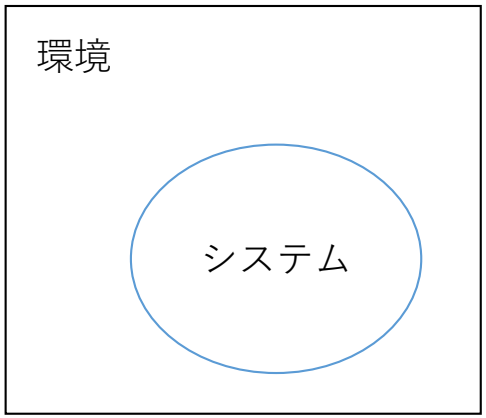
ETロボコンにおける STAMP/STPAの試行および ウエブベースSTPAツールの 設計と開発

阿部惇朗、古川優也、松野裕
日本大学
岡本圭史
仙台高専

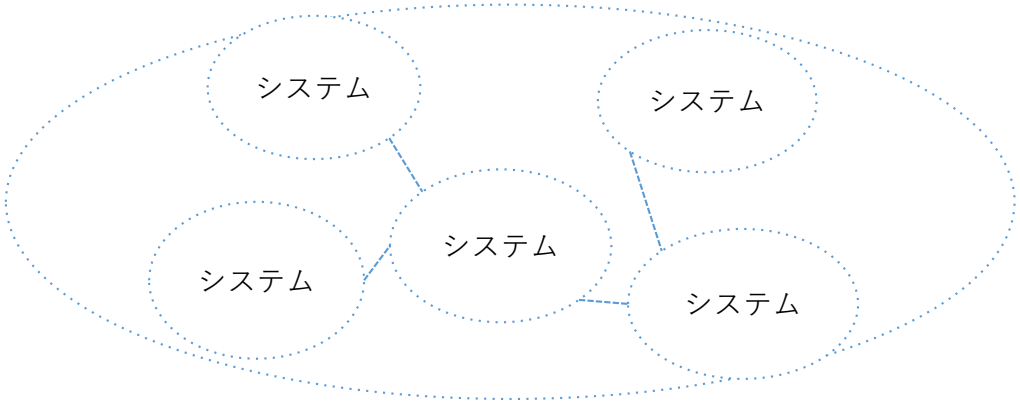
内容

- 研究背景: 複雑化するシステムのリスク分析
- ETロボコンにおけるSTAMP/STPAの試行
- 他のリスク分析手法との比較
- 試行をもとにしたSTAMP/STPAツールの設計
- ウエブベースツールの開発およびデモ

研究背景: 複雑化するシステムのリスク分析



これまで：閉じた環境でのシステム



これから：複雑・ネットワーク化する環境とシステム
→　オープンシステム

システム系全体の
安全性、セキュリティのリスク分析はより重要になる

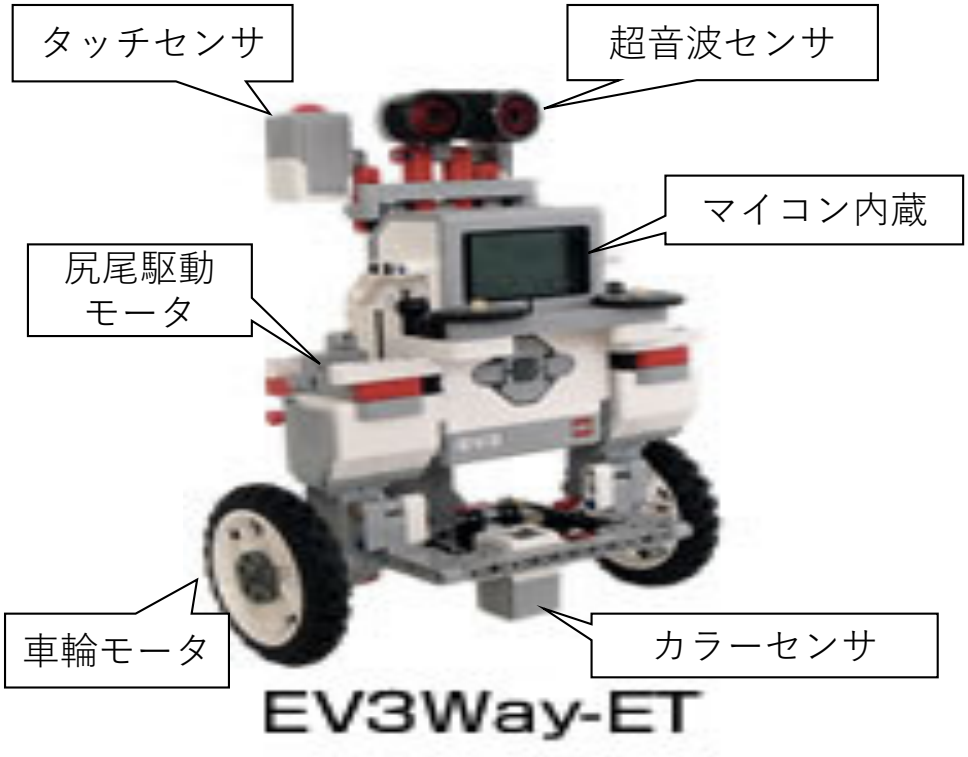
STAMPが注目

ETロボコンにおけるSTAMP/STPAの試行

・ETロボコン

「組込みシステム」分野における技術教育をテーマに、決められた走行体で指定コースを自律走行する競技。
同一のハードウェアに、UML等で分析・設計したソフトウェアを搭載し競う。
ソフトウェアの優劣を競うコンテスト。

URL:http://www.etrobo.jp/2016/



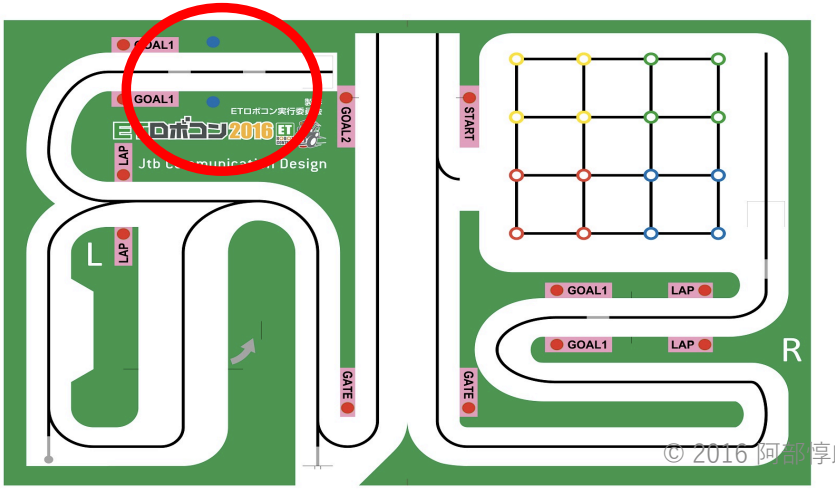
URL:http://www.etrobo.jp/2016/

ETロボコンにおけるSTAMP/STPAの試行

・ルックアップゲートを分析対象

255mmの走行体で235mmのルックアップゲートをくぐる難所の一つ

超音波センサでルックアップゲートを検知し、尻尾を出して傾斜して走り、ゲートを通過する



http://news.mynavi.jp/articles/2011/12/22/etrobocon2011_championship/

Step0　準備１：アクシデント、ハザード、安全制約の識別

・アクシデント：喪失（Loss）を伴う、システムの事故。
・ハザード：アクシデントにつながるシステムの状態。
・安全制約：システムが安全に保たれるために必要なルール。

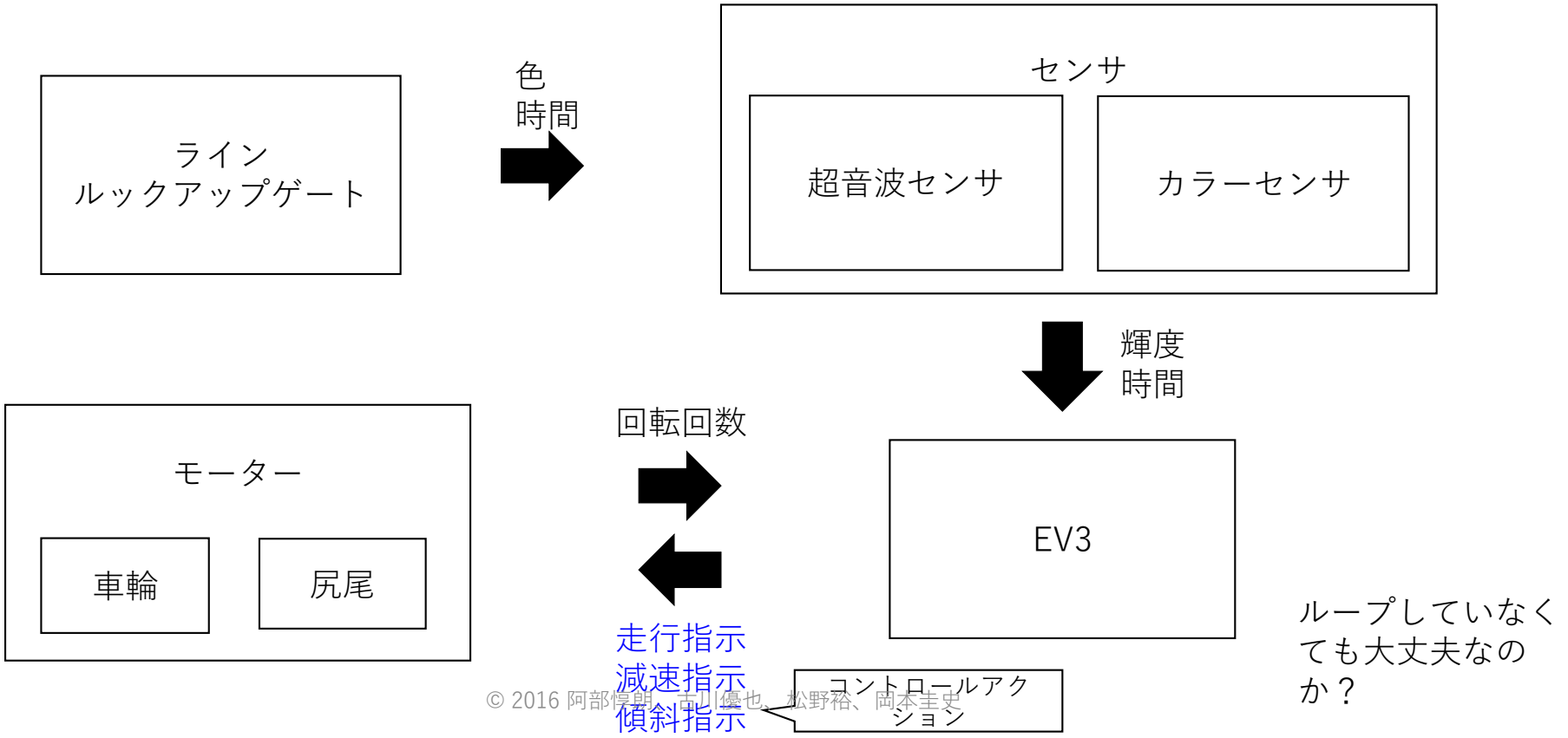
表　アクシデント、ハザード、安全制約の識別

アクシデント	ハザード	安全制約
ゲートに接触	車体が適切な角度まで傾いていない	車体が傾くまで走行してはいけない
コースアウトする	ライントレースできていない	EV3は常にラインをトレースしなければならない
傾斜時に転倒	スピードが速い	ゴール後に一定の速度になっている

初めてのSTAMP/STPA参照

Step0　準備２：コントロールストラクチャの構築

ルックアップゲート通過のコントロールストラクチャ



ループしていなくても大丈夫なのか？

Step1：安全でないコントロールアクション（UCA）の識別

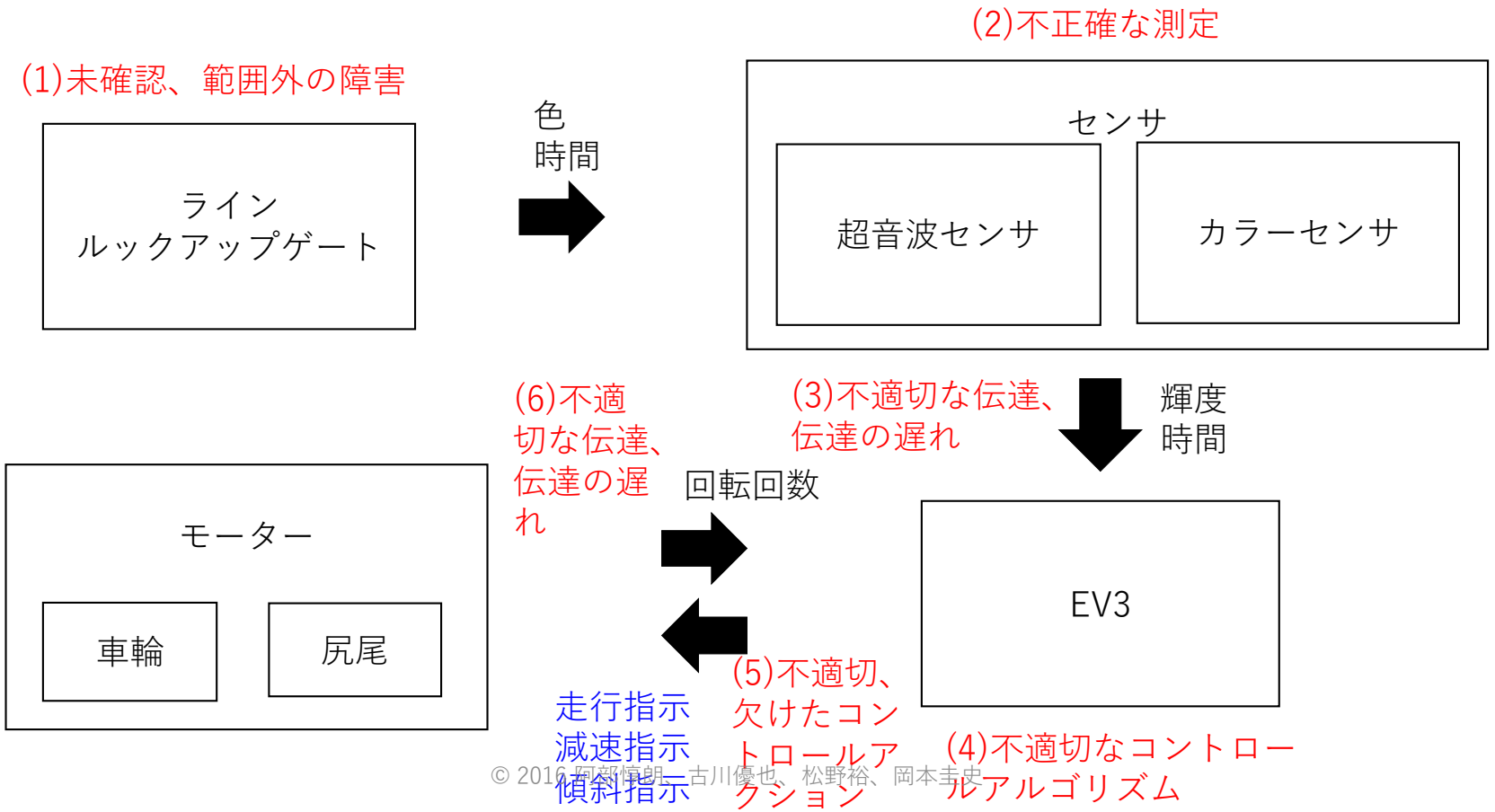
表　UCAの識別

コントロールアクション	与えないとハザード	与えるとハザード	早すぎ、遅すぎ、誤順序でハザード	早すぎる停止、長すぎる適用でハザード
傾く	超音波センサからEV3に測定結果が伝わらないため、傾かない UCA1	超音波センサからEV3に誤った測定結果を伝えたため、傾かない UCA3	超音波センサからEV3に測定結果が遅れて伝わるため、ゲートにぶつかる UCA5	EV3からモーターへのコントロールアクションが早すぎる停止により適切な角度まで傾かない UCA7
	EV3からモーターに命令が伝わらないため、傾かない UCA2	EV3からモーターに誤った命令がつたわるため、傾かない UCA4	EV3からモーターに命令が遅れて伝わ	
減速	モーターからEV3に測定結果が伝わらないため、距離が測れず減速できない UCA8	モーターからEV3に 伝わるため、任意の る UCA9		
走行	カラーセンサからEV3に測定結果が伝わらないため、コースアウトする UCA11	カラーセンサからEV 果を伝えたため、コ UCA13		すぎる停止により、コー
	EV3からモーターに命令が伝わらないため、コースアウトする UCA12	EV3からモーターに誤った命令を伝えたため、コースアウトする UCA14	EV3からモーターに命令が遅れて伝わるため、コースアウトする UCA16	走行命令が長すぎる適用により、コースアウトする UCA18

モーターからEV3に測定結果が伝わらないため、距離が測れず減速できない
UCA8

Step 2 ：Hazard Causal Factorの特定

ルックアップゲート通過のコントロールストラクチャ



Step 2 ：Hazard Causal factorの特定

対処可能な範囲なものを赤として選んだ

表　HCFの特定

	(1)未確認、範囲外の障害	(2)不正確な測定	(3)不適切な伝達、伝達の遅れ	(4)不適切なコントロールアルゴリズム	(5)不適切、欠けたコントロールアクション	(6)不適切な伝達、伝達の遅れ
超音波センサからEV3に測定結果が伝わらないため、傾かない UCA1			超音波センサからEV3への伝達が不適切			
EV3からモーターに命令が伝わらないため、傾かない UCA2				アルゴリズム	EV3からの不適切なコントロールアクション	
超音波センサからEV3に誤った測定結果を伝えたため、傾かない UCA3	外部の要因により想定外の測定結果が伝わる	超音波セ 不正確				
EV3からモーターに誤った命令を伝えたため、傾かない UCA4				アルゴリズム	EV3からの不適切なコントロールアクション	
超音波センサからEV3に測定結果が遅れて伝わるため、ゲートにぶつかる UCA5			超音波センサからEV3への伝達の遅れ			
EV3からモーターに命令が遅れて伝わるため、ゲートにぶつかる UCA6				プログラムのアルゴリズムが不適切	EV3からのコントロールアクションの遅れ	
EV3からモーターへのコントロールアクションが早すぎる停止により適切な角度まで傾かない UCA7				プログラムのアルゴリズムが不適切	EV3からの不適切なコントロールアクション	

外部の要因により想定外の測定結果が伝わる

シナリオと対策

UCA3:超音波センサからEV3に誤った測定結果を伝えたため、傾かない

シナリオ１
(1)外部の要因により想定外の測定結果が伝わる。

対策：ゴールを通過するまで超音波センサの測定結果を反映しない。

シナリオ２
(2) 超音波センサの故障などにより誤ったの測定結果が伝わる。

対策：想定外の値の測定結果が伝達された場合、距離を計測して傾くプログラムに切り替える。

シナリオと対策

① ルックアップゲートに近づき、超音波センサが一定の距離を検知しているが、プログラムのアルゴリズムが不正確なためモーターに命令が伝わらずH1が起こる。 ✔ テストOK！

② 飛行物体などにより想定外の測定結果が伝わる。 ✔ テストOK！

③ 超音波センサの故障などにより誤った測定結果が伝わる。 ✔ テストOK！

④ ルックアップゲートに近づき、超音波センサが一定の距離を検知しているがプログラムのアルゴリズムが不正確なためモーターに誤った命令がいきH1が起こる。 ✔ テストOK！

⑤ ルックアップゲートに近づき、超音波センサが一定の距離を検知しているが不適切なコントロールアルゴリズムによりH1が起こる。 ✔ テストOK！

⑥ ルックアップゲートに近づき、超音波センサが一定の距離を検知しているがEV3からモーターへの遅れたコントロールアクションによりH1が起こる。 ✔ テストOK！

⑦ 超音波センサが一定の距離を検知した後、不適切なコントロールアルゴリズムによりH1が起こる。 ✔ テストOK！

⑧ ゴールを通過したが、モーターからの測定結果が遅れて伝わりH2が起こる。 ✔ テストOK！

⑨ カラーセンサが検知しているが、プログラムのアルゴリズムが不正確なためモーターに命令が伝わらずH3が起こる。 ✔ テストOK！

⑩ 外乱光や、コースの状態などによりカラーセンサの測定結果が誤った結果となりH3が起こる。 ✔ 現地で調整！

⑪ カラーセンサが検知しているが、プログラムのアルゴリズムが不正確なためモーターに誤った命令が伝わりH3が起こる。 ✔ テストOK！

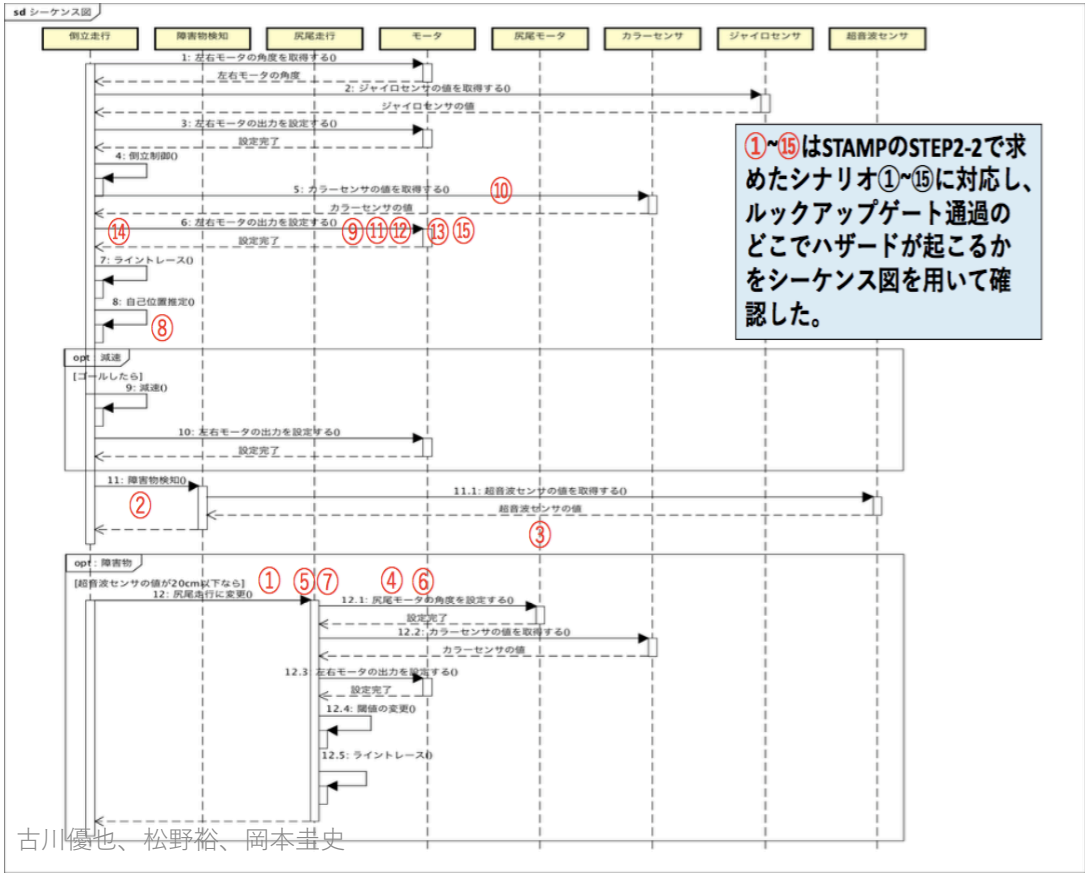
⑫ カラーセンサが検知しているが不適切なコントロールアルゴリズムによりH3が起こる。 ✔ テストOK！

⑬ カラーセンサが検知しているがEV3からモーターへの遅れたコントロールアクションによりH3が起こる。 ✔ テストOK！

⑭ カラーセンサが検知した後走行命令が出されるが、不適切なコントロールアルゴリズムによりH3が起こる。 ✔ テストOK！

⑮ カラーセンサが検知した後走行命令が出されるが、不適切なコントロールアルゴリズムによりH3が起こる。 ✔ テストOK！

ルックアップゲート通過時のシーケンス図



結果と原因

結果

・東京大会で予選敗退
　　本番では目標の完走を達成することができなかった

原因

・EV3のバックボタンが効かなくなった(ハードウェア故障)
　　ハードウェアは大丈夫と思い込み対策を怠った(予備の機体を買う)
・実際のコースで走行するテストが十分ではなかった
　　研究室内でのテストと実際の運用状況とは大きく異なることを認識して　　いなかった

STAMPで分析したチェック項目は有用であったが、思い込みなどで活かすことができなかった

疑問点

・コントロールストラクチャの粒度、大きさの決定

・ループしなくてよいのか？

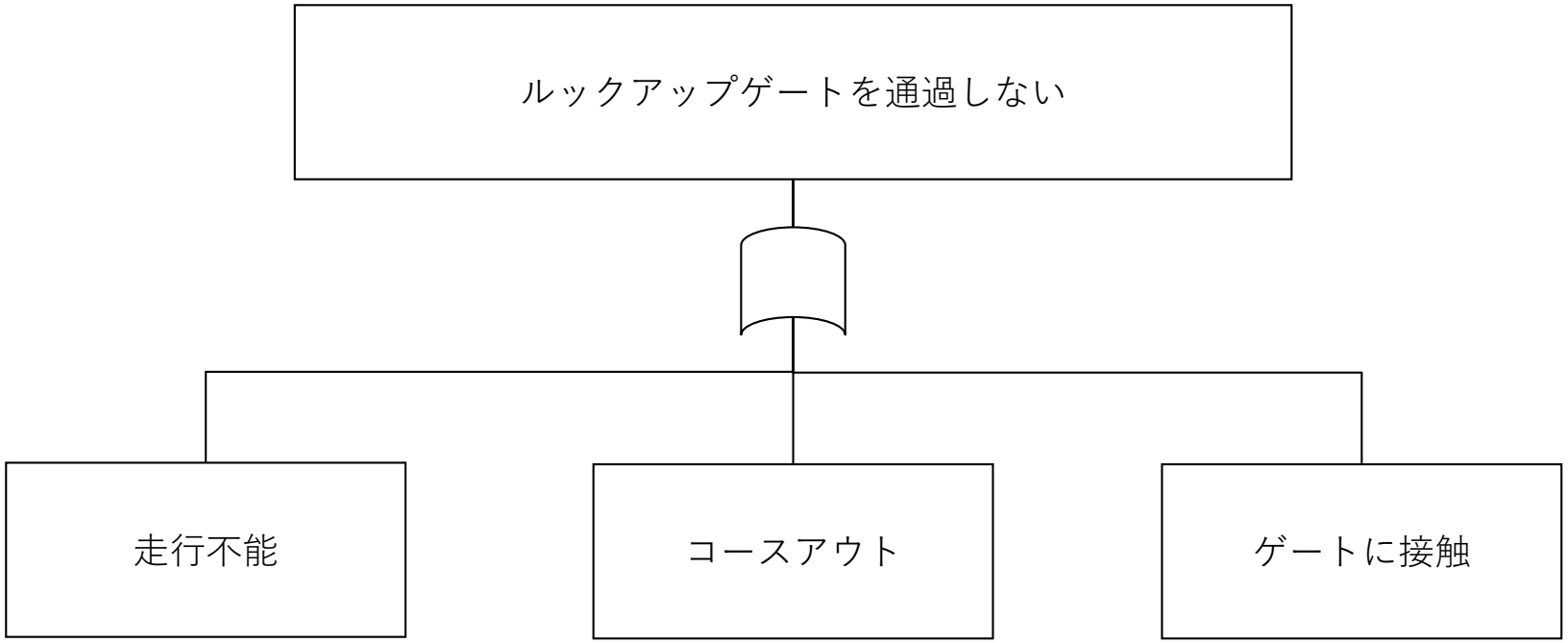
・同じガイドワードが一つのコントロールループで複数回出てきてもいいのか

・コントロールストラクチャとガイドワードを対応、ガイドワードの解釈

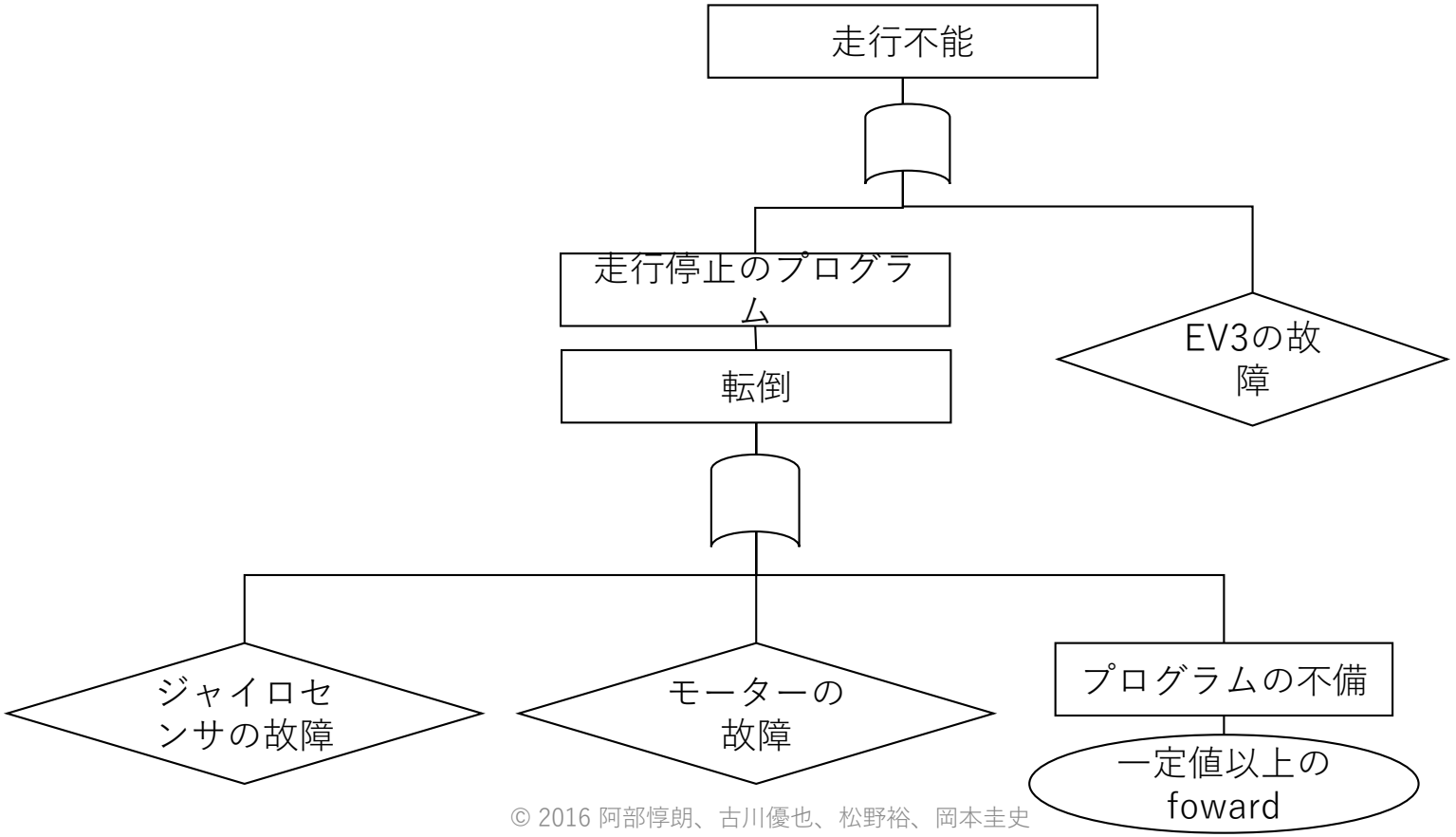
・UCA選択の基準
　　どれがUCAに至るか適切に選択できたと言えない

FTAとの比較

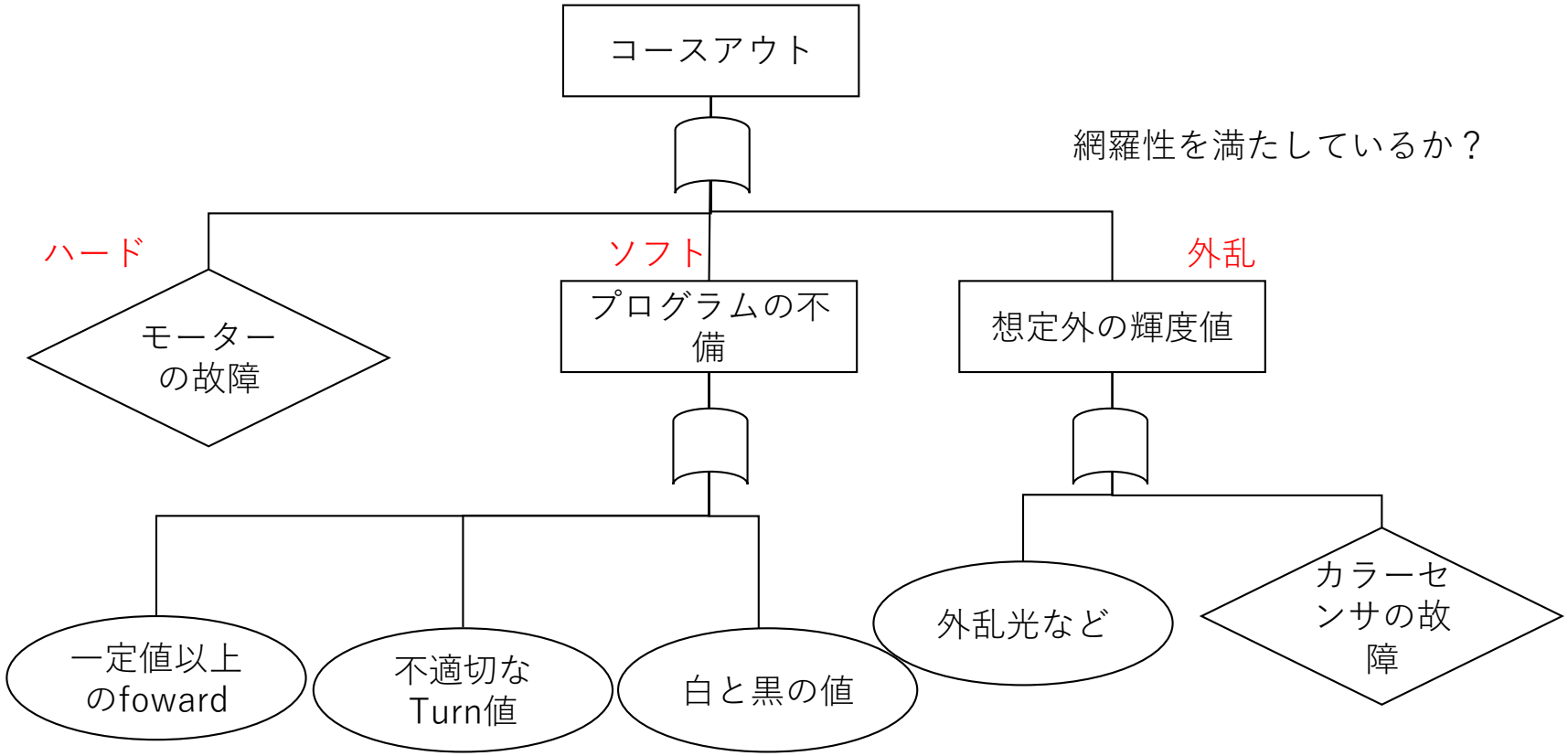
・頂上事象として「ルックアップゲートを通過しない」を定め、ツリー解析を行った。



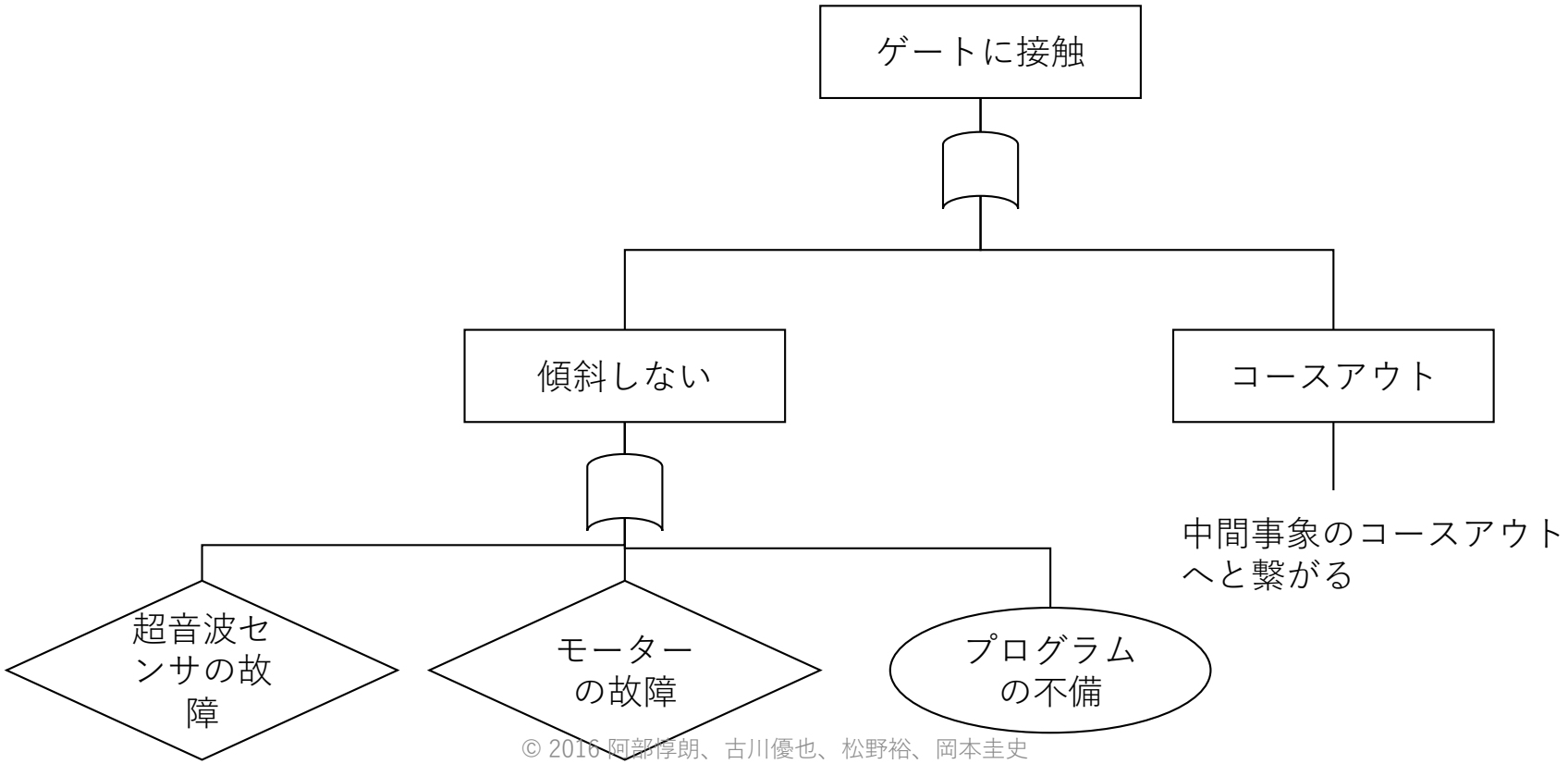
中間事象ごとの解析結果



中間事象ごとの解析結果



中間事象ごとの解析結果



分析結果の比較

	ハード	ソフト	他
FTA	・ジャイロセンサ ・カラーセンサ ・超音波センサ ・モーター ・EV3	・速度の設定 ・曲がる時の強さ ・輝度値の設定	・外乱光
STAMP	・ジャイロセンサ ・カラーセンサ ・超音波センサ ・モーター ・EV3 ・ケーブル	・プログラム全体 ・待機時間など	・外乱光

・ハードに関しては、STAMPにより繋がり（ケーブル）に着目できた
・ソフトに関しては、FTAでは関数やパラメーターレベルまで分析したが、STAMPでは「プログラム全体」レベルの分析になった

システム全体をSTAMPで分析し、細かい部分はFTAで分析

STAMPとFTAの比較

	モデル	着眼点	粒度	網羅(MECE)性
FTA	木構造（ツリー）	コンポーネント単体	細かい	確信が持てない場合がある
STAMP	コントロールストラクチャ（ネットワーク）	コンポーネントとコンポーネント間の流れ	大まか	コントロールストラクチャが描ければ、その範囲における網羅性は定義できる

試行をもとにしたSTAMP/STPAツールの設計

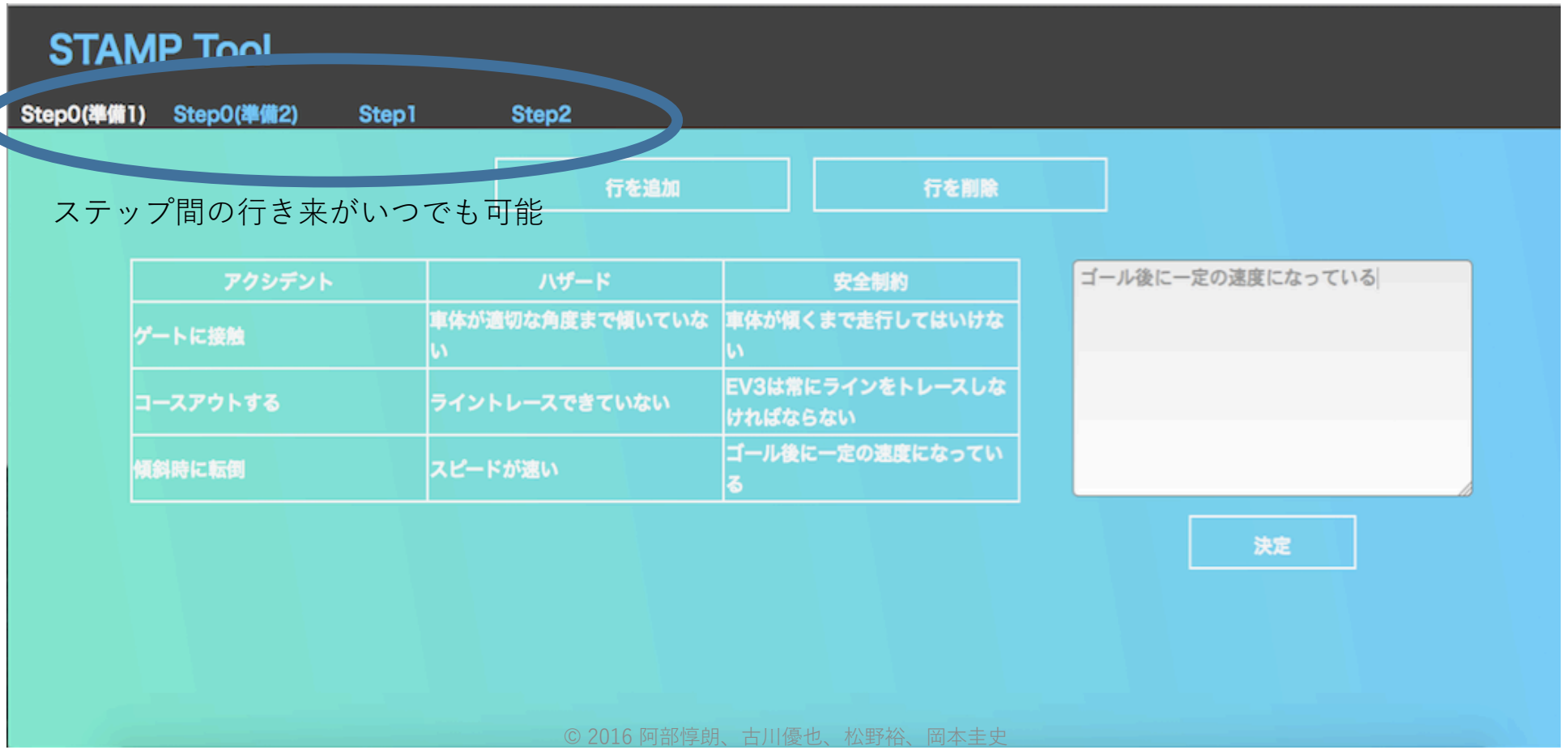
・STAMP/STPAは、Step（手順）がわかり易い

・Step を行き来して分析しなければならない、表が巨大になりがち

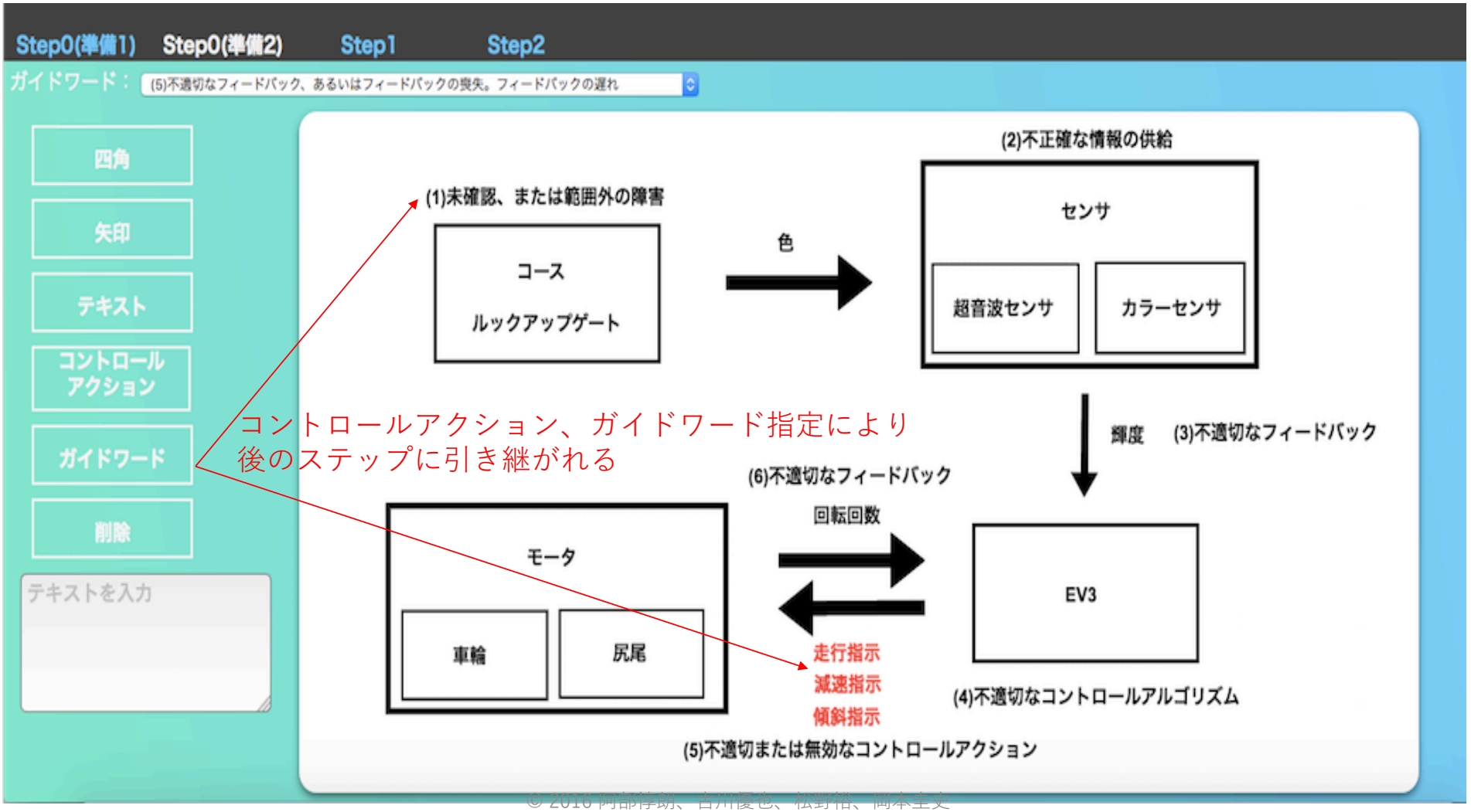
・既存ツールとしてXSTAMPPなどがあるが、eclipseのプラグインであるなど手軽に使えるものが少ない

わかりやすさを保ちつつ機能を絞り、stepの行き来が容易であり、前手順の引き継ぎができる、手軽に使えるwebベースツールを設計

STAMP/STPAツールのデモ



ステップ間の行き来がいつでも可能



STAMP Tool

Step0(準備1)　Step0(準備2)　Step1　Step2

コントロールアクション	与えられないとハザード	与えられるとハザード	早すぎ、遅すぎ、誤順序でハザード	早すぎる停止、長すぎる適用でハザード
走行指示	UCA1 超音波センサからEV3に測定結果が伝わらないため、傾かない	UCA3 超音波センサからEV3に誤った測定結果を伝えたため、傾かない	UCA5 超音波センサからEV3に測定結果が遅れて伝わるため、ゲートにぶつかる	UCA7 EV3からモータへのコントロールアクションが早すぎる停止により適切な角度まで傾かない
走行指示	UCA2 EV3からモータに命令が伝わらないため、傾かない	UCA4 EV3からモータに誤った命令が伝わるため、傾かない	UCA6 EV3からモータに命令が遅れて伝わるため、ゲートにぶつかる	EV3からモータへのコントロールアクションが早すぎる停止により適切な角度まで傾かない
減速指示	UCA8 モータからEV3に測定結果が伝わらないため、距離が測れず減速できない	UCA9 モータからEV3に誤った測定結果が伝わるため、任意の場所以外で減速する	UCA10 モータからEV3に遅れて測定結果が伝わるため、任意の場所以外で減速する	
傾斜指示	UCA11 カラーセンサからEV3に測定結果が伝わらないため、コースアウトする	UCA13 カラーセンサからEV3に誤った測定結果を伝えたため、コースアウトする	UCA15 カラーセンサからEV3に測定結果が遅れて伝わるため、コースアウトする	UCA17 走行命令が早すぎる停止により、コースアウトする
傾斜指示	UCA12 EV3からモータに命令が伝わらないため、コースアウトする	UCA14 EV3からモータに誤った命令を伝えたため、コースアウトする	UCA16 EV3からモータに命令が遅れて伝わるため、コースアウトする	UCA18 走行命令が長すぎる適用により、コースアウトする

STAMP Tool

Step0(準備1)　Step0(準備2)　Step1　Step2

	(10)未確認、または範囲外の障害	(2)不適切なコントロールアルゴリズム（作成時の欠陥、プロセスの変更、誤った修正や適用）	(6)不正確な情報の供給、または情報の欠如。測定の不正確性。フィードバックの遅れ	(5)不適切なフィードバック、あるいはフィードバックの喪失。フィードバックの遅れ	(5)不適切なフィードバック、あるいはフィードバックの喪失。フィードバックの遅れ	(8)不適切または無効なコントロールアクション、コントロールアクションの喪失
UCA1 超音波センサからEV3に測定結果が伝わらないため、傾かない				超音波センサからEV3への伝達が不適切		
UCA2 EV3からモータに命令が伝わらないため、傾かない		プログラムのアルゴリズムが不適切				EV3からの不適切なコントロールアクション
UCA3 超音波センサからEV3に誤った測定結果を伝えたため、傾かない	ルックアップゲートの状態により想定外の測定結果が伝わる		超音波センサの測定結果が不正確	超音波センサからEV3への伝達が不適切		
UCA4 EV3からモータに誤った命令が伝わるため、傾かない		プログラムのアルゴリズムが不適切				EV3からの不適切なコントロールアクション
UCA5 超音波センサからEV3に測定結果が遅れて伝わるため、ゲートにぶ				超音波センサからEV3への伝達の遅れ		

STAMP Tool

Step0(準備1)　Step0(準備2)　Step1　Step2

UCA1 超音波センサからEV3に測定結果が伝わらないため、傾かない

- シナリオ1-1 (5)不適切なフィードバック、あるいはフィードバックの喪失。フィードバックの遅れ
- シナリオ1-2 (5)不適切なフィードバック、あるいはフィードバックの喪失。フィードバックの遅れ

シナリオ1-2 (5)不適切なフィードバック、あるいはフィードバックの喪失。フィードバックの遅れ

シナリオ追加　対策　戻る

まとめ

・STAMP/STPAをETロボコンを例として試行
　　システムを大枠で捉え、リクス分析を行うことができた

・FTA分析との比較
　　コンポーネント間の繋がりに着目することができた
　　プログラムの詳細の分析はFTAの方が良い？

・Stepの行き来が容易で、前手順の引き継ぎができるツールを設計、ウエブベースで開発中