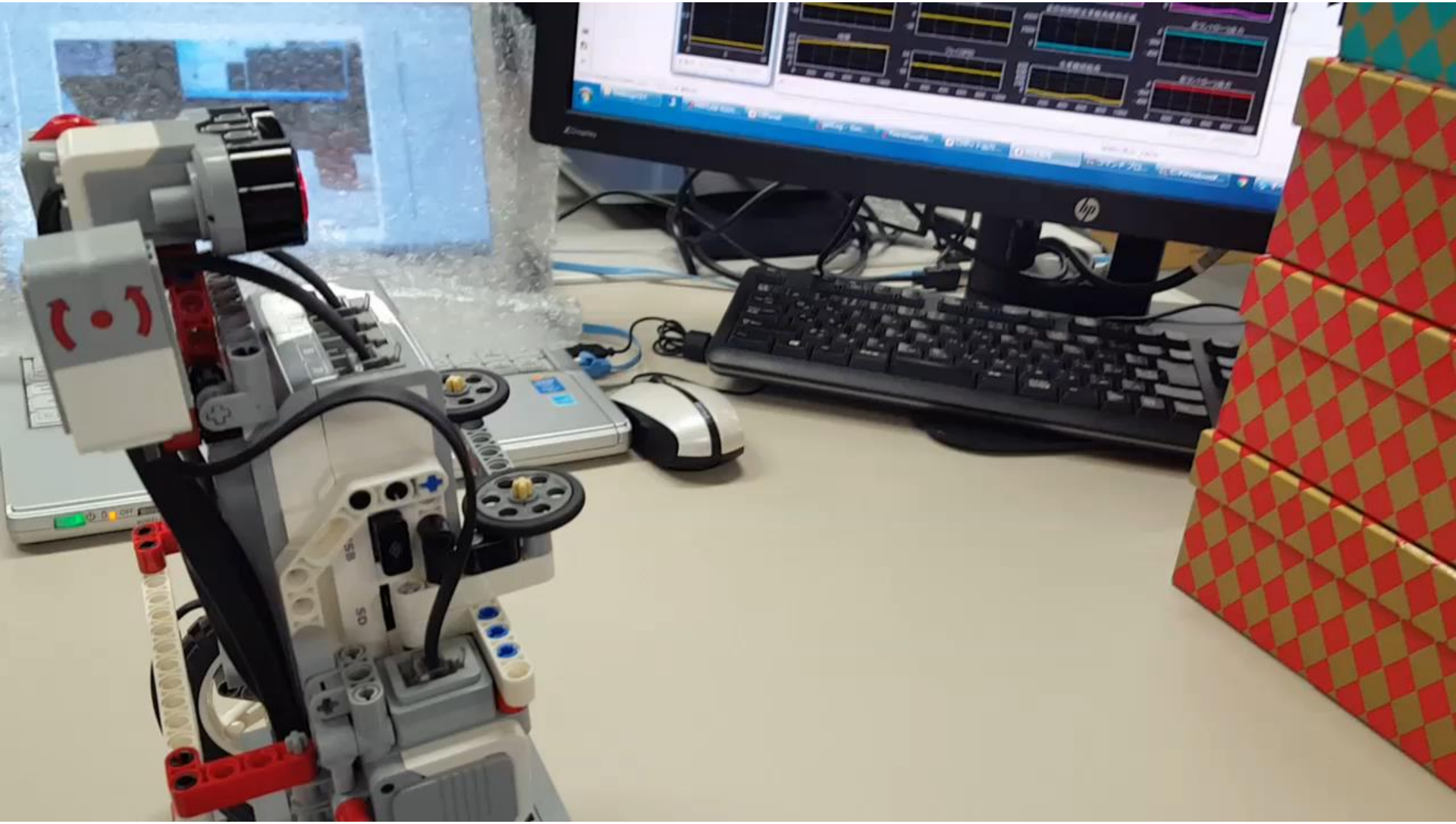
外部パッドによりロボットの前後、左右操作を行う。

自立制御はロボット自身が、ロボットの移動はユーザーがそれぞれ制御する

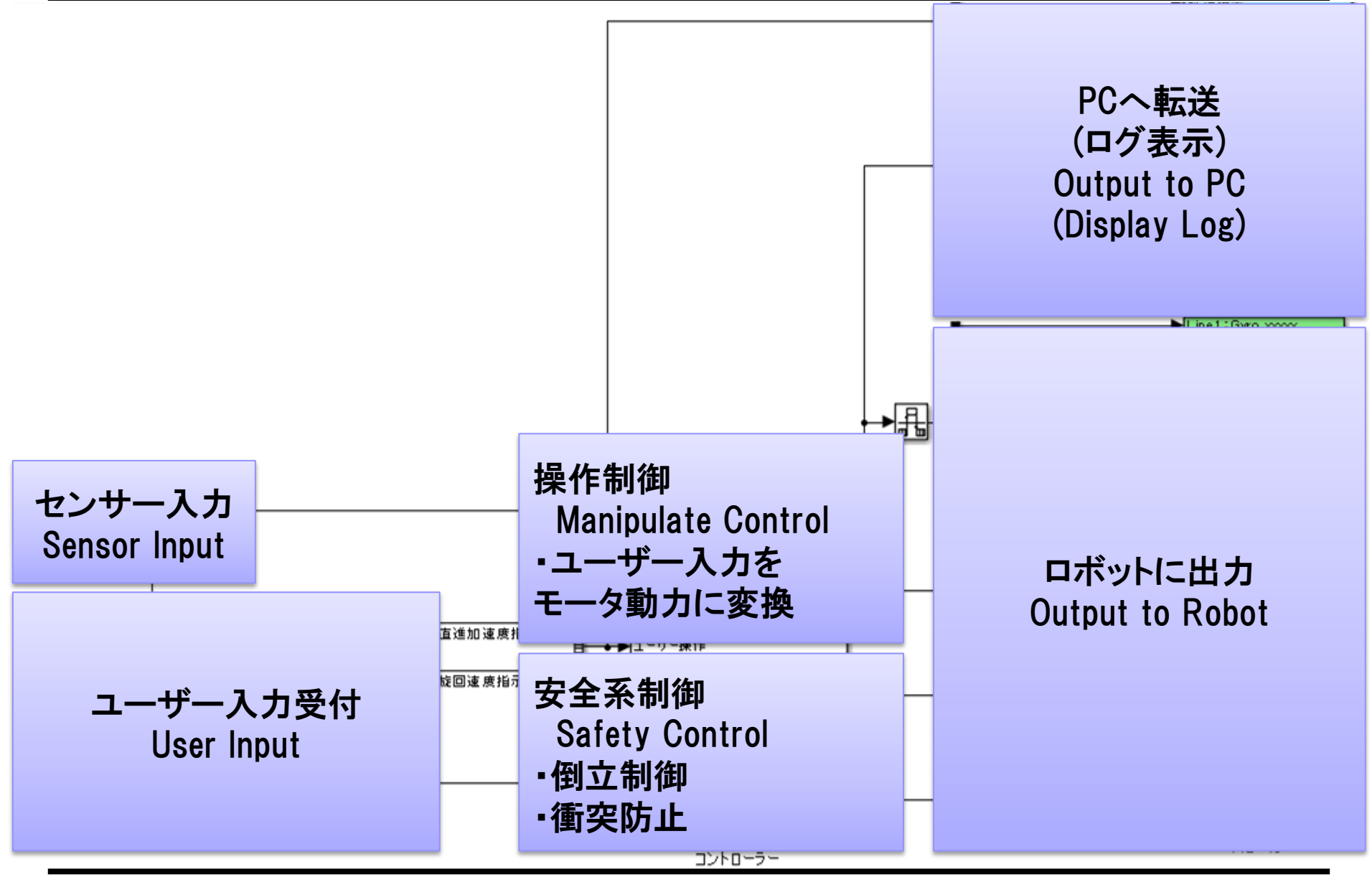
ロボットの紹介

SEC
Software Reliability
Enhancement Center

ロボットの紹介



ロボットの紹介



STPAの実施

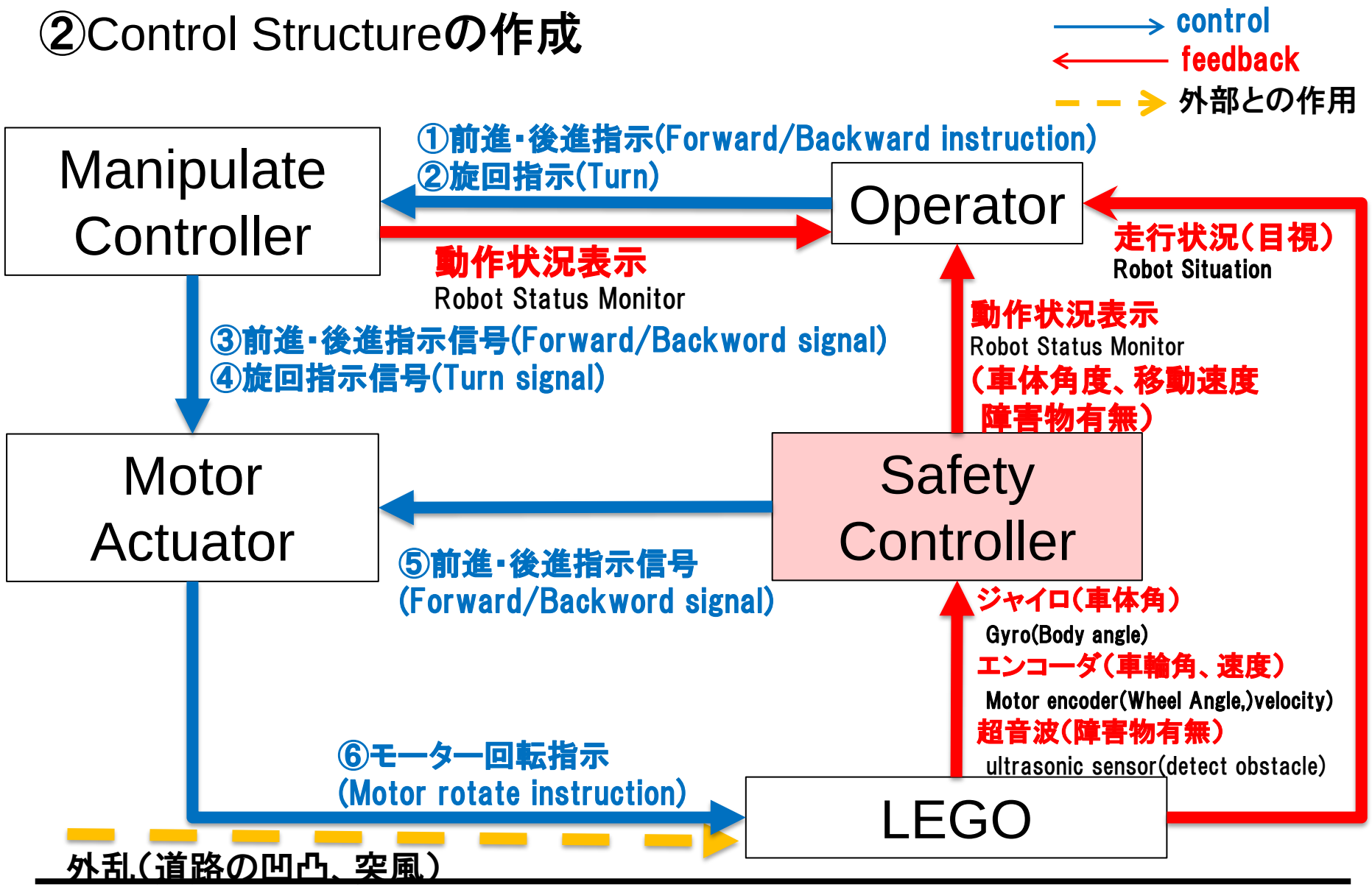
SEC Software Reliability Enhancement Center

①Accident, 安全機能, Hazard, Safety Constraintの定義

- **Accident**　損失に繋がるようなイベント
  - [A-1] ロボットが転倒する fall
  - [A-2] ロボットが障害物にぶつかる collide with obstacle
- **安全機能**safety function　アクシデントを防ぐために用意された機能
  - ロボットの重心を一定に保つ姿勢制御機能
  - 障害物を検知したら停止する衝突防止機能 anti-collide function
- **Hazard**　アクシデントに繋がるような安全機能の状態、条件
  - [H-1] ロボットの重心が制御可能域を逸脱する
  - [H-2] 障害物を検知しても停止が間に合わない
- **Safety Constraint**　ハザードからシステムを安全に保つための要件・制約
  - [SC1-1] ロボットの重心を常に制御可能範囲内に抑える
  - [SC2-1] 衝突防止策が間に合う範囲で障害物検知する

STPAの実施

②Control Structureの作成



STPAの実施

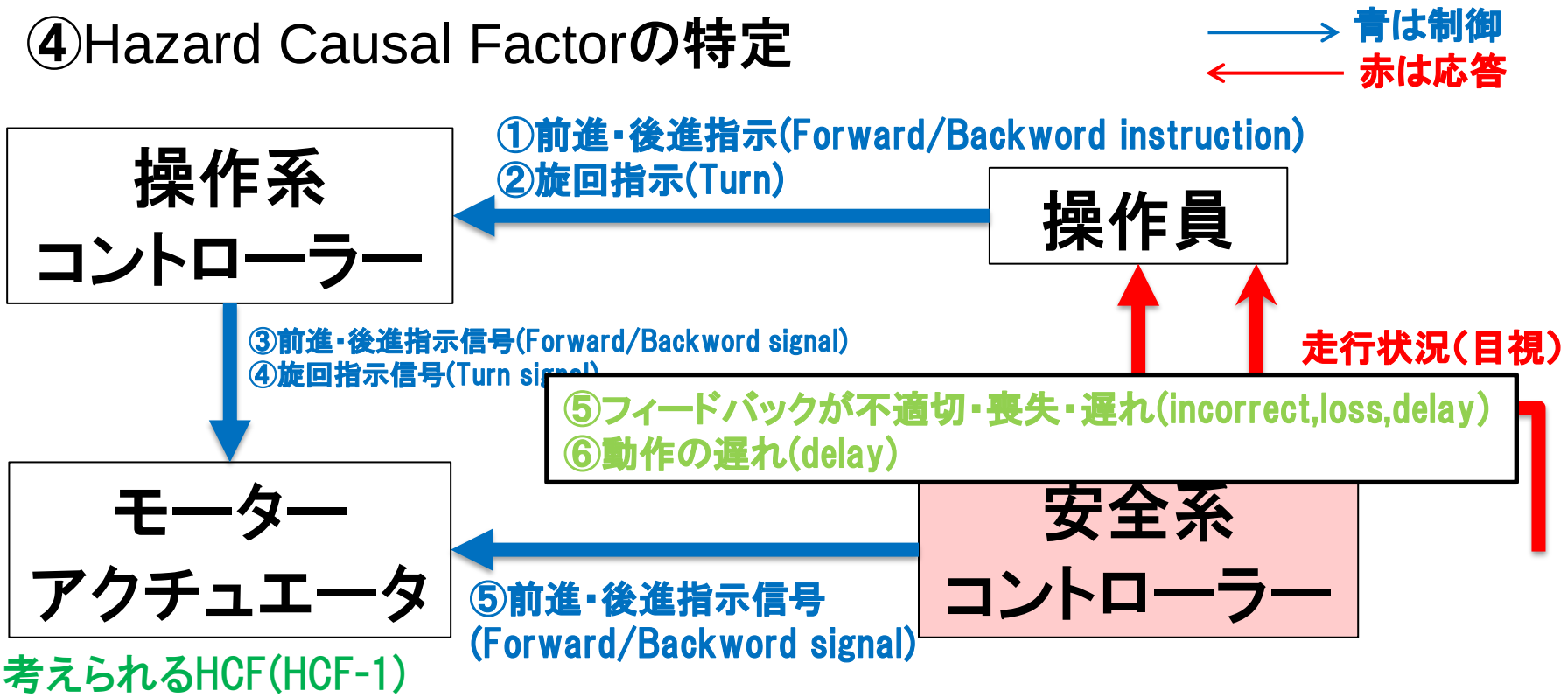
SEC Software Reliability Enhancement Center

③Unsafe Control Actionの抽出

#	Control Action	Source Controller	Destination	Not Providing	Incorrectly Providing	Too early / Too Late	Stop too soon /Applying too long
1	Forward/ Backward	Operator	Manipulate Ctrl-er	- None -	(UCA1-P)LEGOが不安定な状態での前進・後進指示による転倒 (HC1-1違反)	- None -	- None -
2	Turn	Operator	Manipulate Ctrl-er	- None -	(UCA2-P)LEGOが不安定な状態での旋回指示による転倒 (HC1-1違反)	- None -	- None -
3	Forward/ Backward	Manipulate Ctrl-er	Motor Actuator	- None -	(UCA1-P)LEGOが不安定な状態での前進・後進指示による転倒 (HC1-1違反)	- None -	- None -
4	Turn	Manipulate Ctrl-er	Motor Actuator	- None -	(UCA2-P)LEGOが不安定な状態での旋回指示による転倒 (HC1-1違反)	- None -	- None -
5	Forward/ Backward	Safety Ctrl-er	Motor Actuator	(UCA3-N)LEGOの重心を制御できず転倒 (HC1-1違反) (UCA4-N)障害物前で停止できず衝突 (HC2-1違反)	(UCA3-P) LEGOの重心を制御できず転倒 (HC1-1違反) (UCA5-P)障害物前で前進してしまい衝突 (HC2-1違反)	(UCA3-T) LEGOの重心を制御できず転倒 (HC1-1違反) (UCA4-T)障害物前で停止できず衝突 (HC2-1違反)	- None -
6	Motor rotate	Motor Actuator	LEGO	(UCA3-N)LEGOの重心を制御できず転倒 (HC1-1違反)	(UCA3-P) LEGOの重心を制御できず転倒 (HC1-1違反) (UCA5-P)障害物前で前進してしまい衝突 (HC2-1違反)	(UCA3-T) LEGOの重心を制御できず転倒 (HC1-1違反) (UCA4-T)障害物前で停止できず衝突 (HC2-1違反)	- None -

STPAの実施

④Hazard Causal Factorの特定



考えられるHCF(HCF-1)

段差の前後で操作員が急な前進、後退命令をだし、LEGOの姿勢が不安定になった。操作員は復帰を操作系コントローラーに指示を出すことにより試み、操作系コントローラーはモーターアクチュエーターに対し後退指示を正しく出した。一方で、安全系コントローラーも姿勢安定化のためにモーターアクチュエーターに対し前進・後進指示信号を出した。この際、安全系コントローラーは前進命令を、操作系コントローラーは後退命令を出したため、モーターアクチュエータはその合算値:0をモーターに伝え、結果LEGOはモーターを動かさず、転倒した。

STPAの実施

SEC Software Reliability Enhancement Center

④HCFの特定⇒対策案検討

[推定される原因]

段差の前後で操作員が急な加速、減速命令をだし、LEGOの姿勢が不安定になった。操作員は復帰を操作系コントローラーに指示を出すことにより試み、操作系コントローラーはモーターアクチュエーターに対し後退指示を正しく出した。一方で、安全系コントローラーも姿勢安定化のためにモーターアクチュエーターに対し前進・後進指示信号を出した。この際、安全系コントローラーは前進命令を、操作系コントローラーは後退命令を出したため、モーターアクチュエータはその合算値：0をモーターに伝え、結果LEGOはモーターを動かさず、転倒した。

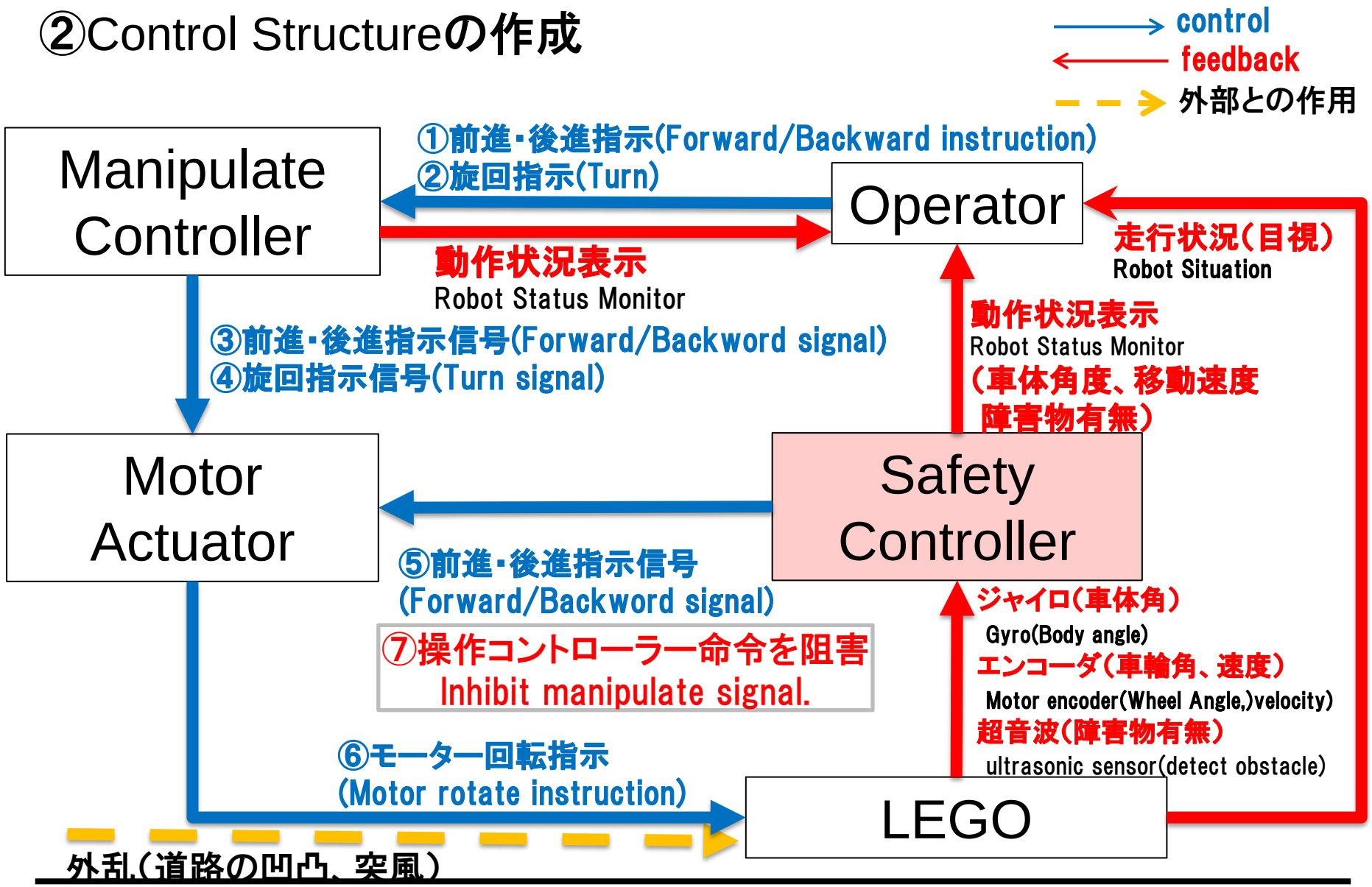
[対策案]

- 操作要求信号に対して、最大速度と最大加速度、加加速度を制限する（PID制御との干渉、UTの停止指示と操作要求信号の干渉による転倒防止）
- ジョイスティックから手を放すと停止する安全設計
- ルールベース制御(ロボットが不安定な時は操作系コントローラー入力を受け付けない)の採用
- 衝突防止時/ルールベース制御時にロボットから音を出して、操作員に衝突防止が働いていることを知らせる。

STPAの実施

SEC Software Reliability Enhancement Center

②Control Structureの作成

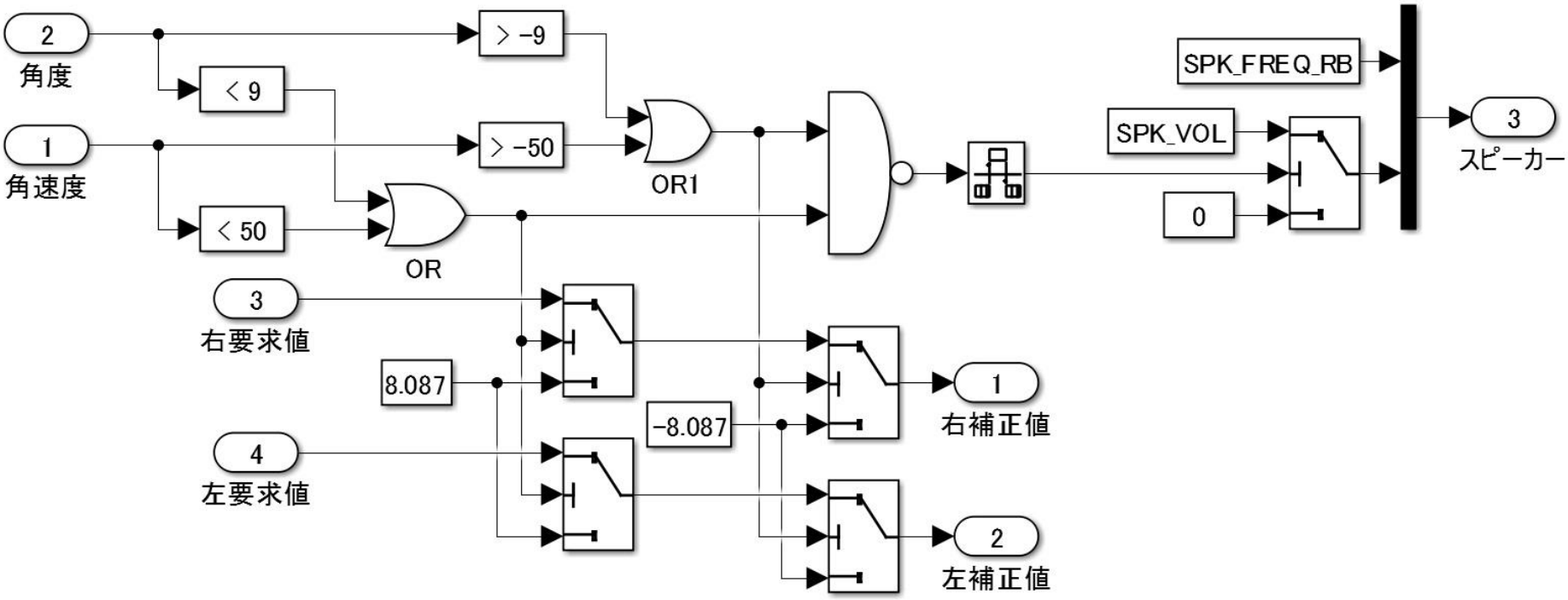


実施結果を基にした対策の適応

ルールベース制御 rule-based control

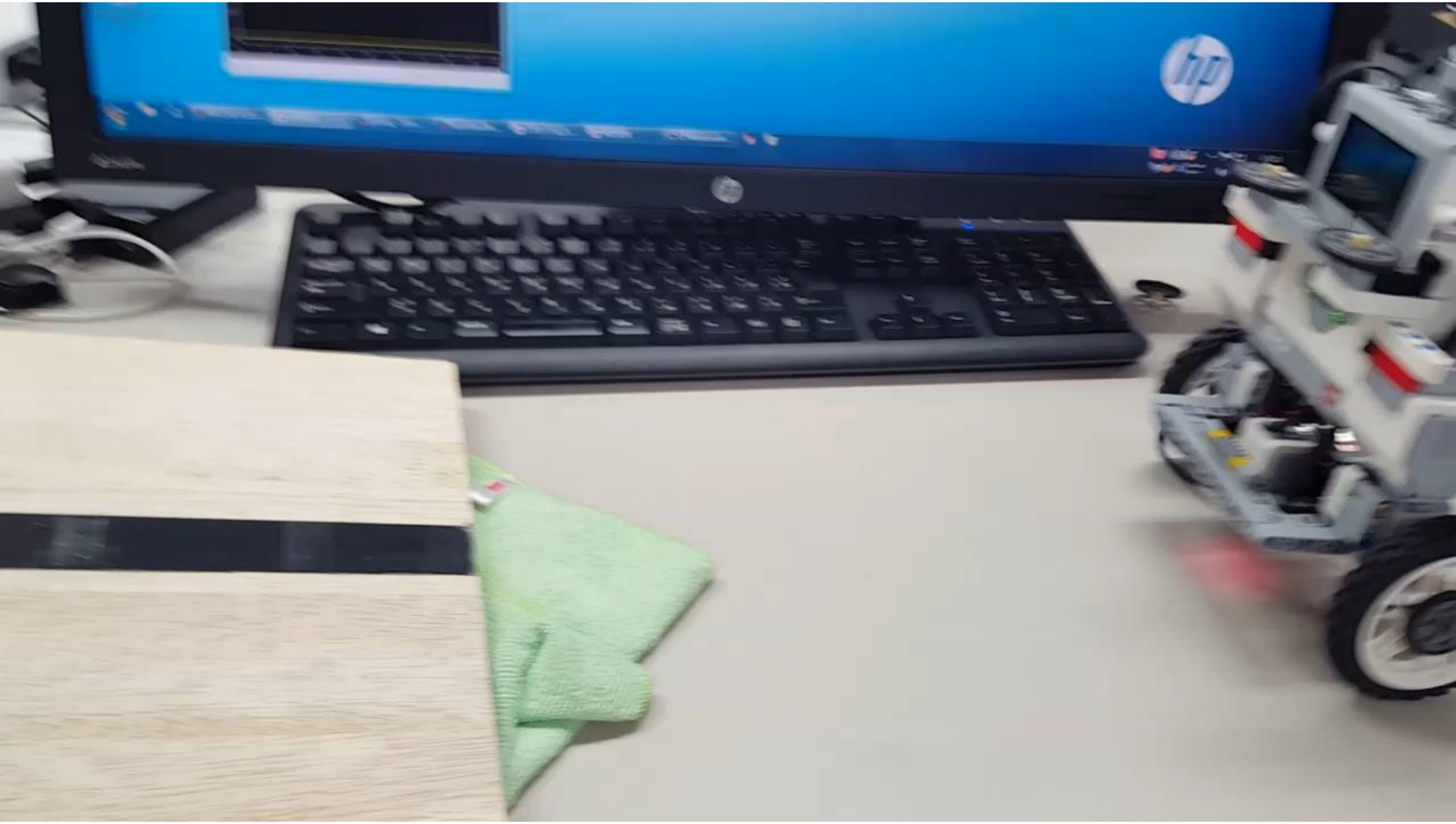
以下のいずれか条件でユーザー入力を無視する⇒姿勢制御のみを行う

- 車体角度が一定以上になった。
- 車体角速度が一定以上になった。



実施結果を基にした対策の適応

SEC
Software Reliability
Enhancement Center



まとめ

- STAMP/STPAを用いることで、二輪倒立ロボットを用いた人間、機械の協調制御システム、および周辺状況の記述から、安全制約を脅かす要因の絞り込みまでを一通り行うことが可能であった。

- この要因への対策を行うことで、ロボットの動作が変化し、対策が効果をなしていることも確認できた。

- この対策により新たなUnsafe Control Actionが生じていないかの確認、さらには環境条件が変わった場合にはその変更を反映しての再度の分析が必要である。