水上セグウェイみなものSTAMP/STPA分析／運用組織の視点からのハザード分析

Safety Analysis of Aquatic Segway, “MINAMO”, using STAMP/STPA

2016年12月6日

会津大学コンピュータ理工学部

清野正典,兼本茂

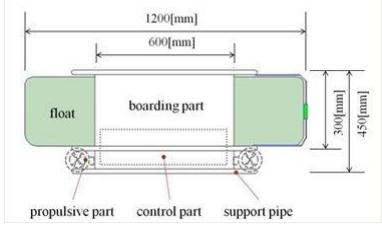
アジェンダ

1. 背景と目的
2. STAMP/STPAを用いた分析
   - 2.1 運用シナリオの想定
   - 2.2 制御構造図の作成
   - 2.3 UCAの抽出
   - 2.4 ハザードシナリオの記述
   - 2.5 コンポーネント安全制約の明示
3. FTAとの比較
4. ワークフロー変更後との安全制約の比較
5. まとめ

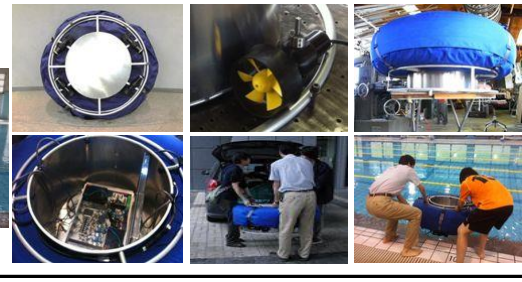
1. 背景と目的

- 人間・機械協調制御をする製品（介護ロボット、自動運転車など）の普及により、設計時のハザード分析やモデルベース設計による十分な安全性の検討が求められてきている。人工知能などのソフトウェアの複雑化が進んでおり、それに対応できる安全評価が必要になる。
- 従来のハザード分析手法（FTA、FMEAなど）はハードウェアのコンポーネント故障や単純なヒューマンエラーを想定した分析手法
  - 人と機械が協調して動作するシステムや、人の管理体制による組織的なシステムの不具合の分析には適していない
- 人と機械が協調して動作するシステムの分析に適しているといわれるSTAMP/STPAを用いて、水上セグウェイ「みなも」を分析対象に複雑システムの安全分析を試み、STAMP/STPAの有効性を検証する

STAMPに基づくみなも（全方位推進型水上移動機）の安全分析

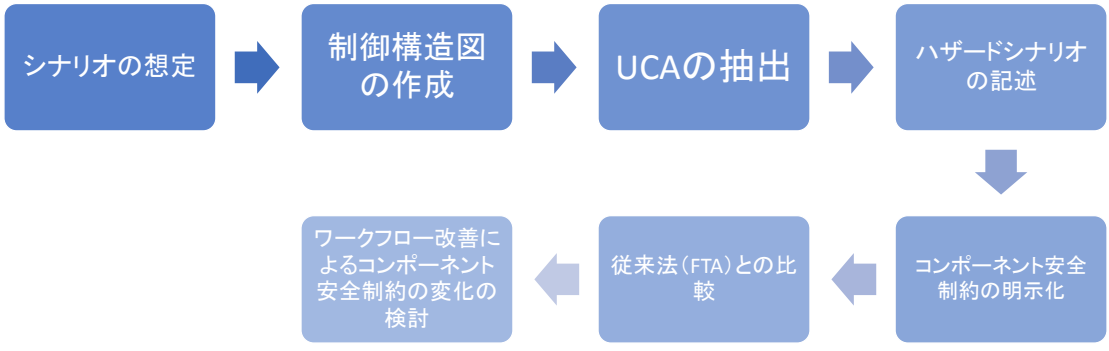


ロボットタイプ：水上活動向け搭乗型ロボット	
外寸：	フロート外径1200mm
	フロート内径（搭乗部）600mm
	高さ450mm（フロート部高さ300mm）
重量：	約45kg
バッテリー：	鉛蓄電池24V×2
推進動力：	コアレスDCモータ150W×4
推進方向：	並進（前後，左右，斜め），旋回
推進速度：	最大60cm/s
センサ：	加速度センサ，ジャイロセンサ，地磁気センサ，GPS，ロードセル
充電稼働時間：	約1時間



本発表での説明の流れ

STAMP/STPAによる分析→従来法との比較→ワークフロー改善



1.1 抽象化した想定シナリオ

（ハード仕様に依存した細かい設計シナリオはこの段階では考えない）

- 海、湖沼など自然環境での運行を想定し、調査計画・出航・帰還を指示する管理者（必ずしも現場駐在はしない）、みなもの点検・保守・出航時の補助、現場での出航の最終判断までを担当する現場責任者、運転者をステークホルダーとする。
- 運行では、出発地から見えない場所まで離れたり、漂流した場合に自力で帰れない場所までの移動を想定する。（ただし、櫂で漕ぐことで自力帰還はできると仮定）
- みなもは、非常に大きな波、高速の船による衝突のような外乱以外では、転覆しにくい構造と仮定。モータパワーも、転覆したり、運転者が落船するほどのスピードは出せないと仮定
- （4つのモータの一部が故障した場合の方向制御機能は今後検討要）

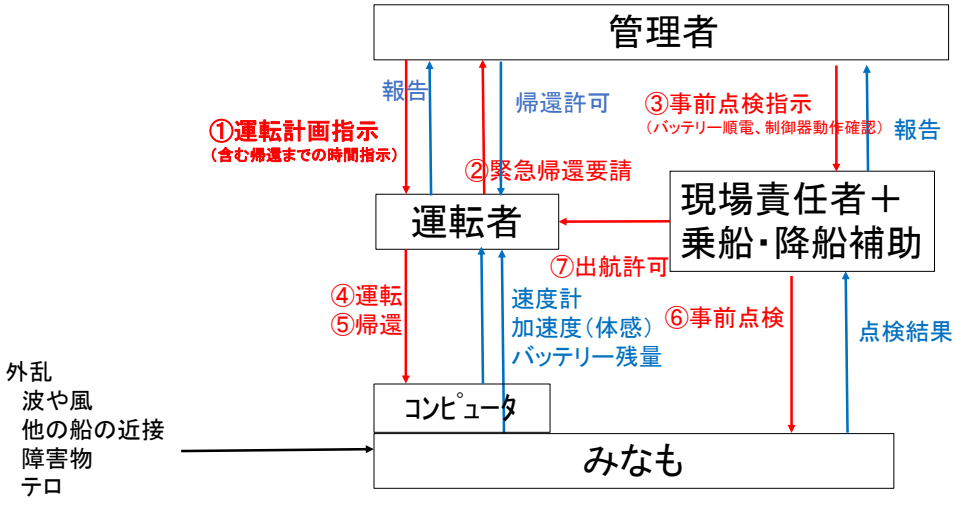
アクシデントとハザードの定義ならびに組織の安全管理責任（Safety related responsibility）

アクシデント：漂流
ハザード：漂流を起こすバッテリー不足や暴走
安全制約：漂流を起こさないこと（バッテリー切れ、暴走など）

Actor	Safety related responsibility
管理者	運転計画・帰還時間の指示 天候条件による帰還判断 補助員への事前点検の指示
補助員（現場責任者）	事前点検（バッテリー充電、コントローラ作動、スクリュー作動、本体欠陥） 現場での出航判断
運転者	運転計画に沿った帰還 緊急時の自己判断による帰還

2016.3.10　兼本@会津大学

1.2 水上セグウェイみなもの安全分析（制御構造図（1））



1.3 制御構造図(1)に基づくUCAの分析

コントロールアクション	主体	被主体	コントロールアクションの前提条件	与えられないとハザード(NotProviding)	与えられるとハザード(IncorrectlyProviding)	早すぎ、遅すぎ、誤順序でハザード(IncorrectTiming)	早すぎる停止、長すぎる適用でハザード(IncorrectlyStop)
①運転計画指示	管理者	運転者	期間までの時間指示も含む	出航しないので安全側	不適切な環境条件での出航指示による遭難(UCA1-P)	事前点検指示前に、運転計画を指示して、点検なしの出航(UCA1-T)	一旦出した運転計画をキャンセルして混乱(UCA1-D)
②緊急帰還要請	運転者	管理者	運転者と管理者のどちらを主体と考えるべきか？ここでは現場優先で考える。 ただし、天気予報情報などで緊急帰還指示をするのや管理者	緊急帰還要請が伝わらずに漂流 または管理者の判断ミスと現場の判断ミスが重なって漂流(UCA2-N)	不必要な帰還要請は安全側	帰還判断が遅れてハザード(UCA2-T)	一旦出した緊急帰還要請をキャンセルして混乱(UCA2-D)
③事前点検指示	管理者	補助員	バッテリー確認、コントローラ動作確認、スクリュー動作確認、本体確認など	事前点検なしで出航させ、ハザード(UCA3-N)	不必要なタイミングでの事前点検は安全側	事前点検が遅れて、点検なしで出航(UCA3-T)	事前点検を途中で中断し、不十分な点検で出航(UCA3-D)
④運転	運転員	みなも	計画に沿って一定時間運行し調査活動を行う	制御指示どおりに動かなくて漂流、ハード故障と強風などの影響がある。バッテリー切れもある(UCA4-N)	指示なしで動いて漂流(UCA4-P)	制御指示より遅れて動いて衝突(これは今回は対象外)	一旦出した制御指示を止めて衝突(対象外)
⑤帰還	運転員	みなも	計画時間内に帰還する	帰還制限時間を忘れてバッテリー切れで帰還できない(UCA5-N)	帰還するだけなので安全側	帰還操作が遅れて、バッテリー切れで帰還できない(UCA5-T)	帰還途中で、再度、沖に出て帰還できなくなる(UCA5-D)
⑥事前点検	補助員	みなも	バッテリー充電、コントローラ点検、スクリュー点検、本体点検	事前点検なしで出航しトラブルで漂流(UCA6-N)	間違った事前点検でトラブル・漂流(UCA6-P)	事前点検が遅れて、点検なしで出航(UCA6-T)	事前点検を途中で中断し、不十分な点検で出航(UCA6-D)
⑦出航許可	補助員	運転員	点検完了を知らせ運行開始を指示	運転開始をしないので安全側	事前点検が終了してないのに運転許可をだし、運転開始でハザード(UCA7-P)	事前点検前の早すぎる許可で運転を開始しハザード(UCA7-T)	該当無し

1.3 制御構造図(1)に基づくUCAの分析

コントロールアクション	主体	被主体	与えられないとハザード(NotProviding)	与えられるとハザード(IncorrectlyProviding)	早すぎ、遅すぎ、誤順序でハザード(IncorrectTiming)	早すぎる停止、長すぎる適用でハザード(IncorrectlyStop)
③事前点検指示	管理者	補助員	事前点検なしで出航させ、ハザード(UCA3-N)	不必要なタイミングでの事前点検は安全側	事前点検が遅れて、点検なしで出航(UCA3-T)	事前点検を途中で中断し、不十分な点検で出航(UCA3-D)
⑦出航許可	補助員	運転員	運転開始をしないので安全側	事前点検が終了してないのに運転許可をだし、運転開始でハザード(UCA7-P)	事前点検前の早すぎる許可で運転を開始しハザード(UCA7-T)	該当無し

③事前点検指示（運転管理者→現場責任者）

- 事前点検なしで出航させ、ハザード（UCA3-N）
  - UCA3-N-HS1:事前点検指示を忘れる、または、指示したものの補助員が聞き間違え事前点検をしないで出航→チェックシートを管理者が確認し最終判断するようなワークフローとする。または、ワークフローを変えて、出航指示は補助員（現場責任者）のみから出す。
- 事前点検が遅れて、点検なしで出航（UCA3-T）
  - UCA3-T-HS1:事前点検の指示は受けたが、日時を間違え、事前点検なしで出航→チェックシートを管理者が確認し最終判断するようなワークフローとする、または、ワークフローを変えて、出航指示は補助員（現場責任者）のみから出す。
- 事前点検を途中で中断し、不十分な点検で出航（UCA3-D）
  - UCA3-D-HS1:事前点検を指示に従った方法で行わない、補助員の判断で省略などで、不十分な事前点検で出航→運転者自身による点検の最終確認を行う
  - UCA3-D-HS2:事前点検を早く終わるよう管理者からの指示があり、補助員が不十分な点検で終了して出航→点検結果の記録をチェックシートで残して運転管理者に報告するなどのワークフローの改善

③事前点検指示（運転管理者→現場責任者）

- 事前点検なしで出航させ、ハザード（UCA3-N）
  - UCA3-N-HS1:事前点検指示を忘れる、または、指示したものの補助員が聞き間違え事前点検をしないで出航→チェックシートを管理者が確認し最終判断するようなワークフローとする。または、ワークフローを変えて、出航指示は補助員（現場責任者）のみから出す。
- 事前点検が遅れて、点検なしで出航（UCA3-T）
  - UCA3-T-HS1:事前点検の指示は受けたが、日時を間違え、事前点検なしで出航→チェックシートを管理者が確認し最終判断するようなワークフローとする、または、ワークフローを変えて、出航指示は補助員（現場責任者）のみから出す。
- 事前点検を途中で中断し、不十分な点検で出航（UCA3-D）
  - UCA3-D-HS1:事前点検を指示に従った方法で行わない、補助員の判断で省略などで、不十分な事前点検で出航→運転者自身による点検の最終確認を行う
  - UCA3-D-HS2:事前点検を早く終わるよう管理者からの指示があり、補助員が不十分な点検で終了して出航→点検結果の記録をチェックシートで残して運転管理者に報告するなどのワークフローの改善

③事前点検指示（運転管理者→現場責任者）

- 事前点検なしで出航させ、ハザード（UCA3-N）
  - UCA3-N-HS1:事前点検指示を忘れる、または、指示したものの補助員が聞き間違え事前点検をしないで出航→チェックシートを管理者が確認し最終判断するようなワークフローとする。または、ワークフローを変えて、出航指示は補助員（現場責任者）のみから出す。
- 事前点検が遅れて、点検なしで出航（UCA3-T）
  - UCA3-T-HS1:事前点検の指示は受けたが、日時を間違え、事前点検なしで出航→チェックシートを管理者が確認し最終判断するようなワークフローとする、または、ワークフローを変えて、出航指示は補助員（現場責任者）のみから出す。
- 事前点検を途中で中断し、不十分な点検で出航（UCA3-D）
  - UCA3-D-HS1:事前点検を指示に従った方法で行わない、補助員の判断で省略などで、不十分な事前点検で出航→運転者自身による点検の最終確認を行う
  - UCA3-D-HS2:事前点検を早く終わるよう管理者からの指示があり、補助員が不十分な点検で終了して出航→点検結果の記録をチェックシートで残して運転管理者に報告するなどのワークフローの改善

⑦出航許可（現場責任者→運転員）

- 事前点検が終了してないのに運転許可をだし、運転開始でハザード（UCA7-P）
  - UCA7-P-HS1:機体に不備があるまま運転許可を出し、トラブルで漂流→管理者を通し最終チェックをした後、管理者から運転開始許可を出す。運転者自身による最終点検。
- 事前点検前の早すぎる許可で運転を開始しハザード（UCA7-T）
  - UCA7-T-HS1:点検結果を受け取る前に間違って運転開始許可を出してしまい、そのまま出航して漂流→管理者を通し最終チェックをした後、管理者から運転開始許可を出す
- 不十分な状態で出航許可を出してハザード(UCA7-P)
  - UCA7-P-HS1:不十分な点検のまま出航許可を出し漂流→点検基準の明確化
  - UCA7-P-HS2:運転者の体調を考慮せずに出航許可を出し漂流→運転者の体調を最重要視する安全文化
  - UCA7-P-HS3:天気予報を見間違えて出航許可を出し漂流→出航ルールの明確化（予報確認、点検基準、運転者の体調など）

⑦出航許可（現場責任者→運転員）

- 事前点検が終了してないのに運転許可をだし、運転開始でハザード（UCA7-P）
  - UCA7-P-HS1:機体に不備があるまま運転許可を出し、トラブルで漂流→管理者を通し最終チェックをした後、管理者から運転開始許可を出す。運転者自身による最終点検。
- 事前点検前の早すぎる許可で運転を開始しハザード（UCA7-T）
  - UCA7-T-HS1:点検結果を受け取る前に間違って運転開始許可を出してしまい、そのまま出航して漂流→管理者を通し最終チェックをした後、管理者から運転開始許可を出す
- 不十分な状態で出航許可を出してハザード(UCA7-P)
  - UCA7-P-HS1:不十分な点検のまま出航許可を出し漂流→点検基準の明確化
  - UCA7-P-HS2:運転者の体調を考慮せずに出航許可を出し漂流→運転者の体調を最重要視する安全文化
  - UCA7-P-HS3:天気予報を見間違えて出航許可を出し漂流→出航ルールの明確化（予報確認、点検基準、運転者の体調など）

⑦出航許可（現場責任者→運転員）

- 事前点検が終了してないのに運転許可をだし、運転開始でハザード（UCA7-P）
  - UCA7-P-HS1:機体に不備があるまま運転許可を出し、トラブルで漂流→管理者を通し最終チェックをした後、管理者から運転開始許可を出す。運転者自身による最終点検。
- 事前点検前の早すぎる許可で運転を開始しハザード（UCA7-T）
  - UCA7-T-HS1:点検結果を受け取る前に間違って運転開始許可を出してしまい、そのまま出航して漂流→管理者を通し最終チェックをした後、管理者から運転開始許可を出す
- 不十分な状態で出航許可を出してハザード(UCA7-P)
  - UCA7-P-HS1:不十分な点検のまま出航許可を出し漂流→点検基準の明確化
  - UCA7-P-HS2:運転者の体調を考慮せずに出航許可を出し漂流→運転者の体調を最重要視する安全文化
  - UCA7-P-HS3:天気予報を見間違えて出航許可を出し漂流→出航ルールの明確化（予報確認、点検基準、運転者の体調など）

対策のまとめ1（コンポーネント安全制約）

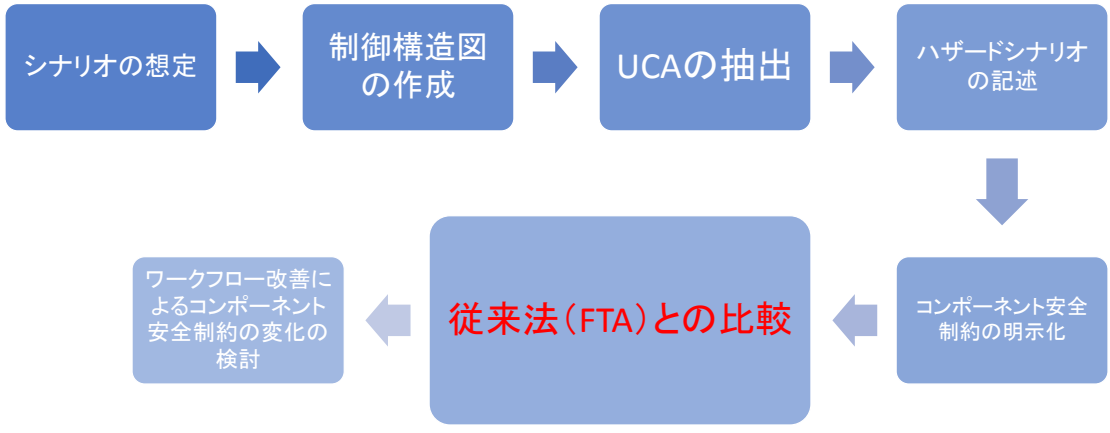
- コントローラー
  - 代替コントローラへの切り替え
  - 電源遮断後の手動による運転
  - コントローラーを介さずにモーターを制御できる機能の追加
- 運転操作・インターロック関連
  - 手動による運転の対応
  - バッテリー残量のアラート機能の追加。補助バッテリーの設置
  - ハッカーによる乗っ取りを検出する監視機能の追加
- 通信
  - GPS機能による位置情報の確認、管理者または補助員からの進行方向の指示
- 点検
  - モータ・スクリューの定期点検。起動前のモータ・スクリューの検査
  - カセンサーの定期点検。起動前のカセンサーの検査
  - 無線機器の事前の動作確認
  - 運転者自身による最終点検。管理者への事前点検結果の報告・確認要求

対策のまとめ2（コンポーネント安全制約）

- ワークフロー改善（1）
  - 事前点検、運転計画、出航指示のワークフローと、チェックシートによる確認ルールの明確化、指示ルート（ワークフロー）の変更も含む
  - チェックシートを管理者が確認し最終判断するようなワークフロー、または、出航指示は現場責任者のみとするワークフローへの変更
  - 点検結果の記録をチェックシートで残し、運転管理者に報告するなどのワークフローの改善
  - キャンセルを含む指示に対する報告の義務付け、ワークフローの改善
  - 点検結果を管理者にフィードバックし、管理者による最終確認を行ったのち管理者からの運転開始許可（現場での勝手な判断を禁止するルール
  - 帰還予定時刻の際の管理者または補助員から帰還命令
  - 天候の正確な事前予測
- ワークフロー改善（2)
  - 出航ルールの明確化（予報確認、現場の判断優先、体調確認など）
  - 精度の良い天気情報の利用
  - 管理者としての判断ルールの明確化
  - 運転者から出した緊急帰還要請のキャンセルルールの明確化と、管理者側からの緊急帰還指示ルールの作成
  - 間違いにくいような手順書の作成（順番にチェックしながら点検を進めるなど）。管理者による再確認
  - 帰還開始前の任務の遂行状況のチェック。管理者へ任務の報告・確認要求
- 訓練、規律・統制
  - 運転者による運転操作の事前訓練（モーターが一部しか動かない場合の操作訓練を含む）
  - 点検作業の十分な訓練。管理者による再確認
  - 遠くの目印を目標にして現在位置を把握する訓練
  - 運転者の安全を最重要視する安全文化

本発表での説明の流れ

STAMP/STPAによる分析→従来法との比較→ワークフロー改善



漂流のFTA

- バッテリー切れ
  - ー充電忘れ
  - ー帰還時間忘れ
  - ーバッテリー故障
- 暴走ーコントローラ故障
  - ーセンサ故障
  - ーモータ故障
  - ー運転ミス
- 天候悪化
  - ー管理（予測）ミス
  - ー現場の判断ミス
- 想定外の外乱
  - ー大型船との衝突など

FTAとの比較（オレンジ：STAMPのみ、赤：FTAのみ、ただしSTAMPにも暗黙で含まれる）

- バッテリー切れ
  - バッテリー切れでモータが動かず、帰還できずにそのまま漂流(UCA4-N-HS1)
  - 立ち往生
    - 帰還するための進行方向がわからずに立ち往生でバッテリー切れ(UCA5-T-HS4)
  - 充電忘れ
    - 点検手順書の中に暗黙で含まれる
  - 帰還時間忘れ
    - 帰還制限時間を間違って把握していて、制限時間を超えても任務を行うことでバッテリーが切れそのまま漂流(UCA5-T-HS3)
  - バッテリー故障
    - バッテリー切れに含まれる
  - 任務やり残し
    - 帰還途中で任務のやり残しに気づき再度沖に出てしまいバッテリー切れで帰還できなくなる(UCA5-D-HS2)
  - 進行方向間違い
    - 帰還途中で進行方向を間違えて進み、再度沖に出てしまいバッテリー切れで帰還できなくなる(UCA5-D-HS1)
- 暴走
  - コントローラ故障
    - コントローラの故障で制御指示通りに動かなくて漂流(UCA4-N-HS3)
  - カセンサ故障
    - カセンサー故障で制御指示が出せずに漂流(UCA4-N-HS5)
    - カセンサー故障で、操船制御指示が乱れ思い通りの方向に進まずに漂流(UCA4-P-HS2)
  - モータ・スクリュー故障
    - モータ・スクリューの故障で機体を動かせずに漂流(UCA4-N-HS4)
    - モータ・スクリューの一部故障で、操船制御指示どおりに進まずに漂流(UCA4-P-HS3)

FTAとの比較

- 天候悪化
  - 管理（予測）ミス
    - 運転者から天候が悪化しつつあるという報告があったが、管理者が予報から大丈夫という判断をして帰還せずに漂流(UCA2-N-HS1)
    - 運転者からの帰還判断の要請（天候悪化）への判断が遅れて帰還できなくなった(UCA2-T-HS1)
  - 現場の判断ミス
    - 現場の天候を知らずに出航指示を出して遭難(UCA1-P-HS1)
    - 現場の天気予報を読み違えて出航指示で遭難(UCA1-P-HS2)
    - 想定時間内に任務が完了せず、任務を延長してしまった結果、帰還操作が遅れてバッテリーが切れる(UCA5-T-HS1)
- 想定外の外乱
  - 強風で機体が思うように動かせず、帰還前にバッテリーが切れそのまま漂流(UCA5-T-HS2)
  - 大型船との衝突など
- 指示のミス
  - 管理者からの指示ミス
    - 点検終了前に出航指示を出して遭難(UCA1-T-HS1)
    - 一旦出した運転計画や出航指示をキャンセルしたが伝わずに出航して遭難(UCA1-D-HS1)
    - 一旦出した緊急帰還要請をキャンセルしたが伝わらず、運転継続したのに、管理者は帰還したと思い込んで救助をださなかった(UCA2-D-HS2)
    - 事前点検指示を忘れる、または、指示したものの補助員が聞き間違え事前点検をしないで出航(UCA3-N-HS1)
  - 補助員からの指示ミス
    - 機体に不備があるまま運転許可を出し、トラブルで漂流(UCA7-P-HS1)
    - 点検結果を受け取る前に間違って運転開始許可を出してしまい、そのまま出航して漂流(UCA7-T-HS1)

FTAとの比較

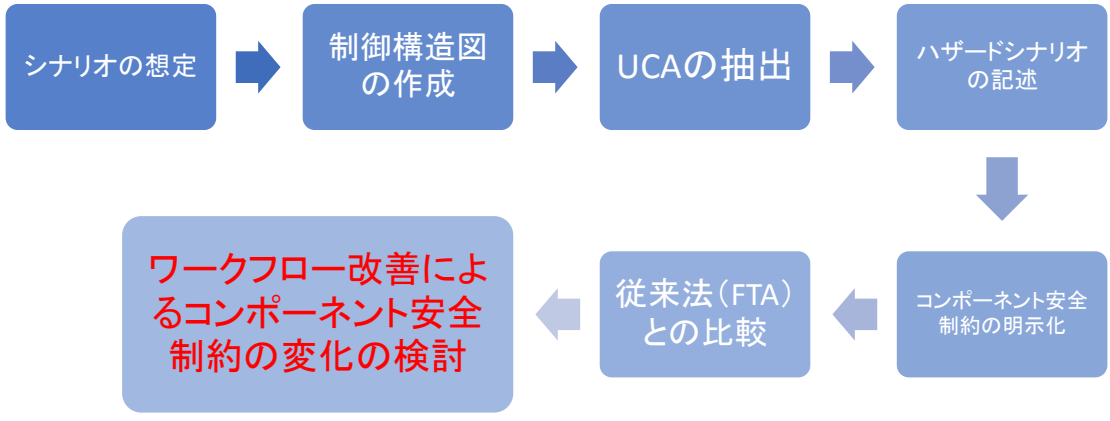
- 無線通信切断
  - 無線通信が切断され緊急帰還要請が伝わらずに、漂流(UCA2-N-HS3)
- 運転ミス
  - 運転スキルが十分でなく、うまく操船できずに漂流(UCA4-P-HS4)
- 点検ミス、点検なし
  - 事前点検の指示は受けたが、日時を間違え、事前点検なしで出航(UCA3-T-HS1)
  - 事前点検を指示に従った方法で行わない、補助員の判断で省略などで、不十分な事前点検で出航(UCA3-D-HS1)
  - 事前点検を早く終わるよう管理者からの指示があり、補助員が不十分な点検で終了して出航(UCA3-D-HS2)
  - 補助員の悪意により故意に事前点検をしないで出航しトラブルで漂流(UCA6-N-HS1)
  - 補助員が事前点検を忘れ、そのまま出航しトラブルで漂流(UCA6-N-HS2)
  - 間違った手順書で事前点検し、出航後にトラブルで漂流(UCA6-P-HS1)
  - スキル不足で間違った点検を行い、出航後にトラブルで漂流(UCA6-P-HS2)
  - 管理者からの事前点検指示の受取が遅れ、事前点検をせずに出航(UCA6-T-HS1)
  - 補助員の点検作業における訓練不足により、事前点検が遅れて、点検なしで出航(UCA6-T-HS2)
  - 管理者からの事前点検指示の受取が遅れ、事前点検の開始が遅れる。遅れを取り戻そうとして補助員の判断で点検を省略または中断をし、そのまま出航(UCA6-D-HS1)
- 判断ミス
  - 管理者による判断ミス
    - 運転員の体調を考えずに出航指示で遭難(UCA1-P-HS3)

FTAとの比較

- FTAのみで発想できたハザード要因
  - 充電忘れ
  - バッテリー故障
  - 大型船との衝突など
- STAMPのみで発想できたハザード要因
  - 立ち往生（迷子になる）
  - 任務やり残し
  - 進行方向間違い
  - 判断ミス
  - 指示のミス
  - 無線通信切断
  - 点検ミス、点検なし
  - 判断ミス

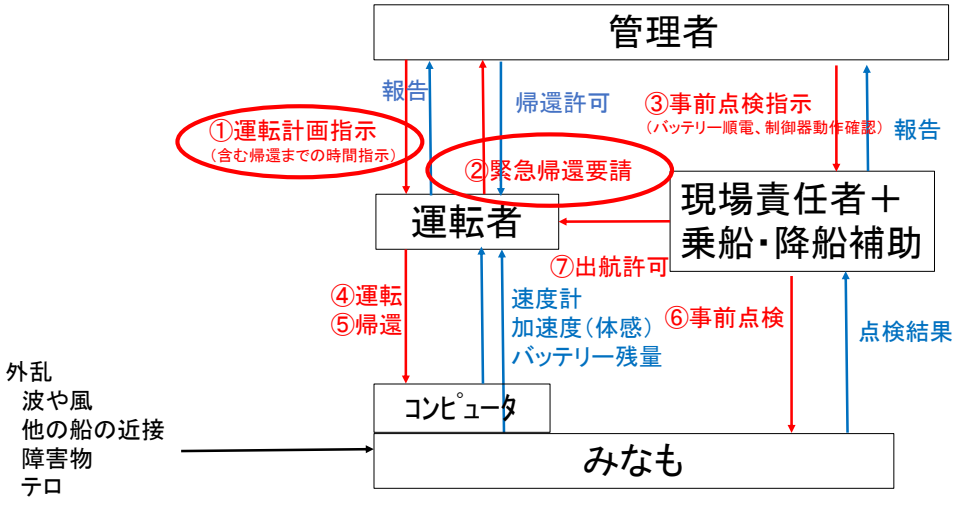
本発表での説明の流れ

STAMP/STPAによる分析→従来法との比較→ワークフロー改善

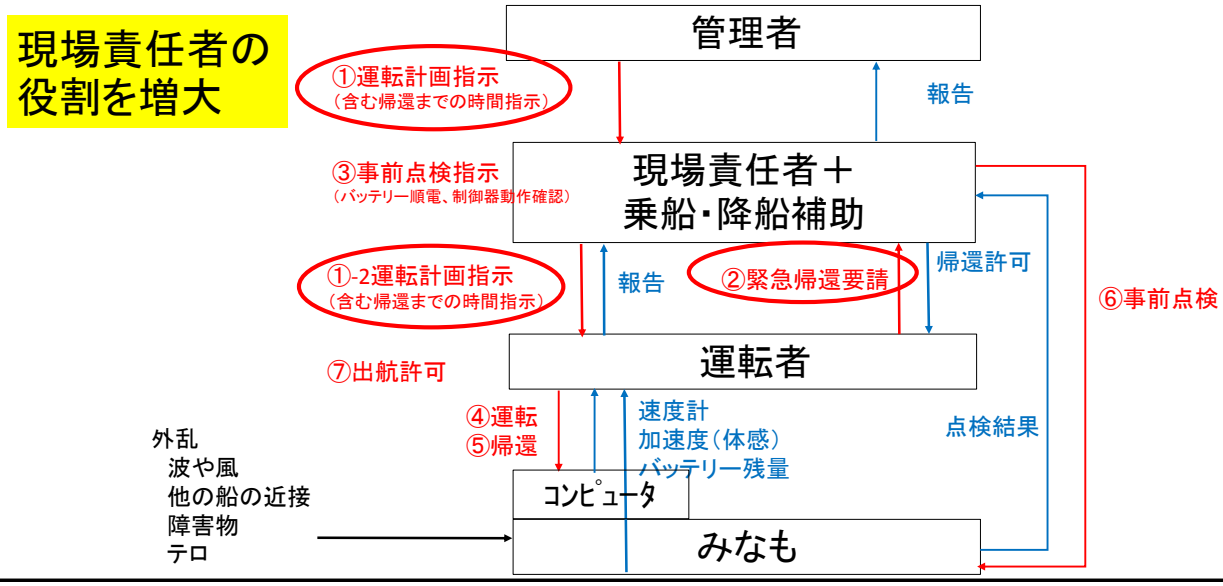


2016.3.10　兼本@会津大学

1.2 水上セグウェイみなもの安全分析（制御構造図（1））



ワークフロー変更後との安全制約の比較（変更後の制御構造図）



コントロールアクション	主体	被主体	コントロールアクションの前提条件	与えられないとハザード（NotProviding）	与えられるとハザード（IncorrectlyProviding）	早すぎ、遅すぎ、誤順序でハザード（IncorrectTiming）	早すぎる停止、長すぎる適用でハザード（IncorrectlyStop）
①運転計画指示	管理者	現場責任者	期間までの時間指示も含む	出航しないので安全側	不適切な運転計画指示による遭難（UCA1-P）	~~事前点検指示前に、運転計画を指示して、点検なしの出航（UCA1-T）~~	一旦出した運転計画をキャンセルして混乱（UCA1-D）
①-2運転計画指示	現場責任者	運転者	期間までの時間指示も含む	出航しないので安全側	不適切な環境条件での出航指示による遭難（UCA12-P）	~~帰還判断が遅れてハザード（UCA2-T）~~	該当なし
②緊急帰還要請	運転者	現場責任者	運転者と管理者のどちらを主体と考えるべきか？ここでは現場優先で考える。 ただし、天気予報情報などで緊急帰還指示をするのや管理者	緊急帰還要請が伝わらずに漂流（UCA2-N）	不必要な帰還要請は安全側	帰還判断が遅れてハザード（UCA2-T）	~~事前点検を途中で中断し、不十分な点検で出航（UCA3-D）~~
③事前点検指示	管理者	現場責任者	バッテリー確認、コントローラ動作確認、スクリュー動作確認、本体確認など	事前点検なしで出航させ、ハザード（UCA3-N）	不必要なタイミングでの事前点検は安全側	事前点検が遅れて、点検なしで出航（UCA3-T）	事前点検を途中で中断し、不十分な点検で出航（UCA3-D）
④運転	運転員	みなも	計画に沿って一定時間運行し調査活動を行う	制御指示どおりに動かなくて漂流、ハード故障と強風などの影響がある。バッテリー切れもある（UCA4-N）	指示なしで動いて漂流（UCA4-P）	制御指示より遅れて動いて衝突（これは今回は対象外）	一旦出した制御指示を止めて衝突（対象外）
⑤帰還	運転員	みなも	計画時間内に帰還する	帰還制限時間を忘れてバッテリー切れで帰還できない（UCA5-N）	帰還するだけなので安全側	帰還操作が遅れて、バッテリー切れで帰還できない（UCA5-T）	帰還途中で、再度、沖に出て帰還できなくなる（UCA5-D）
⑥事前点検	現場責任者	みなも	バッテリー充電、コントローラ点検、スクリュー点検、本体点検	~~事前点検なしで出航しトラブルで漂流（UCA6-N）~~	間違った事前点検でトラブル・漂流（UCA6-P）	事前点検が遅れて、点検なしで出航（UCA6-T）	事前点検を途中で中断し、不十分な点検で出航（UCA6-D）
⑦出航許可	現場責任者	運転員	点検完了を知らせ運行開始を指示	運転開始をしないので安全側	不十分な状態で出航許可を出してハザード（UCA7-P）	~~事前点検前の早すぎる許可で運転を開始しハザード（UCA7-T）~~	該当無し

対策のまとめ1（コンポーネント安全制約）

（緑：変更後に不要になった対策、赤：新たに必要になった対策）

- コントローラー
  - 代替コントローラへの切り替え
  - 電源遮断後の手動による運転
  - コントローラーを介さずにモーターを制御できる機能の追加
- 運転操作・インターロック関連
  - 手動による運転の対応
  - バッテリー残量のアラート機能の追加。補助バッテリーの設置
  - ハッカーによる乗っ取りを検出する監視機能の追加
- 通信
  - GPS機能による位置情報の確認、管理者または補助員からの進行方向の指示
- 点検
  - モータ・スクリューの定期点検。起動前のモータ・スクリューの検査
  - カセンサーの定期点検。起動前のカセンサーの検査
  - 無線機器の事前の動作確認
  - 運転者自身による最終点検。管理者への事前点検結果の報告・確認要求（現場ですべて確認できるため不要になった）
  - 点検基準の明確化（現場の責任が大きくなったため点検基準を事前に明確化しておくことが大事という新たな対策がでてきた）

対策のまとめ2（コンポーネント安全制約）

（緑：変更後に不要になった対策、赤：新たに必要となった対策）

- ワークフロー改善（1）
  - 事前点検、運転計画、出航指示のワークフローと、チェックシートによる確認ルールの明確化、指示ルート（ワークフロー）の変更も含む
  - チェックシートを管理者が確認し最終判断するようなワークフロー、または、出航指示は現場責任者のみとするワークフローへの変更（現場責任者が出航指示をすることで解決）
  - 点検結果の記録をチェックシートで残し、運転管理者に報告するなどのワークフローの改善（現場ですべて確認できるため不要になった）
  - キャンセルを含む指示に対する報告の義務付け、ワークフローの改善
  - 点検結果を管理者にフィードバックし、管理者による最終確認を行ったのち管理者からの出航許可（現場での勝手な判断を禁止するルール）（現場ですべて確認ならびに出航許可ができるため不要になった）
  - 帰還予定時刻の際の管理者または補助員から帰還命令
  - 天候の正確な事前予測
- ワークフロー改善（2）
  - 出航ルールの明確化（予報確認、現場の判断優先、体調確認など）（現場の責任が大きくなったため各種の判断基準を事前に明確化しておくことが大事という対策がより強調される）
  - 精度の良い天気情報の利用
  - 管理者としての判断ルールの明確化
  - 運転者から出した緊急帰還要請のキャンセルルールの明確化と、管理者側からの緊急帰還指示ルールの作成（現場ですべて確認できるため不要になった）
  - 間違いにくいような手順書の作成（順番にチェックしながら点検を進めるなど）。管理者による再確認
  - 帰還開始前の任
  - 務の遂行状況のチェック。管理者へ任務の報告・確認要求
- 訓練、規律・統制
  - 運転者による運転操作の事前訓練（モーターが一部しか動かない場合の操作訓練を含む）
  - 点検作業の十分な訓練。管理者による再確認
  - 遠くの目印を目標にして現在位置を把握する訓練
  - 運転者の安全を最重要視する安全文化
  - 運転者の体調を最重要視する安全文化

ワークフローの変更による変化

- 変更後に新たに必要となった対策
  - 点検基準の明確化
  - 出航ルールの明確化（予報確認、現場の判断優先、体調確認など）
- 変更によって不要となった対策
  - 運転者自身による最終点検。管理者への事前点検結果の報告・確認要求
  - チェックシートを管理者が確認し最終判断するようなワークフロー、または、出航指示は現場責任者のみとするワークフローへの変更
  - 点検結果の記録をチェックシートで残し、運転管理者に報告するなどのワークフローの改善
  - 点検結果を管理者にフィードバックし、管理者による最終確認を行ったのち管理者からの出航許可
  - 運転者から出した緊急帰還要請のキャンセルルールの明確化と、管理者側からの緊急帰還指示ルールの作成

考察：ワークフローの変更による安全制約の変化

- 現場責任者に権限が集中するため、管理者を通したダブルチェックなどが減り、現場責任者と管理者管間における人と人の相互作用によるハザードシナリオの減少が期待できる
- 現場責任者の責任（運転者の体調管理、点検作業）が大きくなるため、権限の集中によって引き起こされるハザードシナリオを防ぐための対策（運転者の体調を最重要視する安全文化や点検基準の明確化）が新たに必要となる

まとめ

- 抽象化したステークホルダーの責任、運用シナリオを最初に定義しておくと、議論の混乱が少なくなる。あまり具体的な仕様にとらわれすぎると自由な発想を妨げる。KJ法と同じくブレーンストーミングの際は批判をしない
- UCAとHCFに記号を付けておくと、複数人での議論の際に混乱がなくわかりやすくなる
- FTAは、コンポーネント単独のハザードは網羅できるが、詳細なシナリオの記述力が足りない
- ワークフローの変更による安全制約の改善効果が明確になる
- STAMP/STPAでは、
  - 人や組織が絡んだ場合のハザードの分析に有効
  - 特に、ワークフローに潜むハザードの分析に有用
  - ハードの故障は、ブロック図を詳細化すればFTAと同等になる