STAMP/STPA事例の振り返りと GSNを用いたSTPAプロセスの説明支援

（妥当性保証）

日本大学　　仙台高専

秋山 泰澄　　岡本 圭史
松野 裕

研究背景と目的

・昨年度のSTAMPワークショップなど、日本でもSTAMP/STPAに
注目が集まっている。しかしながら、まだ適用が初期段階にあり、
各企業も試行の段階にある

・昨年のSTAMPワークショップで発表された研究事例を参照し、
STAMP/STPAの手順を行う上で課題とされる点、及び工夫されている点を
抽出し、実際にSTAMP/STPAを実施する際に重要なポイントをまとめ、
GSN(Goal Structuring Notation)により表記。

・GSNとは、
アシュアランスケース（システム安全性の議論のモデル化、可視化）の
表記法の一種。

有効性の評価をするために既存の研究にGSNを適用。

もくじ

①STAMP/STPAの各ステップで課題とされる点、
　工夫されている点

②STAMP/STPAの各ステップの勘所をGSNで表記

③ ②で提案したGSN表記による勘所の
　研究事例への適用(Step0-1)

①STAMP/STPAの各ステップで課題とされる点、工夫されている点

Step0-1　アクシデント、ハザード、安全制約の識別

・対象システムに潜むアクシデント、ハザード、
　安全制約をどこまで網羅出来るか
　（アクシデントを一部のものに絞り込んでいる事例は別）

Step0-2　コントロールストラクチャの作成

・特定の複数のノード同士の関係性の明確さ

→これらのステップに入る前に、前提として対象システムの
　要求仕様書を用意している研究事例が存在した
　※昨年のSTAMPワークショップ一般講演の中で4件

Step1　　UCAの抽出

・コントロールストラクチャのノード数やCAの数が多いと、
このステップで各コントロールアクションの主体と被主体の
関係の把握が難しくなる　※CA：コントロールアクション

→UCAの表に記載された各CAにおいて主体と被主体の
関係を明確化させている事例があった
昨年のSTAMPワークショップ一般講演の中で3件

Step2　　HCFの特定

・ハザードシナリオの抽出（どれくらい抽出出来るか）

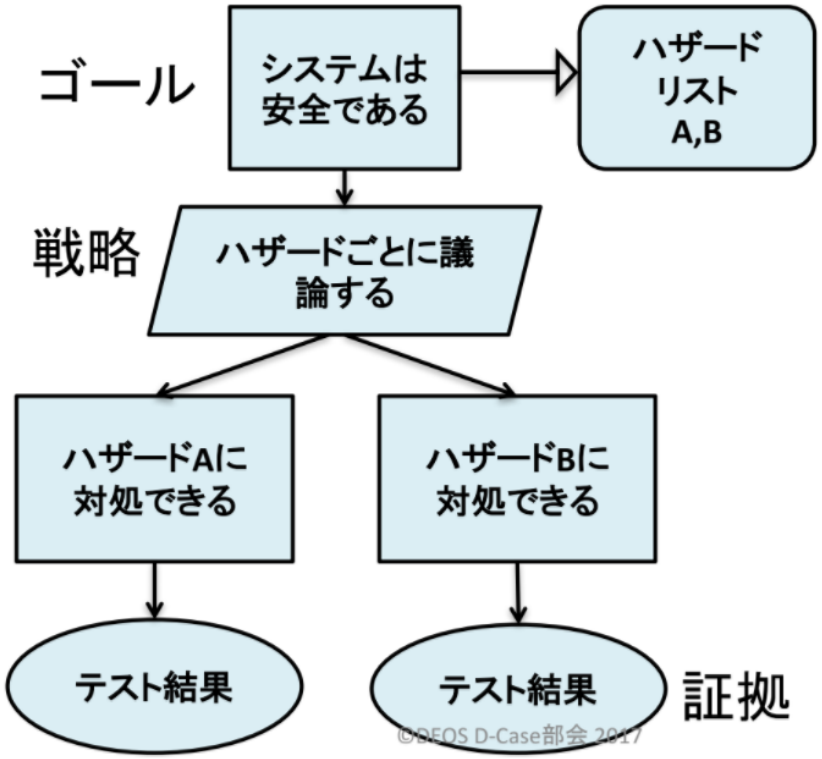
→参考になりうる事例は存在しなかった

②STAMP/STPAの各ステップの勘所をGSNで表記

・GSN（Goal Structuring Notation）とは

「議論」をモデル化、可視化したもので、実用的には
安全性の主張とそれを支持する議論構造を表すことを想定している。

GSNの簡単な例

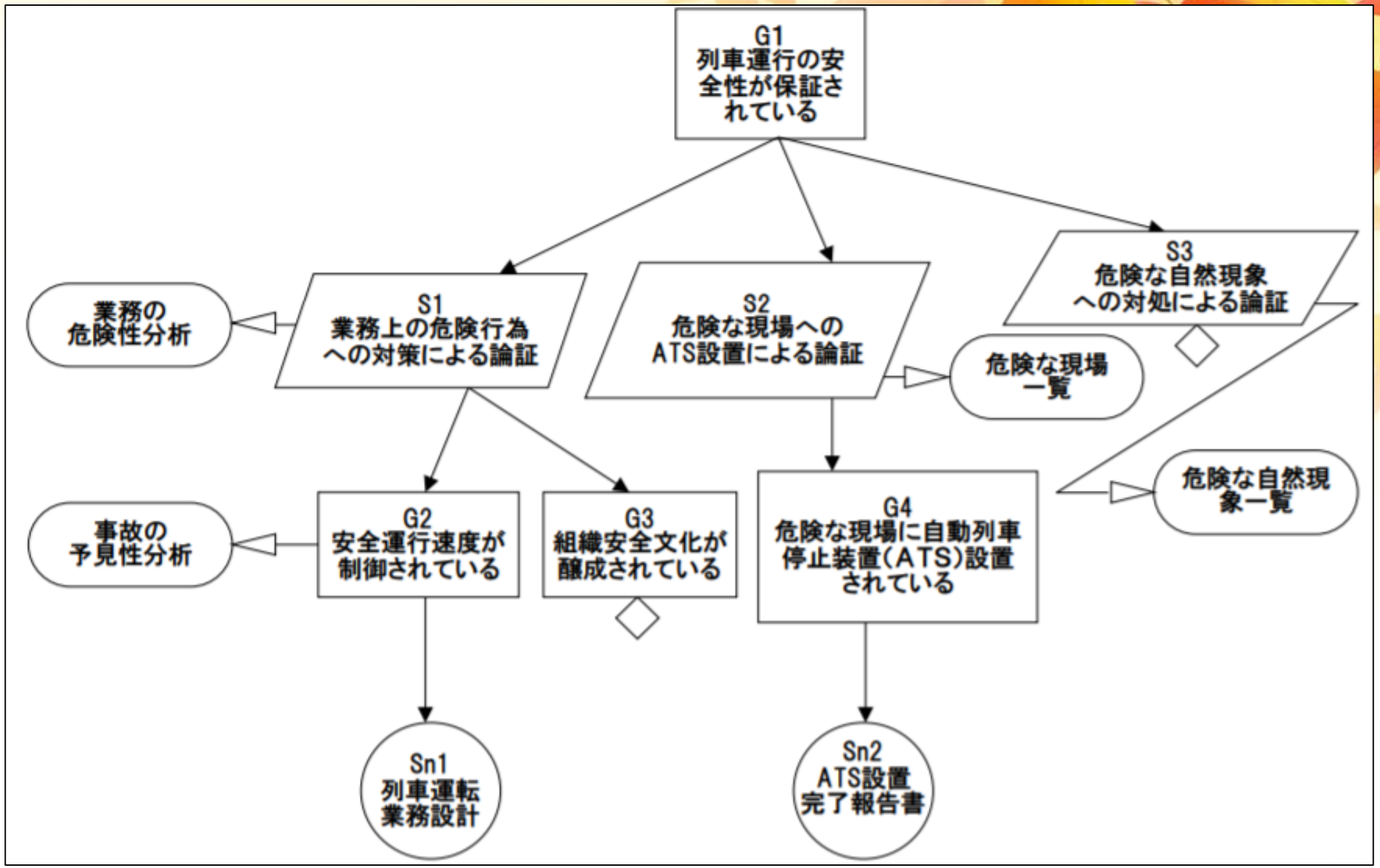


ステークホルダ：システム開発に関わる人々全員

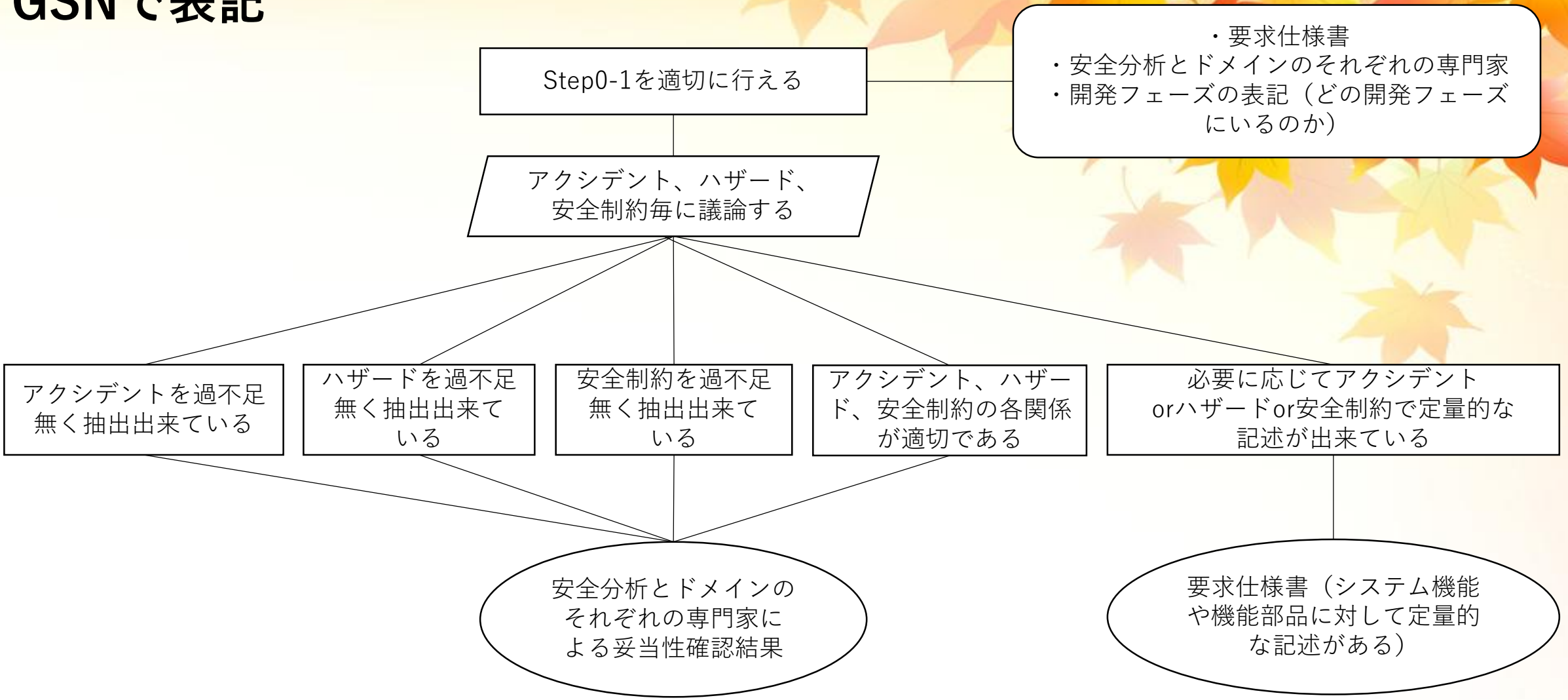
GSNで使用する基本的なノード

ノード	記号	説明
ゴール（Goal）	ゴール	ステークホルダ間で同意したいゴール
戦略（Strategy）	説明	上位のゴールの分解の仕方を説明
前提（Context）	前提	ステークホルダとの合意済みの主張や説明 ゴールや戦略が必要とな理由の情報
証拠（Evidence）	証拠	ゴールが達成できていることを示す証拠 証拠は明確に定義されたドキュメント
未達成（Undeveloped）		まだ具体化できていないゴールや説明であることを示す。（未定義要素）

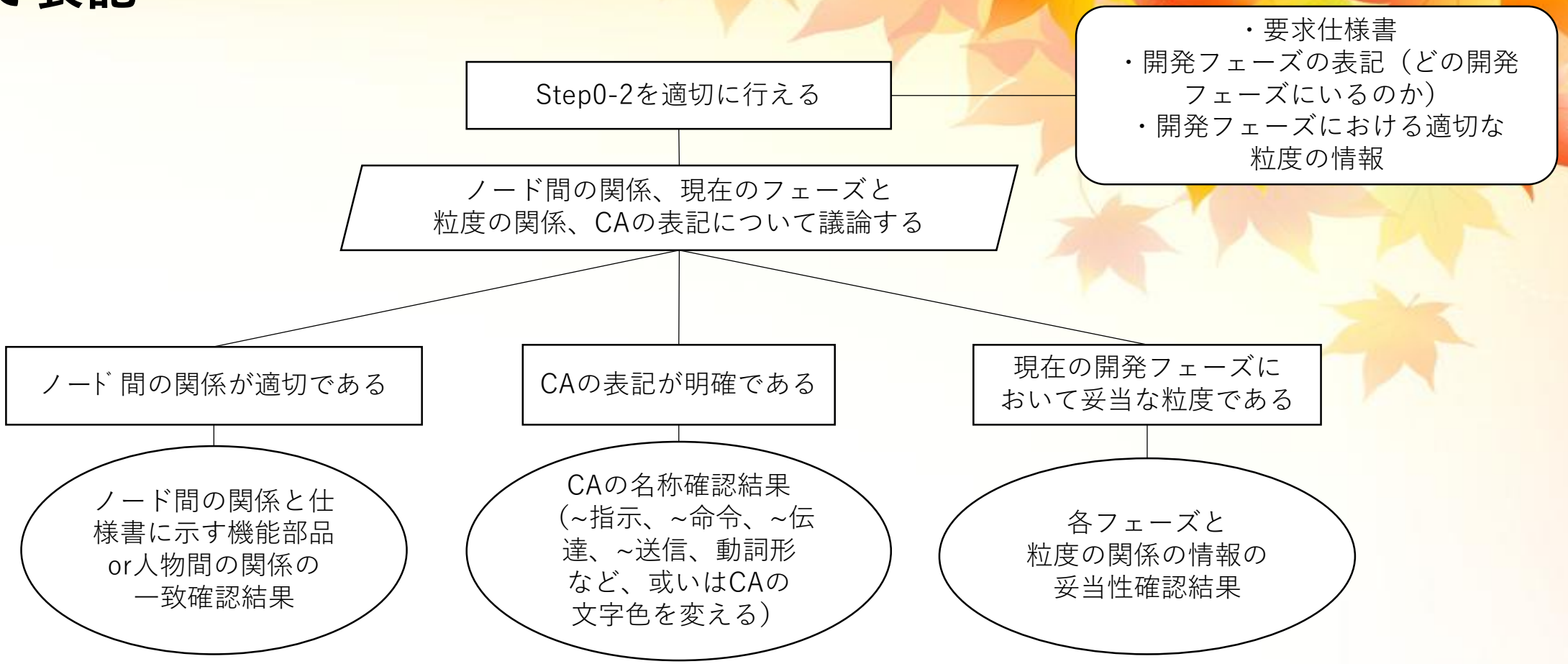
・GSNの適用例


G1
列車運行の安全性が保証されている
S1
業務上の危険行為への対策による論証
S2
危険な現場へのATS設置による論証
S3
危険な自然現象への対処による論証
業務の危険性分析
危険な現場一覧
危険な自然現象一覧
G2
安全運行速度が制御されている
G3
組織安全文化が醸成されている
G4
危険な現場に自動列車停止装置(ATS)設置されている
事故の予見性分析
Sn1
列車運転業務設計
Sn2
ATS設置完了報告書

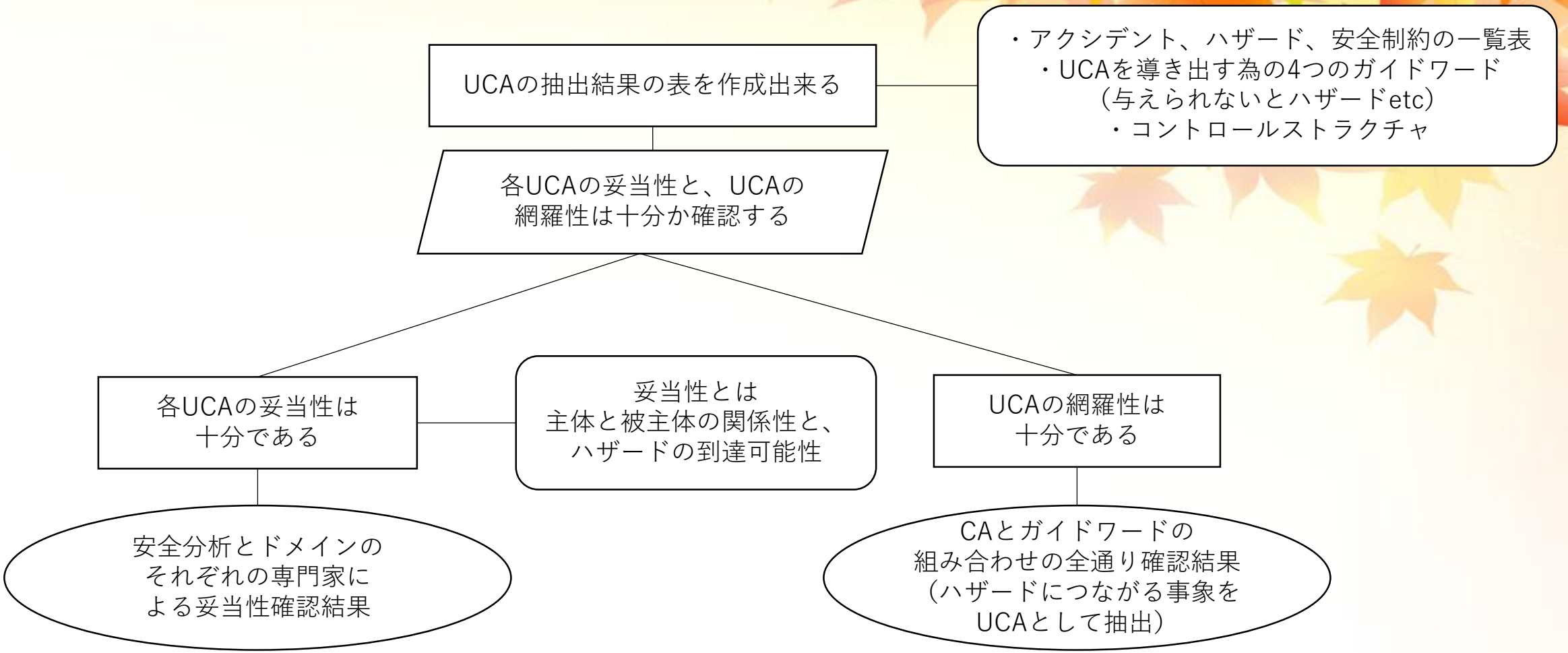
・Step0-1（アクシデント、ハザード、安全制約の識別）の勘所をGSNで表記



・Step0-2（コントロールストラクチャの作成）の勘所をGSNで表記



・Step1（UCAの抽出）の勘所をGSNで表記



・Step2（HCFの特定）の勘所をGSNで表記

※HCF特定の為のガイドワード
①コントロール入力や外部情報の誤りや喪失
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）
③不整合、不完全、または不正確なプロセスモデル、不適切な操作。
④コンポーネントの不具合、経年による劣化。
⑤不適切なフィードバック、或いはフィードバックの喪失、遅れ
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
⑦操作の遅れ
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。
⑨コントロールアクションの衝突。プロセス入力の喪失or誤り。
⑩未確認、または範囲外の障害、外乱。
⑪システムにハザードを引き起こすプロセス出力
⑫アクチュエータの動作が不十分
⑬センサーの動作が不十分

HCFの特定を適切に行えている

・HCF特定の為のガイドワード※
・UCA一覧表
・コントロールストラクチャ
・安全分析とドメインのそれぞれの専門家

ハザードシナリオの妥当性、網羅性、ハザード要因表の妥当性、要因表とシナリオの対応の妥当性の4つの観点からトップゴールを分解

ハザードシナリオの妥当性は十分である

安全分析とドメインのそれぞれの専門家の確認結果

各UCAのハザードシナリオを抽出できている（ハザードシナリオの網羅性は十分である）

ハザードシナリオ確認結果（各UCAにおいてガイドワードを1つずつ当てはめ、ハザードとなり得るならばハザードシナリオを作成し（1つのガイドワードに複数のハザードシナリオが在っても可）、尚且つ対策も記述）

ハザード要因表の妥当性は十分である

ハザード要因表の確認結果（直前に網羅したハザードシナリオを参照し、縦軸:UCA 、 横軸:ガイドワードとした、ハザード要因の一覧表を作成）

ハザード要因表とシナリオの対応は妥当である

ハザード要因とシナリオの対応の確認結果（個々のシナリオについて、それぞれ対応したガイドワードと表中に記載した同内容のシナリオに対応したガイドワードが一致）

③ ②で提案したGSN表記による勘所の研究事例への適用(Step0-1)

・Step0-1（アクシデント、ハザード、安全制約の識別）の勘所をGSNで表記（適用例）

※第一回STAMPワークショップの以下の研究事例を参照した

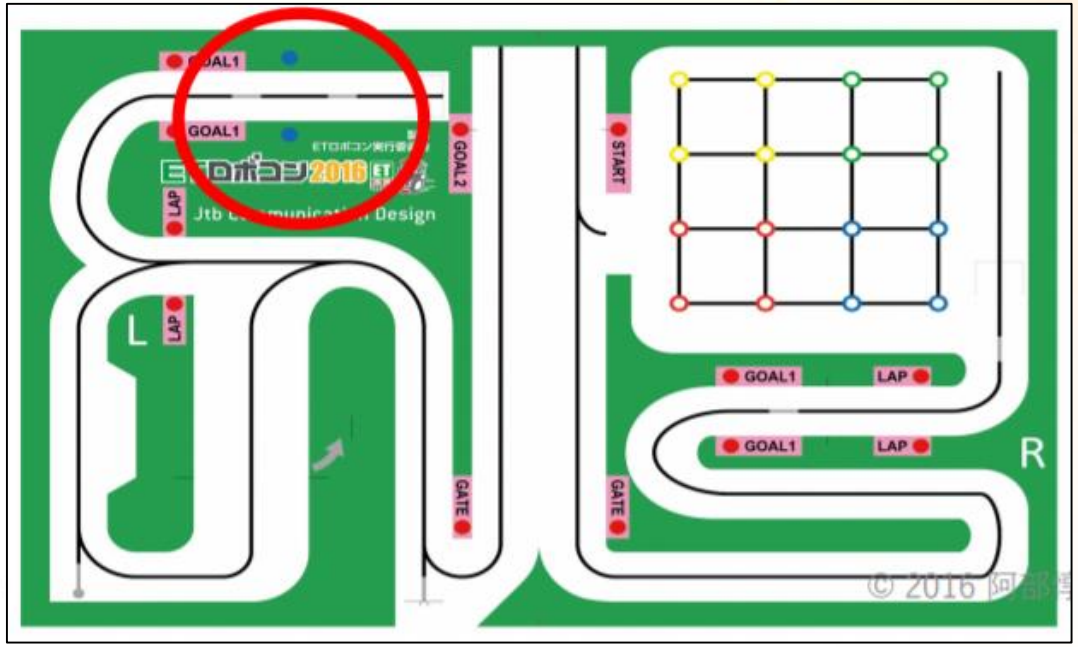
ETロボコン走行体システムへのSTAMP/STPA適用事例の紹介
（仙台高等専門学校　大友楓雅、菊池雄太郎、力武克彰、岡本圭史）

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

↓左側の黒いラインをトレースして走行



・Step0-1（アクシデント、ハザード、安全制約の識別）の勘所をGSNで表記（適用例）

本事例には、ETロボコンで用いる走行体の要求仕様書が無かった
その状態でのStep0-1の分析結果が右下の通りである

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

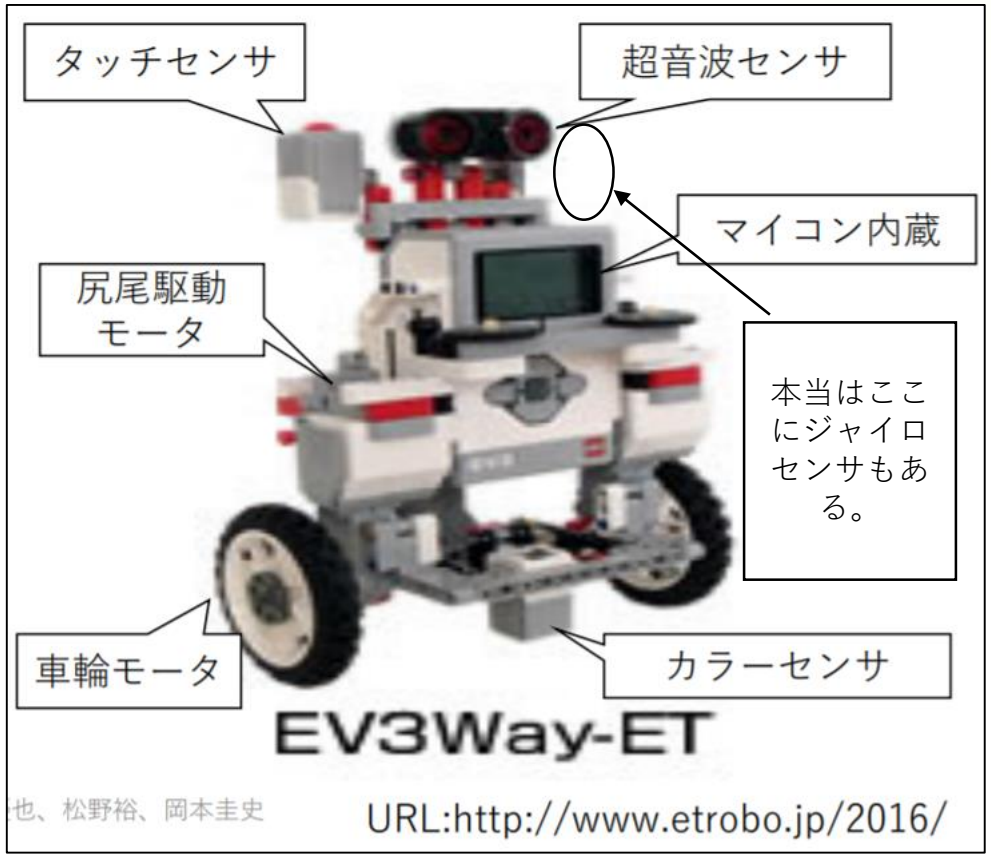
デベロッパー部門プライマリクラスとは
- ジャイロセンサを用いて傾き制御
- 輝度値センサを用いてライントレース
- ゴール後に難所に挑戦可能
  - ➢今回は競技開始からゴールまでを分析対象とした

要求仕様書が無く、安全制約に定量的な記述が出来ていない。

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

・Step0-1（アクシデント、ハザード、安全制約の識別）の勘所をGSNで表記（適用例）

こちらで要求仕様書を作成し、同様にStep0-1の分析を行う



ETロボコンで用いるEV3の機能

EV3走行体(幅170mm、高さ255mm、超音波センサ、カラーセンサ、ジャイロセンサ、車輪モータ、尻尾モータ搭載)

①超音波センサ
→コース上のルックアップゲートを検知し、尻尾を使って走行体を傾斜させる
ルックアップゲートの高さ235mmなので車体を傾斜させないとゲートに接触する

(計測可能距離：3~250cm)

(距離計測精度：+/- 1cm)

(障害物認識可能範囲(角度):約20度　(尚、センサ正面方向を角度の中心とする))

(センサ正面から10度ずれた場合の計測可能距離：約60cm)
(↑60cmまで離し、そこから物体を横に動かすときの
計測可能幅：センサ正面方向中心として左右約11cm)

②カラーセンサ
→コース上の黒いラインを検知し、車輪モータを用いて黒いライン上を走行させる

(カラーモード(黒、青、緑、黄色、赤、白、茶 及び無色を認識)における、
有効測定距離：約18mm
有効測定幅(距離18mmのとき)：約10mm)

(反射光の強さモード
(発光ランプから反射されるライトの強さを測定する。測定基準は0(非常に暗い)から100(非常に明るい)まで)における、
有効測定距離：約26mm
有効測定幅(距離26mmのとき)：約15mm)

③ジャイロセンサ
→センサを傾ける事により走行体の傾斜角を検知する

プログラム実行直後のセンサの位置を0度とし、時計回りに回転させると
EV3の画面に表示される傾斜角が増える。反時計回りに回転させると
傾斜角が減る。

④タッチセンサ
→前面の赤いボタン押されたか離された時に検出され、単一及び複数押下をカウントできる。ボタン可動域は約4mm

⑤車輪モータ
→車体を走行させる。減速や停止も可能　(最大速度：約44cm/s)

⑥尻尾モータ
→車体を傾斜させる

Afrel様のEV3技術情報のWebページを参考にしている。

・Step0-1（アクシデント、ハザード、安全制約の識別）の勘所をGSNで表記（適用例）

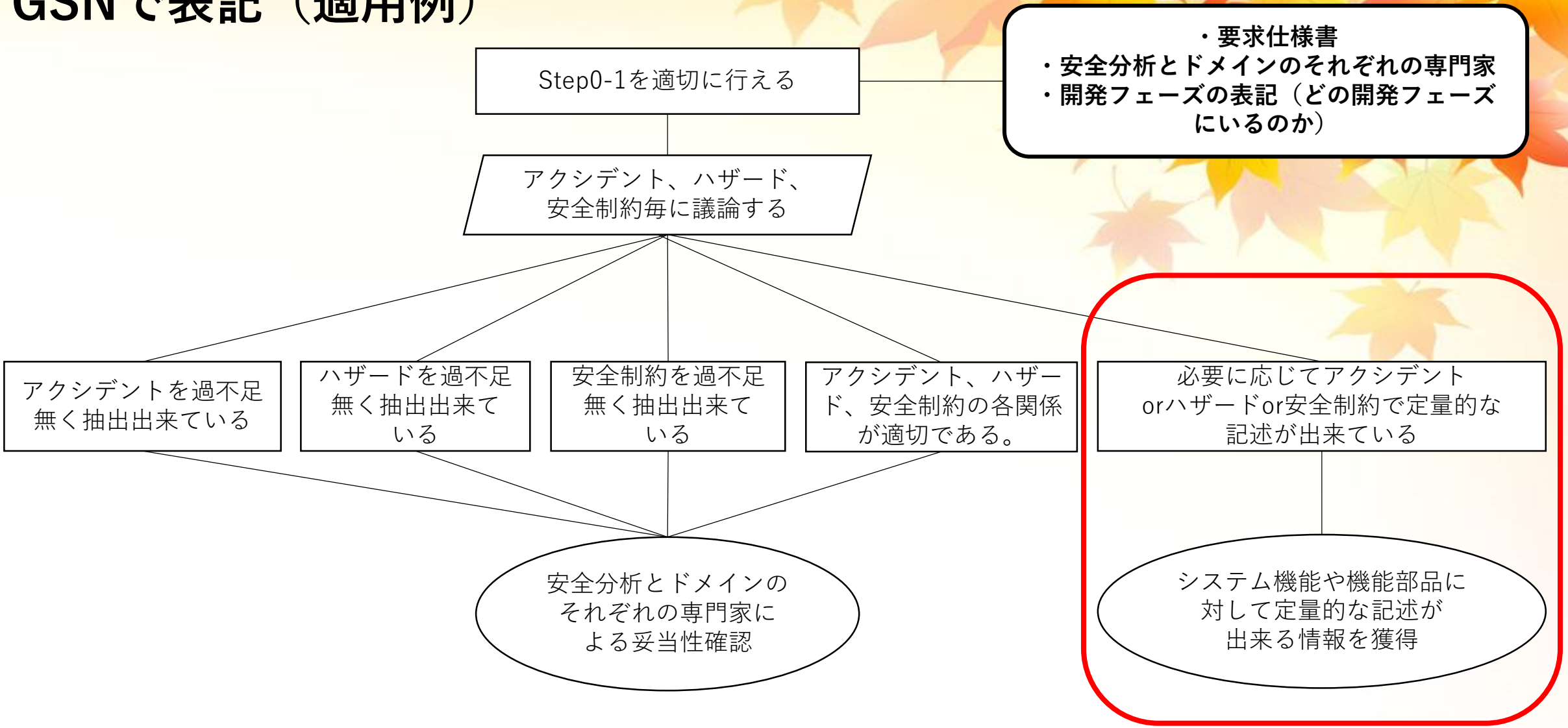
②カラーセンサ
→コース上の黒いラインを検知し、車輪モータを用いて黒いライン上を走行させる

(カラーモード(黒、青、緑、黄色、赤、白、茶 及び無色を認識)における、
有効測定距離：約18mm
有効測定幅(距離18mmのとき)：約10mm)

Afrel様のEV3技術情報の
Webページを参考にしている。

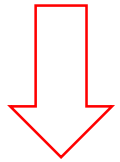
(反射光の強さモード
(発光ランプから反射されるライトの強さを測定する。測定基準は0(非常に暗い)から100(非常に明るい)まで)における、
有効測定距離：約26mm
有効測定幅(距離26mmのとき)：約15mm)

・Step0-1（アクシデント、ハザード、安全制約の識別）の勘所をGSNで表記（適用例）



・Step0-1（アクシデント、ハザード、安全制約の識別）の勘所をGSNで表記（適用例）

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



アクシデントorハザードor安全制約で定量的な記述が出来ている

システム機能や機能部品に対して定量的な記述が出来る情報を獲得

アクシデント	ハザード	安全制約
走行体が転倒	傾斜角が大きい(H1)	転倒しないための傾斜角を予め設定(SC1)
コースアウト	ライントレース出来ていない(H3)	カラーセンサは通常と傾斜時、床から18mmより離れていないこと(SC3)

※外乱光はここでは無いものとする。

まとめ

- STAMP/STPAの既存の研究事例を参照し、各ステップで課題とされる点、工夫されている点を抽出
- 各ステップの分析を行いやすくするために重要なポイントをGSNで表記
- 既存の研究事例に提案したGSNを適用し、分析結果の改訂を試行

今後の課題

- 今回作成したGSNのStep0-1~Step1の各サブゴールについて、何故そのサブゴールにしたかというストラテジーの確立
  ※Step2は「はじめてのSTAMP」を参考に作成
- Step0-2における、開発フェーズと粒度の関係の情報の確立
  （開発フェーズがこの段階なら粒度はこれ位が良い、といったもの）
- より手順化出来るガイドラインの作成

参考文献

- はじめての STAMP/STPA - IPA 独立行政法人 情報処理推進機構
  https://www.ipa.go.jp/files/000055009.pdf
- 名古屋大学 情報連携統括本部情報戦略室 JST, CREST 松野裕
  www.jst.go.jp/crest/crest-os/osddeos/event/201211/ET2012C804.pdf
- 第一回STAMPワークショップで発表された研究事例
  https://www.ipa.go.jp/sec/events/20161205.html