

第5回AI/IoTシステム安全性シンポジウム

Asian STAMP Workshop

2023/12/1 @ 国立情報学研究所

自動運航システムの設計・検証のためのSTPAの活用事例紹介

Introduction of Examples Using STPA in Design and Verification of Autonomous Navigation System

中島 拓也¹ 暮田留依²

¹ 東京大学 大学院新領域創成科学研究科

² 株式会社MTI



目次

1. 背景

- 海運における課題
- MEGURI2040プロジェクトにおける自動運航船開発と実証
- 自動運航船に対するコンセプト開発と安全性

2. モデルを活用したコンセプト設計とSTAMP/STPAの導入

3. STAMP/STPAの実践

- 自動運航船システムへのSTPA適用事例（先行研究）
- STPA実施のポイント
- 分析の流れ

4. STAMP/STPA結果の検証・妥当性評価シナリオとしての活用

- 記述モデルと数値モデルを組み合わせたシナリオベース検証フレームワークの提案

5. まとめ

目次

1. 背景

- 海運における課題
- MEGURI2040プロジェクトにおける自動運航船開発と実証
- 自動運航船に対するコンセプト開発と安全性

2. モデルを活用したコンセプト設計とSTAMP/STPAの導入

3. STAMP/STPAの実践

- 自動運航船システムへのSTPA適用事例（先行研究）
- STPA実施のポイント
- 分析の流れ

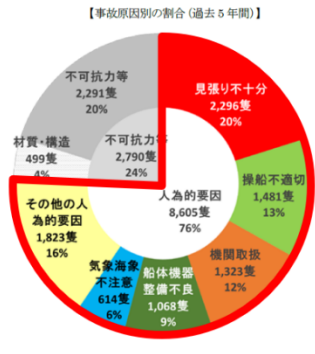
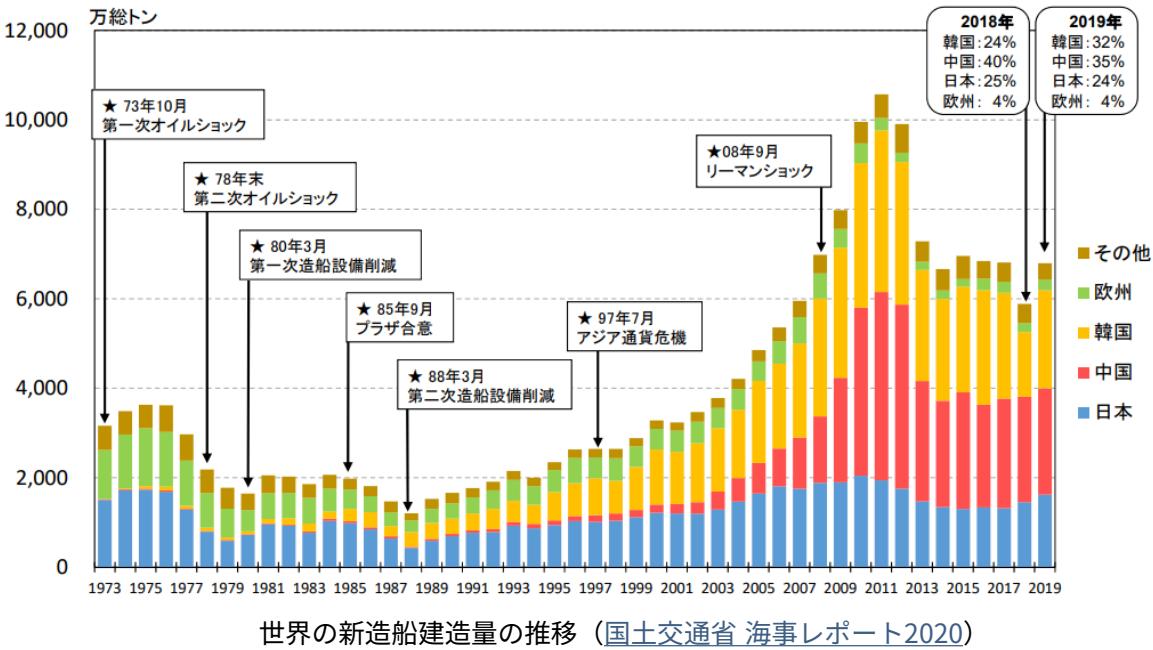
4. STAMP/STPA結果の検証・妥当性評価シナリオとしての活用

- 記述モデルと数値モデルを組み合わせたシナリオベース検証フレームワークの提案

5. まとめ

海運業界をとりまく状況

- 社会インフラとしての役割：世界の約80%，日本の99.6%の貿易量を負担
- ステークホルダー
 - 船の使い手：船主，管理会社，etc.
 - 船や搭載機器，機能の供給者：造船所，船用機器メーカー，etc.
 - 認証・評価機関：各省庁，船級協会，研究所，etc.
- 課題：船の受注競争，船員不足，交通量増加に伴う操船難易度上昇，離島航路の維持 等々．．．
→ 「安全に使える船を安定的に作って動かせる体制」の必要性



海難事故の要因
(国土交通省，2020)



(内航) 海運の課題と自動運航船

- 内航海運
 - 慢性的な船員不足の一方，
モーダルシフトといった輸送量維持/向上の要請
 - 増大する交通量：操船の困難度も上昇の一方
- 自動運航船による，人手に依存しない安全の可能性
 - 要素技術の進歩による，操船タスクの自律化の実現性
 - ヒューマンファクターの補完による安全性向上
 - 例) 画像認識による物標・他船認識，避航航路提案



画像認識による他船検知・見張りシステムの例 (ORCA AI)

鉄道、内航海運の輸送量・分担率を増強



物流革新緊急パッケージ

自動運航船のベネフィット Kim et al. (2022)

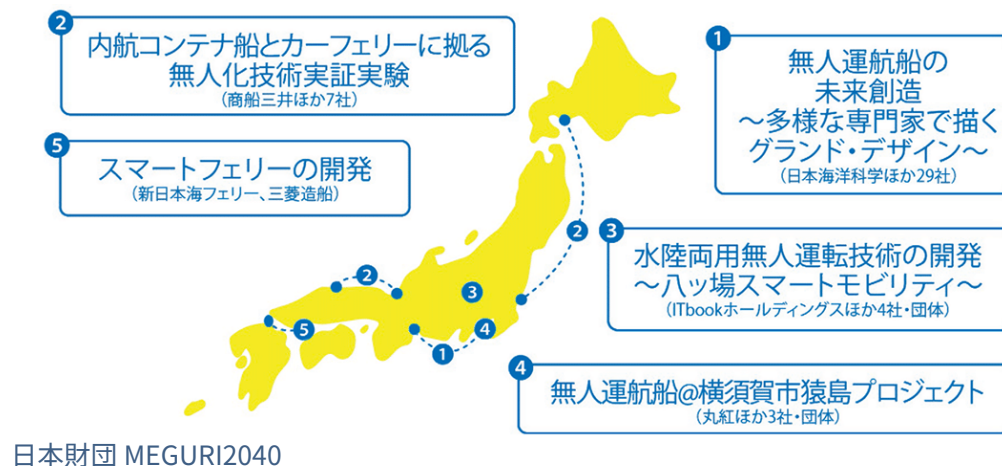
Dimension	Potential benefits of MASS
Safety	●Reduce the number of maritime traffic accidents caused by human factors (e.g., fatigue, human errors, violations, improper maneuvering) ●Reduce and reorganize the workload of human operators while decrease the risks of occupational accidents on board ●Decrease the number of human injuries and fatalities from maritime accidents
Security	●Lessen risk due to the lack of crew to hold hostage
Environment	●Reduce energy consumption through fuel saving measures and innovative ship design ●Support maritime decarbonization and reduction of greenhouse gas emissions
Economy	●Reduce crew cost and proportionally higher cargo capacity due to absences of human-support facilities and systems on board ●Reduce operating costs and improved ship fuel efficiency lead to better economic profitability
Human element	●Move ship crew from the “24 h society” to shore-based office environment ●Address several humanitarian challenges the industry currently faces, such as welfare issues, crew change, stranded seafarers under pandemic situation
Societal influence	●Mitigate the shortage of seafarers ●Increase the attractiveness of seafaring professions ●Mitigate gender imbalance issues in the maritime industry

日本財団 無人運航船プロジェクト「MEGURI2040」

- 世界に先駆けて内航船の無人運航の実証試験を成功（～2022/03）
- 社会実装に向けたPhase2がスタート（2022/10～）

Phase2の実証実験（-2026/03；予定）

Phase1の実証実験（2022）



内航コンテナ船「すざく」
(無人運航実証船 @ DFFASプロジェクト)



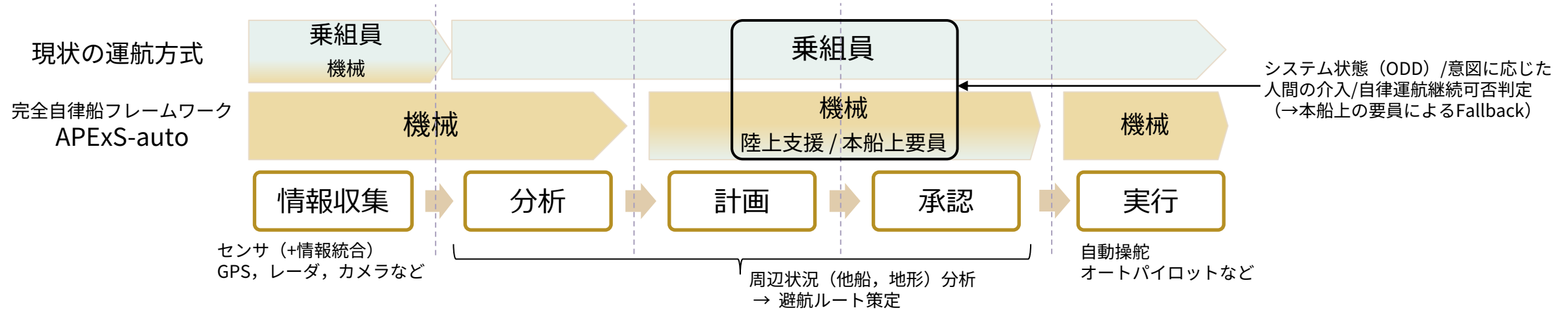
自動運航船（システム）の特徴：自動運転との比較，実装に向けた課題

	自動運航	自動運転
対象タスク	見張り，操船，機器の保守，離着舷等を複数の人間が分担して担当しており，対象タスク・度合が多様	基本的には，1人の運転手の運転タスク（Dynamic Driving Task: DDT）のみを扱う
稼働場所	- 長期間海上での連続航行 - 運転者の交代，機器の頻繁な交換等が難しい（一部不具合がある状態での運航頻度も高い）	陸上かつ断続的稼働のため比較的保守・点検しやすい
操縦性能	大型船の場合は特に急停止，急旋回が困難	ある程度急停止，急旋回が可能
環境影響	波や潮流によりその性能が大きく変化（浅水域・実海域）	路面の状況により性能は変化も比較的予測しやすい
交通ルール	自由度が比較的高い（→遭遇シナリオが多種多様，“正解”の定義が困難）	道路や信号等，移動可能範囲などの制約が多い ↔ 交通ルールは比較的明確
障害物	漁業者や漁網の存在	バイクや自転車，歩行者の存在
自律化ターゲット	- 内航船員28,000人，邦人外航船員2,000人 - 基本的にはBtoB	- 運転免許保有者数8199万人（2021年） - 大半はBtoC，街づくり・生活等への派生影響
自律レベル	遠隔化も含めて，定義が乱立	SAE J3016のレベルが広く普及

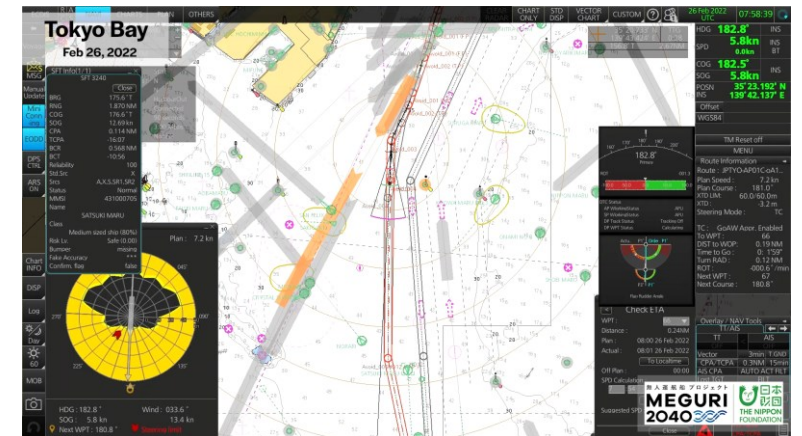
- “自動運航船/システム”の定義やスコープ：統一的/包括的な基準は策定途上（IMO MASS Codeなど）
- 個別のセンサ（GPS，レーダなど）や制御機器（オートパイロット）といった個別機能の性能標準は既に存在
 - 有人/既存船における運航タスクを部分的に担うモジュールは既に商用化，市場が成立
 - 自動運航システム/船の構築：既存技術も取り込んだシステムインテグレーション

自動運航船（システム）の開発

- MEGURI2040のターゲット：操船タスクに関する、製品化/社会実装に対応した自動運航船の開発



- システムを構成する機器，機能群の開発・統合：V-Process
 - ユーザー（船主，管理会社）が意図する船/自動運航システムの運用：Concept of Operations (ConOps) のもと，
 - 複数の船用機器メーカーが機能開発を行い，
 - システムインテグレーターが系全体を統合し，
 - 岸壁・洋上での検査 → 就航
- 統合対象の機能群がなす機能フロー：



提案されたルートに沿って航行中の例
(古野電気：Action Planning Unit)

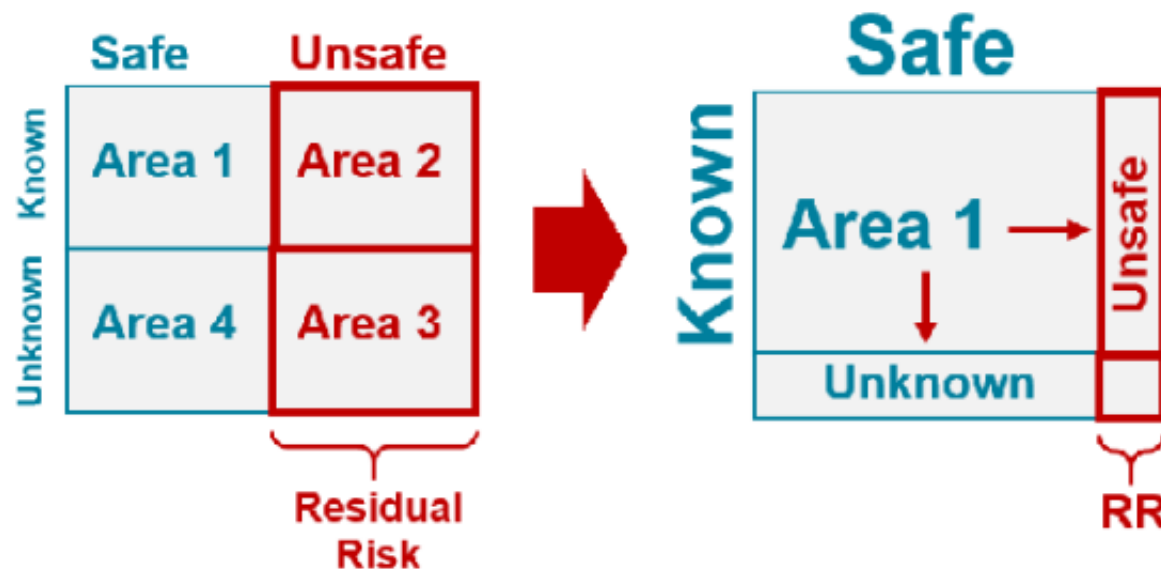
制御指示 / フィードバック のループを孕む一方，モジュールの開発/供給は（ほぼ）タスク粒度で実施

安全性の担保に向けた課題

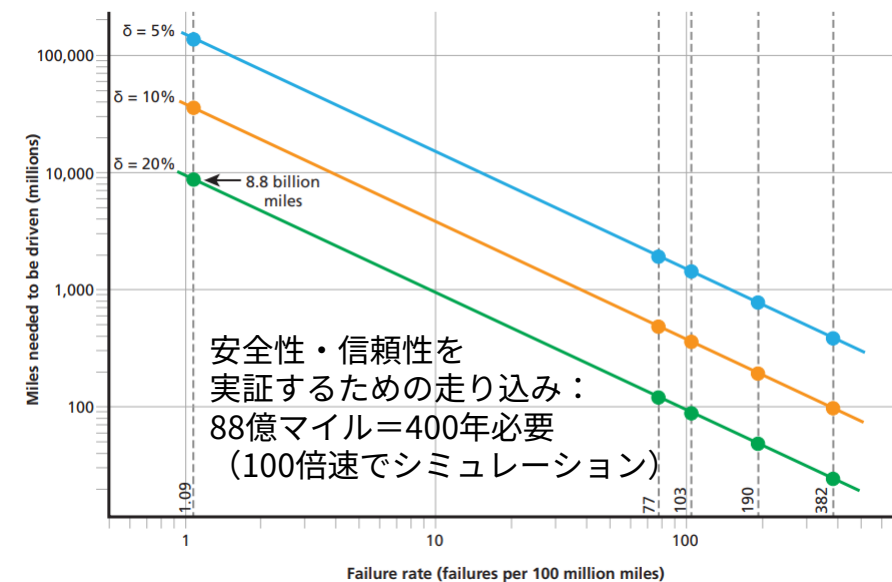
- 自動運航船: ステークホルダーと 機能両面で複雑システムとしての性質
- 安全性の証明/実証: 複雑システムの持つ「想定外」の挙動をいかに削減するか
 - 複雑さ: 要素毎の属性からシステム全体の属性を予測する困難さの度合 (Weaver, 1948)
 - 船舶の場合, (本船搭載・洋上試験の) 前工程ではシミュレーション・リスクアセスメントの実施が肝
- 代替設計: 従来技術と同等の安全性 (equivalent safety) が求められる (MSC Circ.1455)
- コンセプト, 概念設計としてのシステムモデル構築 とリスクアセスメント

→ システミックリスクの明確化: 包括的な安全要求 と テストシナリオの段階的 / 網羅的な定義・検証

自動運転のFailure Rateの見積に必要な走行量
Karla and Paddock (2016)



ISO21448 SOTIFの考え方 Schwalb, E. (2019)



本研究開発の目的

- 自動運航船 / システムの構築：ユーザー要求を起点としたシステムインテグレーションにおける
 - V-Processにおける意思決定：設計 / 検証 / 妥当性評価 で活用可能なシステムモデル群の抽出
 - 機能・安全要求の整備：人の段階的な介入を前提とした要件の定義や検証の目線
- 同等安全性証明のためのリスクアセスメント：網羅的/包括的なシステミックリスク抽出への試み
 - Control Structure以外のモデルも組み合わせ，ガイドワードや定量評価のありかたを整備
 - ◆ プロセスモデルの齟齬への着目：input/output/algorithmおよびassumptionに基づく発想
 - ◆ Contextや，HCF，およびそのBarrierに関してもガイドワードでパターン化
 - シナリオベース検証に繋げるためのテストシナリオ検討手法の実践
 - ◆ シミュレータを活用したMIL/SIL/HILテストや統計的手法への対応

目次

1. 背景

- 海運における課題
- MEGURI2040プロジェクトにおける自動運航船開発と実証
- 自動運航船に対するコンセプト開発と安全性

2. モデルを活用したコンセプト設計とSTAMP/STPAの導入

3. STAMP/STPAの実践

- 自動運航船システムへのSTPA適用事例（先行研究）
- STPA実施のポイント
- 分析の流れ

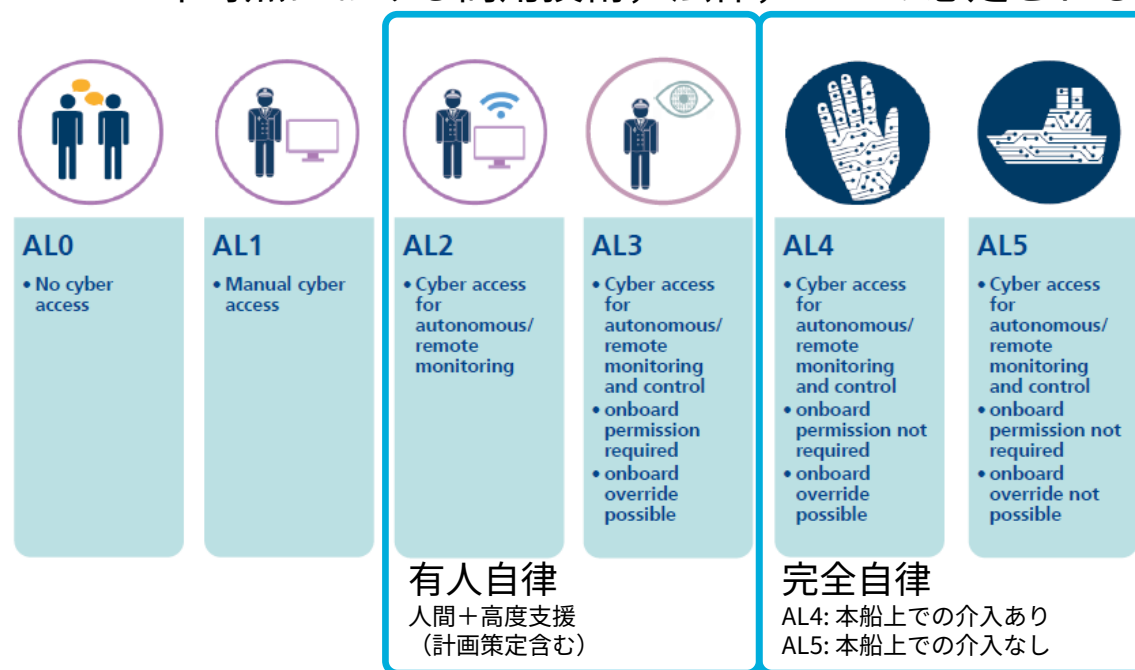
4. STAMP/STPA結果の検証・妥当性評価シナリオとしての活用

- 記述モデルと数値モデルを組み合わせたシナリオベース検証フレームワークの提案

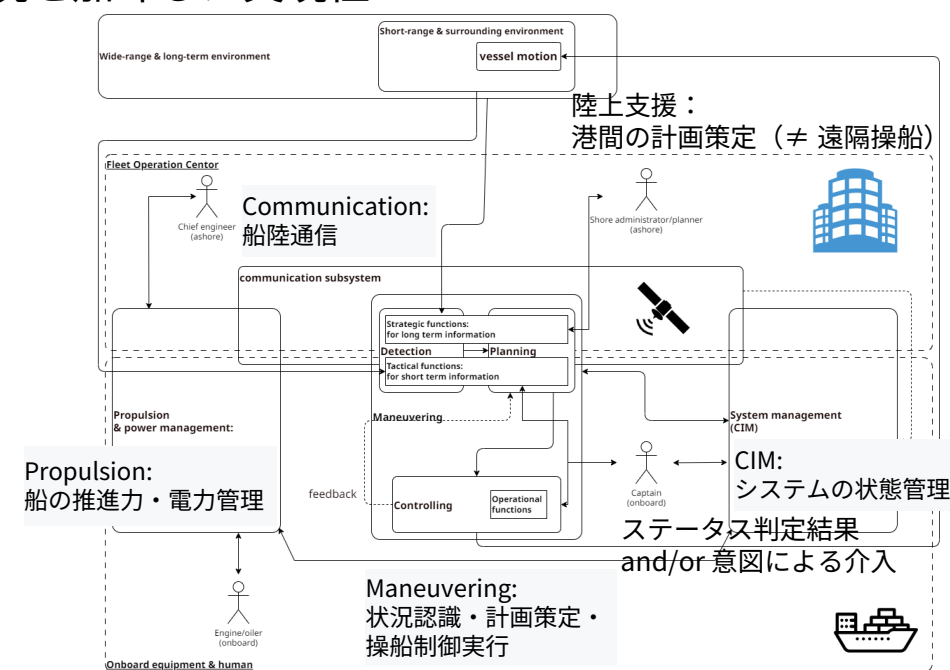
5. まとめ

対象とするシステム：概略

- スコープ
 - 自律レベル: AL-4相当，自律運航機能のODD設定とシステム状態に応じた人間による介入
 - 離棧～着棧における状況認識 → 状況分析 & 意思決定 → 実行 をシームレスに網羅
 - 陸上（FOC: Fleet Operation Center）での計画策定支援・機関システム監視
- ゴール
 - 安全性: 当直負荷を軽減しつつ，自動運航システムを搭載した船舶による運航の安全性担保
 - 2025年時点における商用技術，法律，etc. の想定される状況を加味した実現性



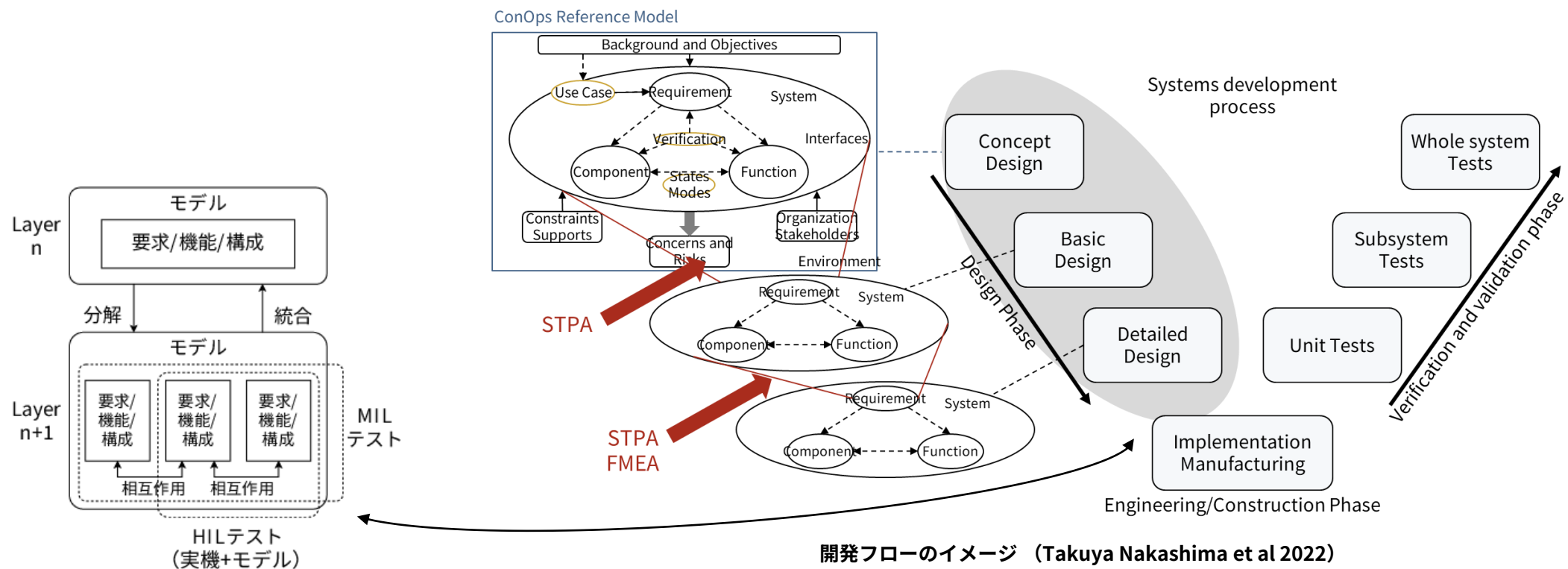
ロイド船級協会による自律運航レベルの定義



自動運航船のシステム概略，ユースケース

システム開発のアプローチ：ConOps，概念設計，リスクアセスメント

- Concept of Operations (ConOps) とコンセプト設計
 - ユーザー（船主/管理会社）の目線で自動運航システムに対する最上位の要求を記述
 - 概念設計：ConOpsと対になる形で，開発目線でのシステムのあり様を表現
(機能要求，サブシステム区分と責務，系全体/機能モジュールのふるまい，etc.)
- リスクアセスメント：ロスシナリオ/テストシナリオや安全要求の抽出
 - 概念設計段階においてSTAMP/STPAを活用しつつ，具体的な実証機器構成に対するFMEAを実施

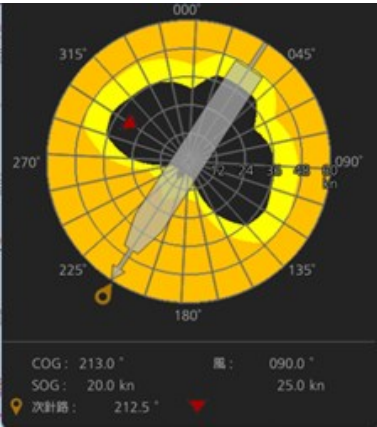


自動運航システムの特徴：ODDとシステムステータス

- 自動運航システムにおけるステータス: 人間によるタスクへの介入の必要度合い
 - Fully Autonomous (FA) : 人間の介入を必要としない完全自律状態（AL4相当）
 - Monitoring with Mind ON (MM) : 人間による介入準備が必要な状態（ふるまいはFA同等）
 - Monitoring with Approval (MA) : 周囲環境悪化などの要因により，避航計画に対する承認が必要な状態（AL3相当）
- システムを特徴づけるODDの評価軸
 - Environmental ODD : 自然環境要因による，本船の運動モデルを考慮した制御継続可能性判断

自動運航船で考えられるODD評価軸（抜粋）

Category	Subcategory	Detail
Scenary	Geography	地形
	Offshore Structure	海上構造物
	Navigational Area	運航海域（要求ルールとの対応）
	Temporarl Area Specifics	航行警報・水路通報 (for Temporal Rule)
Dynamic Elements	Other ships (and type)	各船の動的・静的情報
	Obstacles	流水，海洋生物，魚網，漂流物
	Own ship	制御状態，自船状態
	Support of Own ship	海上/陸上支援の有無・状態
Environmental Condition	Weather and Illumination (Impact on Sensing)	昼夜（Night, Day, Dusk） ， 視界・視程，天候
	Weather (Impact on Actuation)	風向・風速，波高・波向・波周期，潮流流速・龍向
	Connectivity	船陸通信状態



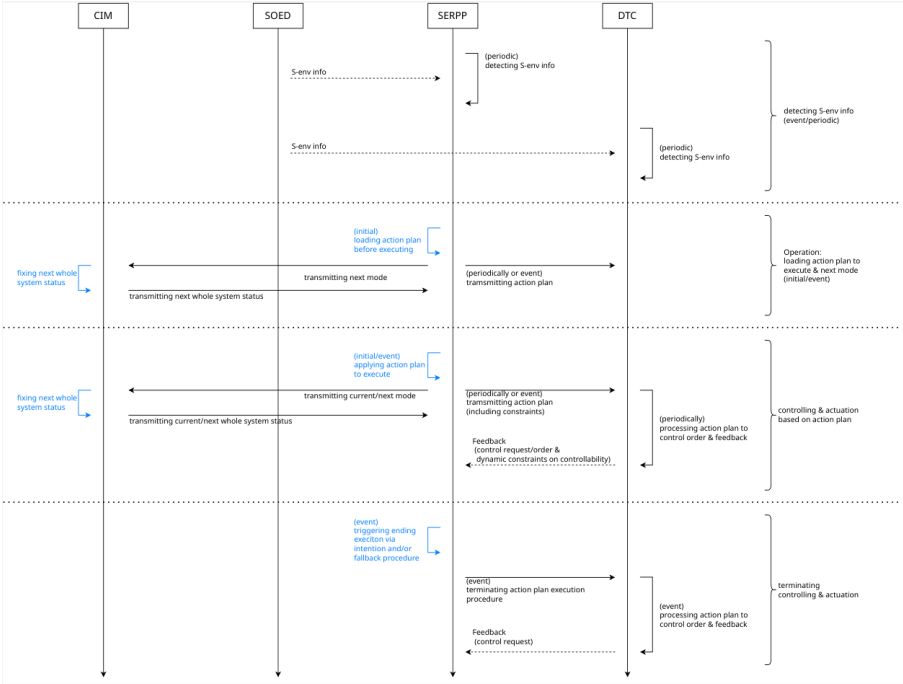
Environmental ODD状態の表示例
(古野電気：Action Planning Unit)

本船状態 と 環境条件から制御可能性を表現
→ 人間により行われてきた判断の補完

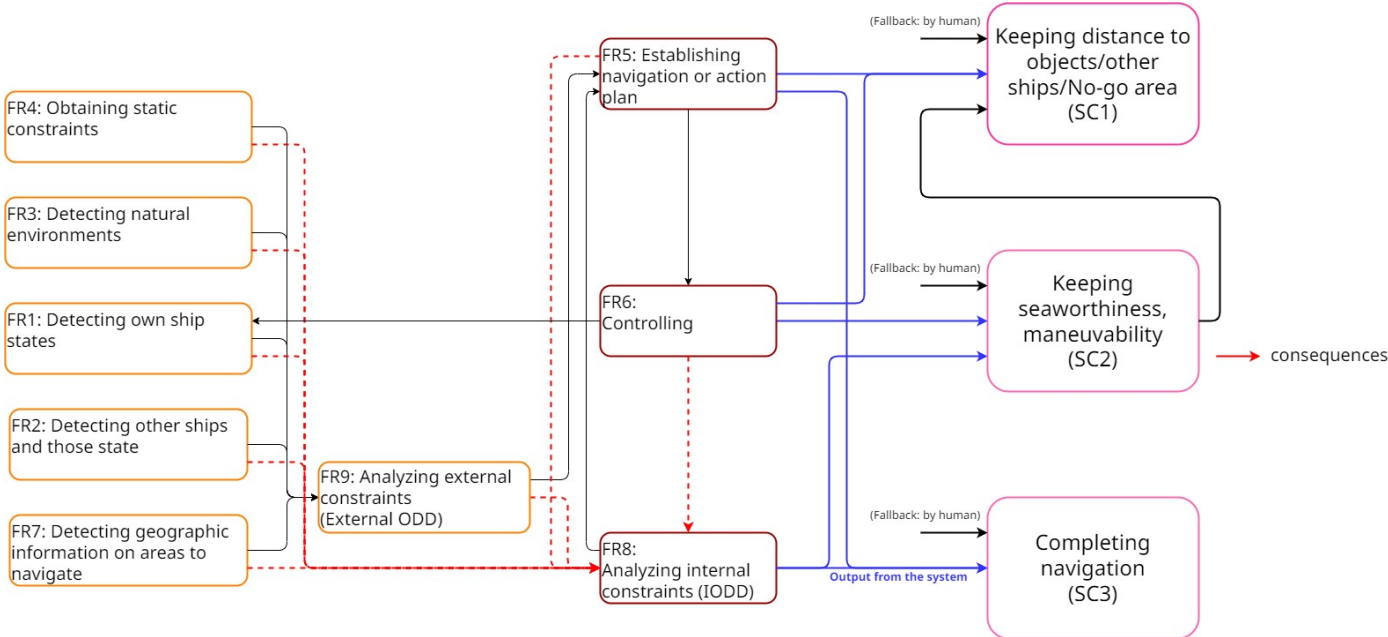
- ODD（など）に起因するシステムの振る舞いを実船（のみ）で全て検証/評価するのは困難
→ シミュレーションベースの検証にも対応可能なシステムモデルとテストシナリオの必要性

自律運航のシステムモデル：分析対象の定義

- 概念設計：ConOpsから誘導されるスコープに対し，機能モジュールを想定したシステムモデル
 - サブシステム構成：Maneuvering / CIM/ Propulsion / Communication
 - 認知（センサ），状況分析 & 計画（航路/船速/etc.）策定，制御実行 タスクと相互作用を加味したモデル
- STAMP/STPAの問題設定と対象
 - システムモデルをコントロールストラクチャに抽出しつつ，ユースケースを反映したふるまいのモデルも参照
 - 安全制約：「船として危険な状態に至らない」= 本船上要員によるフォールバックも含めた安全担保



システムモデルの例：CIM / Maneuvering間シーケンス



自動運航システムの安全制約と基本機能要求

目次

1. 背景

- 海運における課題
- MEGURI2040プロジェクトにおける自動運航船開発と実証
- 自動運航船に対するコンセプト開発と安全性

2. モデルを活用したコンセプト設計とSTAMP/STPAの導入

3. STAMP/STPAの実践

- 自動運航船システムへのSTPA適用事例（先行研究）
- STPA実施のポイント
- 分析の流れ

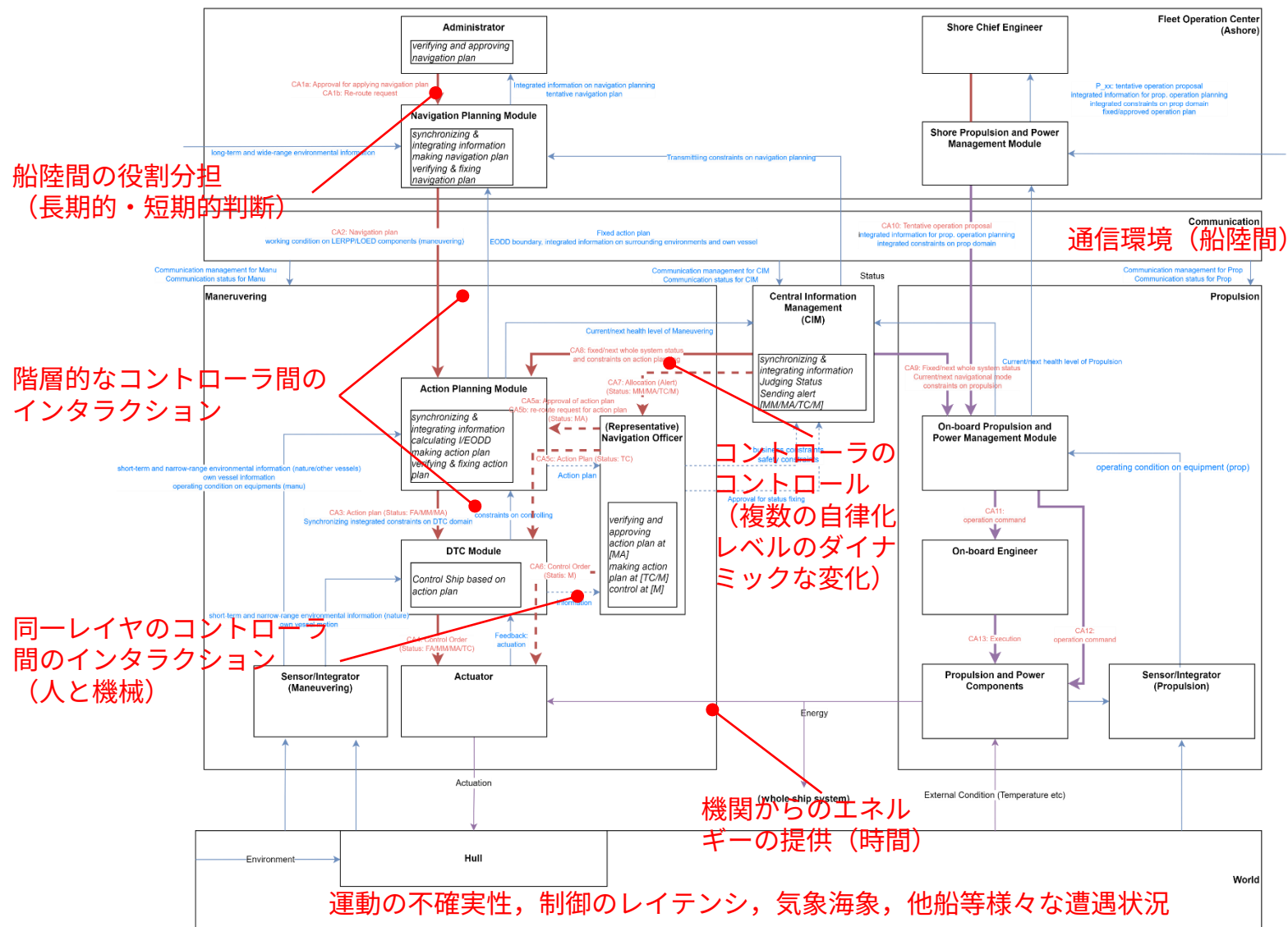
4. STAMP/STPA結果の検証・妥当性評価シナリオとしての活用

- 記述モデルと数値モデルを組み合わせたシナリオベース検証フレームワークの提案

5. まとめ

今回のシステムの特徴（STPAで着目しておくべきポイント）

- 階層的なコントローラ間のインタラクション
- 船陸間の役割分担（長期的・短期的判断）
- 同一レイヤのコントローラ間のインタラクション（人と機械）
- コントローラのコントロール（複数の自律化レベルのダイナミックな変化）
- コントローラのための機関からのエネルギーの提供（時間）
- 運動の不確実性，制御のレイテンシ，気象海象，他船等様々な遭遇状況
- 通信環境（船陸間） 等



Control Structure of the target system

Literature Review (自動運航船システム×STPAの例)

文献	概要（対象システム，SC/UCA/HCFの例）	手法の特徴と限界
Wróbel et al., 2018 (RESS)	STPAを用いた自動運航船の分析．ステークホルダや，陸上コントロール施設，通信インフラ，バーチャルキャプテンなどを想定．一方，コンソールなどもモデルに含め，すべてのインプット・アウトプット信号を分析．あわせて，手法に関連する不確実性を評価する方法紹介．管理可能な不確実性によって影響を受ける可能性があることが示された．	人の段階的な関与，Dynamic Safety Managementという観点での分析が足りていない．What ifに近い（Control Functionを区切ってSTPAを実施している）．Control Structureの構成要素の粒度のばらつきあり．Virtual Captainが，すべての船内機器と手順を制御および調整するAI コンピュータという仮定．
Valdez Banda et al., 2019	自動運航船の設計のために，首尾一貫した透明で追跡可能な安全入力情報を提供する初期のハザード分析と管理のためのプロセスを提案．HazardからMitigation Action (Safety Control) を抽出したうえで，STPAはそのSafety Controlを担保するための4つのGWとして利用．	STPAと叫ぶつつも，4つのガイドワードを用いて個別の制御信号による不具合を分析している．
Chaal et al., 2020	STPA コントロールストラクチャを構築．フレームワークの適用により，船員から提供された情報は，自律型船舶の初期の機能説明を作成する上で不可欠であることが示された．さらに，その結果、自律船の技術的側面に加えて、これらの船を現在の海上運用の組織的管理構造に導入することは，設計の初期段階で対処する必要がある課題をもたらすことも明らかになった．	分析の前段としてのControl Structureのみ．船舶よりも広い概念で，規制など組織的なものも含めて記載している．一方，人と機械のやり取りの部分は解析されていない．
Chaal et al., 2022	System Theoretic Process Analysis (STPA) を使用し、システムリスクを推定するフレームワークにはベイジアン ネットワークが使用．STPA と BN を統合すると，特定された RCO の優先順位付けが可能に．提案された方法は，例示的なケーススタディとして自律海水冷却システム（SWC）の概念に適用．	自動運航船の分析ではなく自律海水冷却システム．ベイジアンネットワークでRisk Control Optionの優先順位付けが可能になる．
Rokseth et al., 2018	STPAを採用して、検証目標と関連する危険なシナリオを生成．これらは範囲を指定または拡張し、検証アクティビティの受け入れ基準を提供し、さらにテスト ケース生成への入力として機能する可能性．ハードウェア、ソフトウェア、および人間のオペレーターの間の相互作用の問題．シナリオの優先順位付けが課題（V&Vの観点，ロスの観点）．	V&Vに繋げるという観点ではKhashtgir et al., 2021と非常に近い．Process variablesを定義しているが，ややContext寄りでProcess Modelそのものにはアプローチしていない．ただし，自動運航システムではなくDPIに対してのもの．
Wróbel et al., 2018 (OE)	STPAを用いた遠隔運航船の分析．ステークホルダや，陸上コントロール施設，通信インフラ，バーチャルキャプテンなどを想定．一方，コンソールなどを定義し，すべての信号を分析．	Wróbel et al., 2018 (RESS)の手法で前提を変更したもの．一連のロスシナリオについては検討していない．人と機械とのやり取りや，時系列的な意思決定の差分を考慮していない．

- STPAガイドワードを用いたハザード抽出（ロスシナリオとしてまとめている事例は少ない）
 - 対策が冗長・膨大となり設計にFBしづらい，検証シナリオの構築につなげづらい，システミックリスク抽出漏れ？
- 長期航海計画・短期航海計画等のコントロールの輻輳や，段階的な自律ステータスの変化は未分析
- 実効的にシステムを建造・検証していく観点で，対象システムの想定がやや非現実的なものがある

今回のSTPAのポイント

- 分析対象
 - Human-Machineの役割の段階的推移，航行モードの推移も含めて分析
 - 長期・中期・短期のコントロール，船陸の役割分担にも注目
- 手法
 - プロセスモデルの齟齬にフォーカスを置いたシステミックリスク抽出
 - 分析ではなく，設計対象であるシステムをより理解するという思想
 - Control Structure以外のモデルの活用，ガイドワードや定量評価のありかたを整備
 - input/output/algorithmおよびassumptionを想定し，Process Model Gapを発想
 - Contextや，HCF，およびそのBarrierに関してもガイドワードでパターン化
- 活用
 - シナリオベース検証に繋げるためのテストシナリオ検討手法の実践

Step 1: Define Purpose of the Analysis

1. 損失の識別

- L-1：人命（自他船乗組員等）の喪失・負傷
- L-2：自船の損失または損害
- L-3：他船や構造物等，海洋環境の損失または損害
- L-4：輸送ミッションの喪失（→ 顧客満足度の損失）

2. システム（※）レベルのハザードの識別

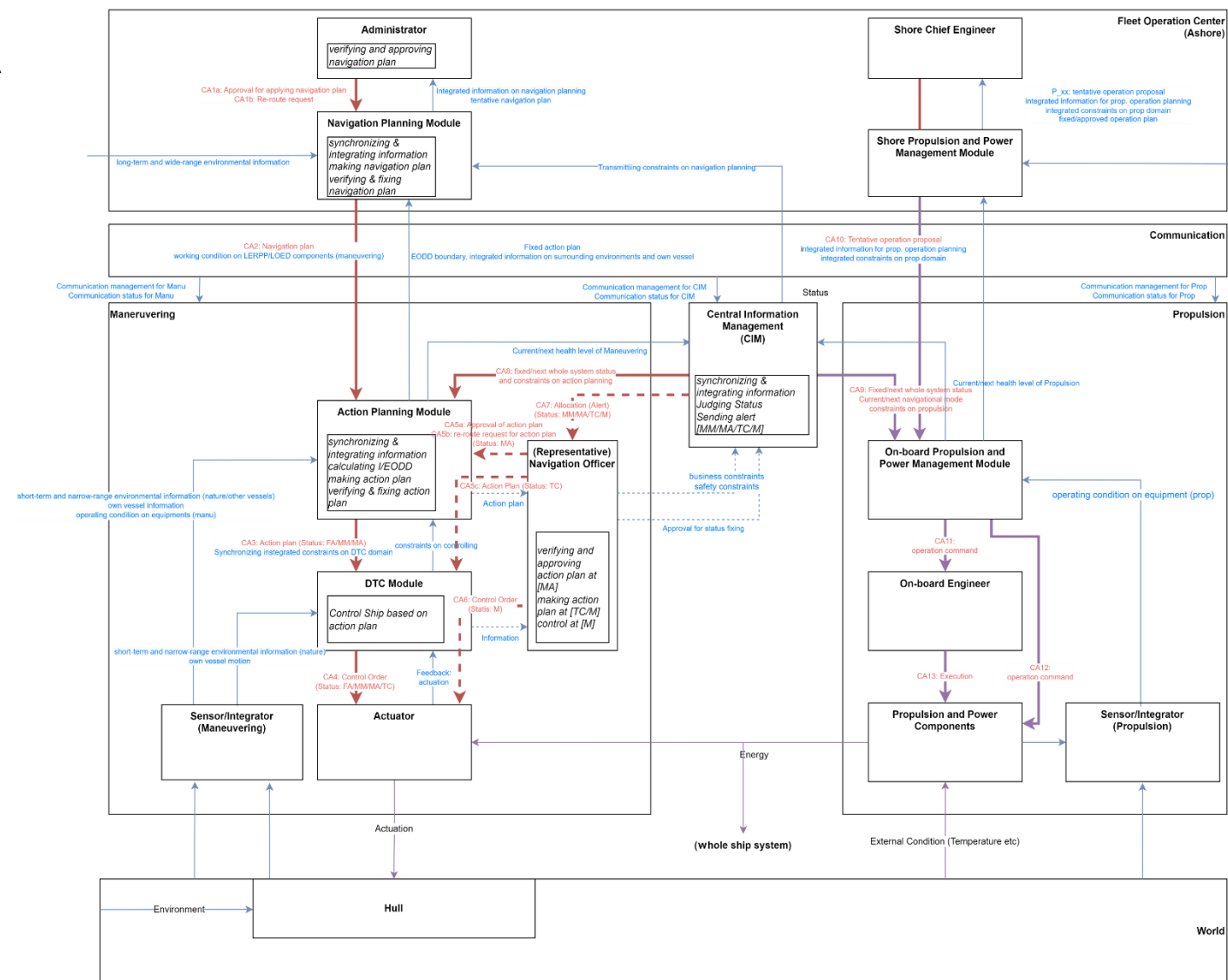
- H-1：自動運航船が，他船や陸地などに接近しすぎる [L-1, L-2, L-3, L-4]
- H-2：自動運航船の堪航性が失われる [L-1, L-2, L-3, L-4]
- H-3：自動運航船が，港から港までの輸送ミッションを完結できない [L-4]

3. システムレベルの制約の定義

SC_ID	Safety Constraints	Accident	Description
SC1	他船・障害物および陸地や浅水域とは，安全な離隔距離を確保しなければならない	衝突・座礁	安全な離隔距離は状況に応じて可変
SC2	堪航性（復原性，安定性の担保）は，いかなる場合でも担保されなければならない	機器破損・荷物破損・転覆・浸水	アクチュエーターの損耗及び損傷・船体の完全性喪失・船内外の環境との適合失敗・Racing（空転）・Slamming（船底衝撃）・許容を超える船体動揺・許容を超える船体応力の蓄積
SC3	運航ミッションを達成しなければならない	大幅な遅延，目的地未達，運航維持する体制喪失	航海意図・制約が不明確で計画達成できない システムが法令を遵守できない

Step 2: Model the Control Structure 【前述】

- 物理アーキテクチャ（機器構成やネットワーク）は仮定せず，機能モジュールを用いて表現（汎用性を持たせる）
- Fleet Operation Centerを想定し，船陸に機能配分
 - Navigation PlanningおよびChief Engineerタスクを陸側に配置
- UnberthingからBerthingまでの一連の航海を対象
- 必要に応じ詳細化予定（特にDTC周り）



Control Structure of the target system

Step 2: Model the Control Structure

- コントロールストラクチャに限らず，時系列的な挙動（航海モードやステータスの違い，処理の関係性や分岐の仕方等）を表現したモデルを構築，分析に活用（高附2022）

シーケンス図

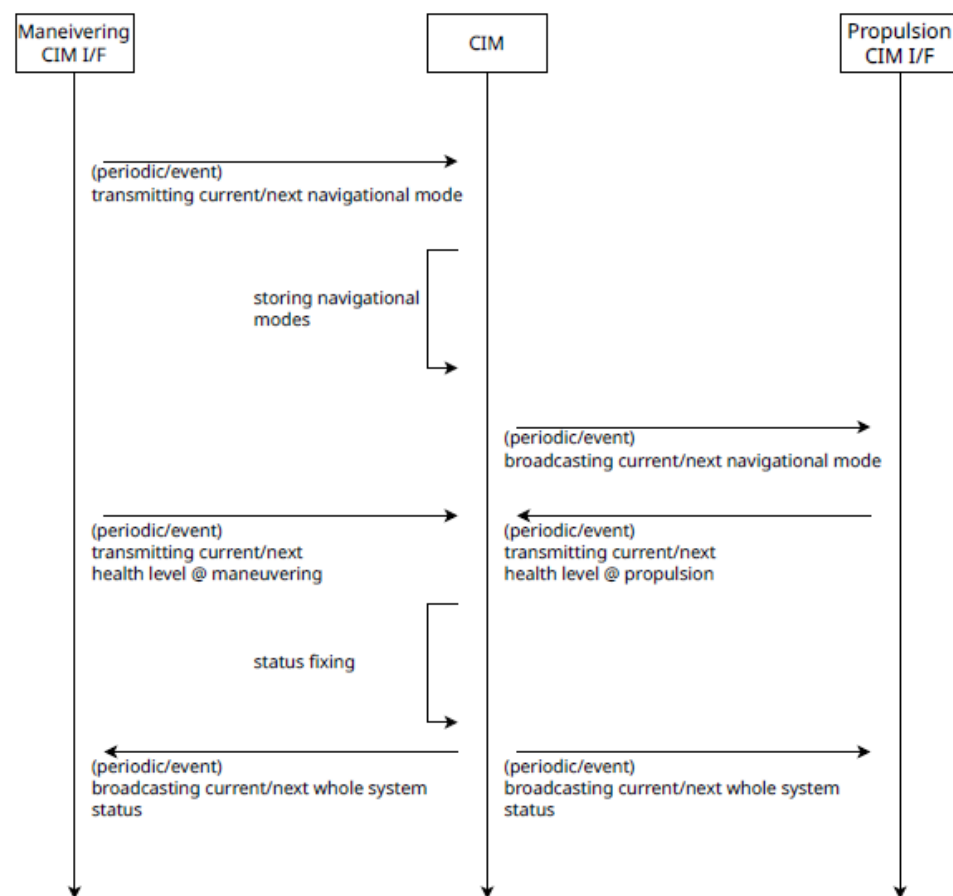


Figure 3.21. Sequence at navigational mode and status exchanging

SOED/SERPPの挙動を示すFFBD

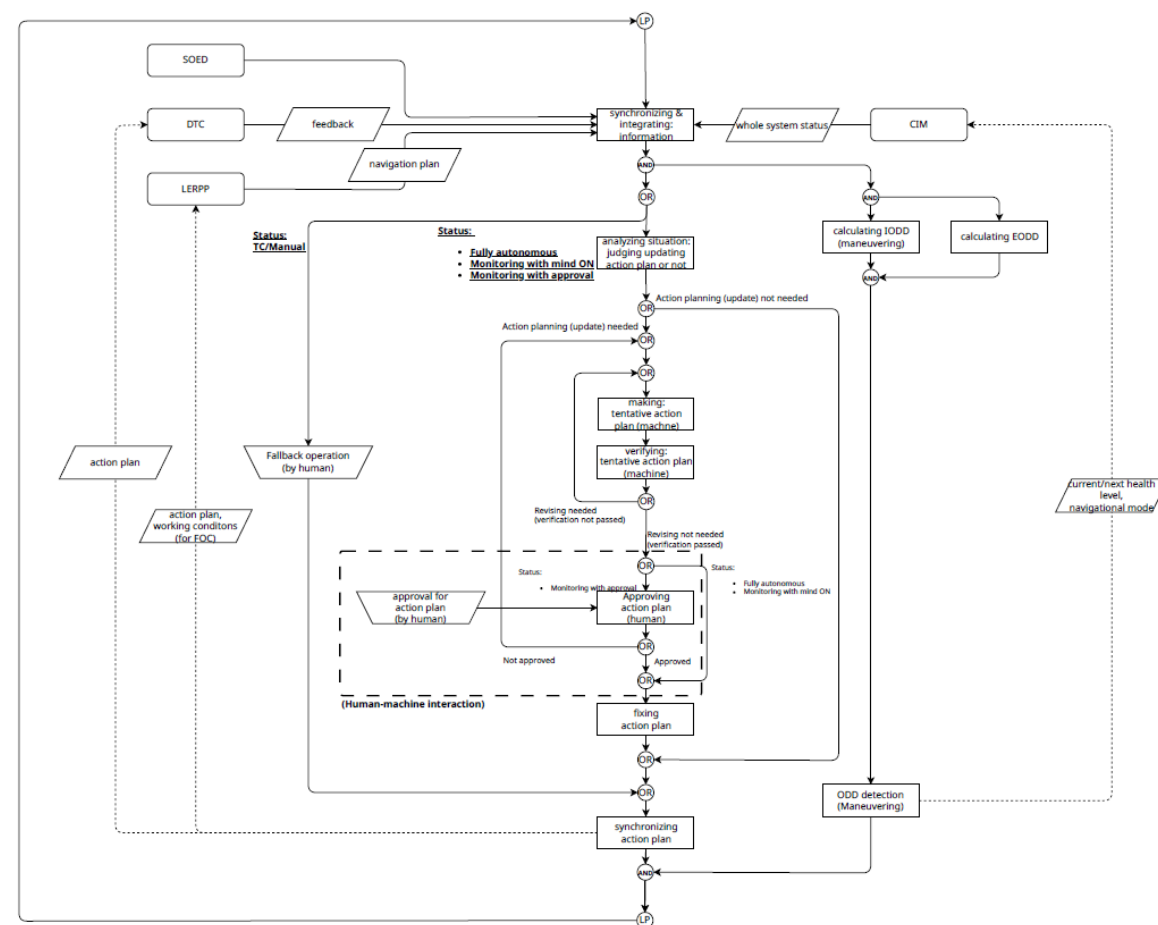
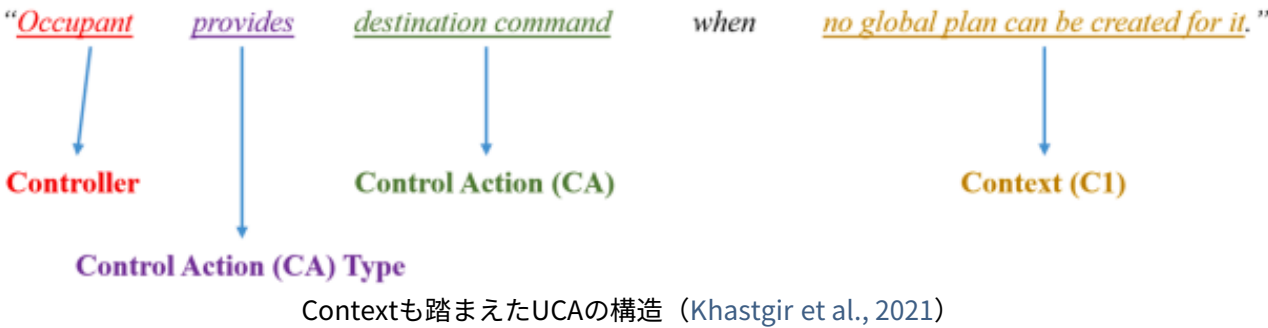


Figure 3.15. Behavior: function flow block diagram of SOED & SERPP

Step 3: Identify Unsafe Control Actions

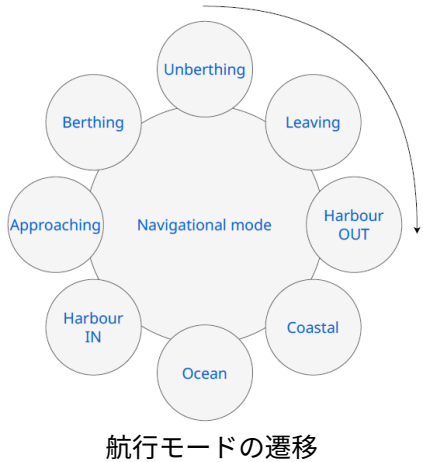
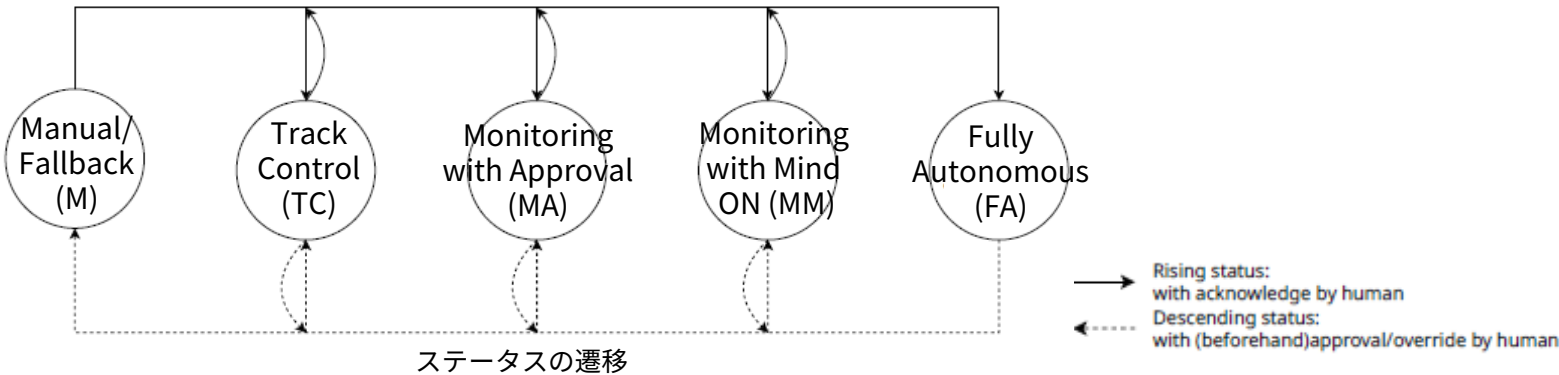
- それぞれのCAに対し，ガイドワード(N/P/T/D)を用いて安全制約に抵触しうる状況を想定
 - Contextを具体化することで，UCAが発生しうる客観的な状況を付記（検証シナリオにも活用）



- Contextは以下の要素の組み合わせで表現
 - ユースケース（航行モード，およびその遷移）
 - ステータス（自律化レベル，およびその遷移）
 - 荒天，他船の位置等，ODDメトリクスを踏まえた設定

自動運航船で考えられるODD評価軸（抜粋）【前述】

Category	Subcategory
Scenary	Geography
	Offshore Structure
	Navigational Area
	Temporal Area Specifics
Dynamic Elements	Other ships (and type)
	Obstacles
	Own ship
	Support of Own ship
Environmental Condition	Weather and Illumination (Impact on Sensing)
	Weather (Impact on Actuation)
	Connectivity



Step 4: Identify Loss Scenarios

- プロセスモデル(*)の齟齬に起因するリスクを抽出
- UCA (with Context) ごとに以下について段階的に整理し，シナリオを構築 (Khastgir et al., 2021)
 - プロセスモデル (Process Model)
 - コントローラが認識するコントロール対象の状態
 - 入力に対する信用／出力に対する期待／プロセスの情報解釈 の視点から抽出 (後述)
 - 齟齬の理由 (Belief Cause)
 - Process Model Beliefの理由
 - 具体のインプットや情報解釈を踏まえて，機能モジュールレベルまで理由を具体化する
 - 原因 (Causal Factor)
 - Belief Causeの根本要因，粒度は様々．HAZID等を踏まえた機能ブロック別の整理表を参照
 - 機能モジュールの故障・不具合検知ミス／性能限界／設計の誤り（前提条件の不一致等）の視点から抽出

(*) プロセスモデル (Process ModelもしくはProcess Model Belief)：

コントローラが認識するコントロール対象の状態．STAMPでは，創発的な事故が起きる主な原因は，不正確なプロセスモデル（プロセスモデルとシステムの実際の状態の不整合）にあるとしており，原因を特定する上でプロセスモデルの導出を重視している．

Step 4: Identify Loss Scenarios - 各モジュールのタスクの詳細化

- Control Structureのほかに、シーケンス図等を参照（Step 2: Model the Control Structure）
- コンセプト設計の情報を踏まえ、機能ブロックの機能の詳細、およびそこに用いるインプット，アウトプット，判断時の解釈（前提・想定）を明らかにし，Process Model, Belief Causeの抽出を容易にする

Process Model抽出のための各Control ActionのInput/Outputと内部アルゴリズムおよびAssumptionの例

Controller	CA	Control Action (to XXX)	Other Output	Input (from XXX)	Input (from XXX) (as other CA)	Function (用いるinput)	Assumption (Process Modelの特定に重要)
Action Planner	CA3	Action Plan (長期航海計画)[CA3.1] (to Controller) 承認依頼 (to Navigation Officer) ※必要に応じて MRMのための計画 (to Controller) ※必要に応じて	o1 Maneuvering健全性 (to CIM) o2 ウェイポイント (群) (to Navigation Planner) o3 到達時間 (速力) (to Navigation Planner)	i1 自船の位置・姿勢に関する情報 (from Sensor (Own)) i2 短期間・周囲の他船の情報 (from Sensor) i3 短期間・周囲の環境情報 (from Sensor) i5 海図情報・NGA (from Navigation Planner)	i4 航海計画 (from Navigation Planner) [CA] i6 行動計画 (from Navigation Officer) [CA] i7 ステータス (from CIM) [CA]	F1 CIMからのステータス情報を踏まえ，立案すべきか判断する F2.1 FA/MMステータス場合，周囲の状況を踏まえ，安全な行動計画を立案し，Controllerに伝える (A1, 1-5) [CA] F2.2 MAステータスの場合，周囲の状況を踏まえ，安全な行動計画を立案し，Navigation Officerへの承認依頼 (A1)を送付したのち，承認をもってControllerに伝える (A1, 1-5) [CA] F2.3 TCステータスの場合，Navigation Officerからの入力情報をそのままDTCに伝える F2.4 Mステータスの場合，DTCへの信号送信を停止する F2.5 MA/TCステータスの場合Navigation Officerからの承認・入力がない場合は，直ちにMRMを実行する(A3, 1-7) [CA]※実装しない F3 Shore Operatorが意思決定を行うために，i1-i4を統合し，常時表示する	a1 Controller/Actuator/Hull Modelの性能は限定された情報（場合によってはstatic）で判断する．また，不具合の有無はステータス情報で判断する a2 他船が等速直線運動をすると仮定して状況判断する a1' 入力されたインプット（Staticな情報）をもとに判断

アウトプットは何か？
(うちコントロールアクションは？)

インプットは何か？
(うちコントロールアクションは？)

内部のアルゴリズムにてどのように
インプット情報を用いているか？

アルゴリズム処理内で
前提・想定があるか？

【参考】FRAM (Functional Resonance Analysis Method) との親和性

- レジリエンス・エンジニアリングにおける安全解析手法 (Hollnagel 2013)
 - 機能共鳴：複数の機能が相互にインタラクションした結果、外乱に柔軟に対応する一方で、逆にエスカレーションなどを起こし、安全を脅かすこと。「成功」からも「危険」は生じる
 - 失敗と成功の同義性．帰納法的，統合 ↔ 演繹法的，分解（FMEA）
- 複数の機能のインタラクションを明らかにし，その関係性の中に安全にかかわるシステムの特徴を見出す
＝プロセスモデルの齟齬を抽出するガイドとしても活用可能

どの情報を前提としているのか？
制御のための情報は何か？等
情報の使われ方も含めてシステムの
挙動を明確化している点が類似
（今後関係性を詳細化：特に”資源”
となる機関や通信等も絡める）

表 1 機能の6要素

I: 入力	機能の動作トリガー
P: 前提	機能が動作開始するための事前条件
C: 制御	機能の挙動方法を操作する事後条件
R: 資源	機能の動作に必要な資源（事後条件）
T: 時間	機能実行可能時間（事後条件）
O: 出力	機能の出力

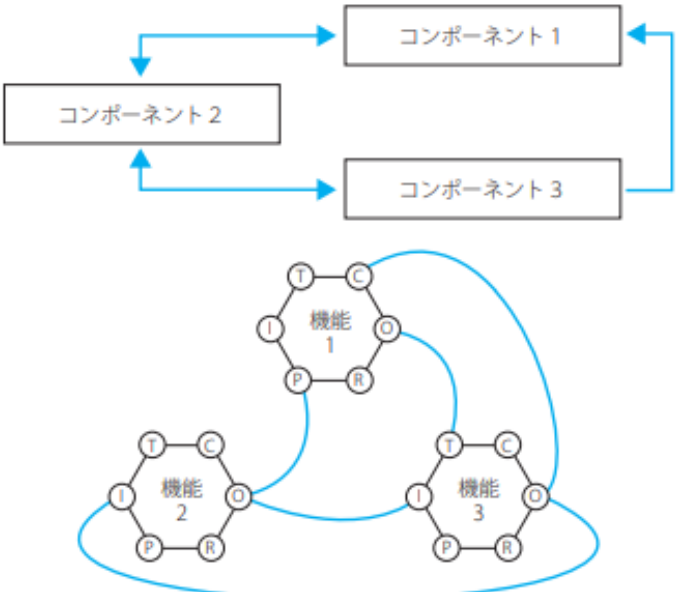


図 1 STAMP モデルと FRAM モデル

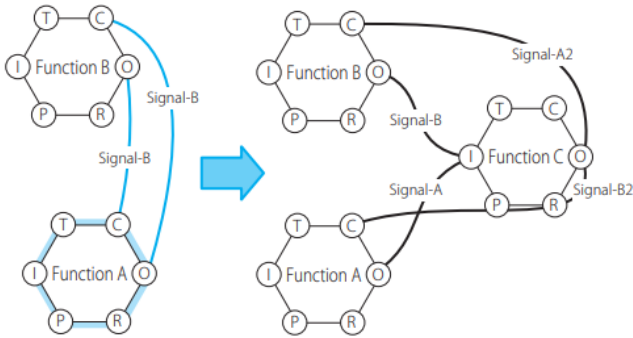


図 3.2.2-3 制御同士の競合を防止するための中間バッファの追加

- Tempo: インタラクションの速度の変化
- Escalation: インタラクションの強度の増大
- Dilemmas: インタラクションの強度の減少
- Coupling: 複数のインタラクション間の依存
- Reframing: インタラクション構造の再構築

Step 4: Identify Loss Scenarios - ロスシナリオの具体例

ロスシナリオの具体例

UCA_ID	UCA	SC_ID	Context	From	To	Process Model	PMB_ID	Belief Cause	GW_ID	機能ブロック	ISC	LS_ID
UCA3-P-1	SERPP (machine)より他船・陸と近づくAction PlanがDTCに伝わり、そのまま他船・陸との距離近接に至る[SC1]	SC1	他船や陸が自船周囲にいる状況，航行中（全航海モード），ステータス"FA/MM"	SERPP (machine)	DTC	自船周囲の他船・陸を認識していない／実際と異なる位置で認識している	1	情報が現実と異なるにもかかわらず，確度の高い他船情報が得られていると認識している	i2	Sensor（他船）Integrator	SC2	LS1
UCA3-P-1	SERPP (machine)より他船・陸と近づくAction PlanがDTCに伝わり，そのまま他船・陸との距離近接に至る[SC1]	SC1	他船や陸が自船周囲にいる状況，航行中（全航海モード），ステータス"FA/MM"	SERPP (machine)	DTC	自船周囲の他船・陸を認識していない／実際と異なる位置で認識している	1	情報が現実と異なるにもかかわらず，確度の高い自船（船位・速力）情報が得られていると認識している	i1	Sensor（自船）Integrator	SC1	LS2
UCA3-P-1	SERPP (machine)より他船・陸と近づくAction PlanがDTCに伝わり，そのまま他船・陸との距離近接に至る[SC1]	SC1	他船や陸が自船周囲にいる状況，航行中（全航海モード），ステータス"FA/MM"	SERPP (machine)	DTC	自船周囲の他船・陸を認識していない／実際と異なる位置で認識している	1	情報が現実と異なるにもかかわらず，確度の高い地理情報（NGA）が得られていると認識している	i5	Sensor（地理）Integrator	SC7	LS3
UCA3-P-1	SERPP (machine)より他船・陸と近づくAction PlanがDTCに伝わり，そのまま他船・陸との距離近接に至る[SC1]	SC1	他船や陸が自船周囲にいる状況	SERPP (machine)	DTC	自船周囲の他船・陸を認識していない／実際と異なる位置で認識している	1	最新の情報を取得していると認識している（センサ情報が揃っていない→通信の遅れ，等）	com	Communication	通信(SC8?) SC1/2/3/7	LS4
UCA3-P-1	SERPP (machine)より他船・陸と近づくAction PlanがDTCに伝わり，そのまま他船・陸との距離近接に至る[SC1]	SC1	他船や陸が自船周囲にいる状況，航行中（全航海モード），航海途中で一旦自動運航システムをOFFとし，再起動した状況，ステータス"FA/MM"	SERPP (machine)	DTC	自船周囲の他船・陸を認識していない／実際と異なる位置で認識している	1	最新の情報を取得していると認識している（過去の情報が残っている状態で計画策定を行う）	com	Integrator	SC1/2/3/7	LS5
UCA3-P-1	SERPP (machine)より他船・陸と近づくAction PlanがDTCに伝わり，そのまま他船・陸との距離近接に至る[SC1]	SC1	他船や陸が自船周囲にいる状況，航行中（全航海モード），ステータス"FA/MM"	SERPP (machine)	DTC	自船周囲の他船・陸を認識していない／実際と異なる位置で認識している	1	情報が現実と異なるにもかかわらず，海図情報が正しく得られていると認識している	i5	Sensor（地理）Integrator	SC7	LS6
UCA3-P-1	SERPP (machine)より他船・陸と近づくAction PlanがDTCに伝わり，そのまま他船・陸との距離近接に至る[SC1]	SC1	他船や陸が自船周囲にいる状況，航行中（全航海モード），ステータス"FA/MM"	SERPP (machine)	DTC	自船の制御装置は計画を正しく追従できると認識している	1/2	（制御装置の性能を自然環境情報をベースに見積もっており）確度の高い自然環境情報が得られていると認識している	i3/To	Sensor（自然環境）Integrator	SC3	LS7
UCA3-P-2	SERPP (machine)より制御できないAction Planが伝わり，人のバックアップ操船も間に合わず，操縦不能→転覆・船体ダメージに至る[SC2]	SC2	航行中（全航海モード），ステータス"FA/MM" ※人のバックアップが入った場合の分析必要	SERPP (machine)	DTC	自船の制御装置は計画を正しく追従できると認識している	2	（制御装置の性能をステータスを基に判断しており）確度の高い制御性能の情報が得られていると認識している	To/a1	SERPP (machine)	SC5/6	LS14

Contextは

- ・ 航行モード
- ・ ステータス
- ・ その他（荒天，他船の位置等）

をベースに記載

Process Modelの齟齬は

- 1入力に対する信用
- 2出力に対する期待
- 3プロセスの情報解釈（及びその仮定）

の視点から抽出

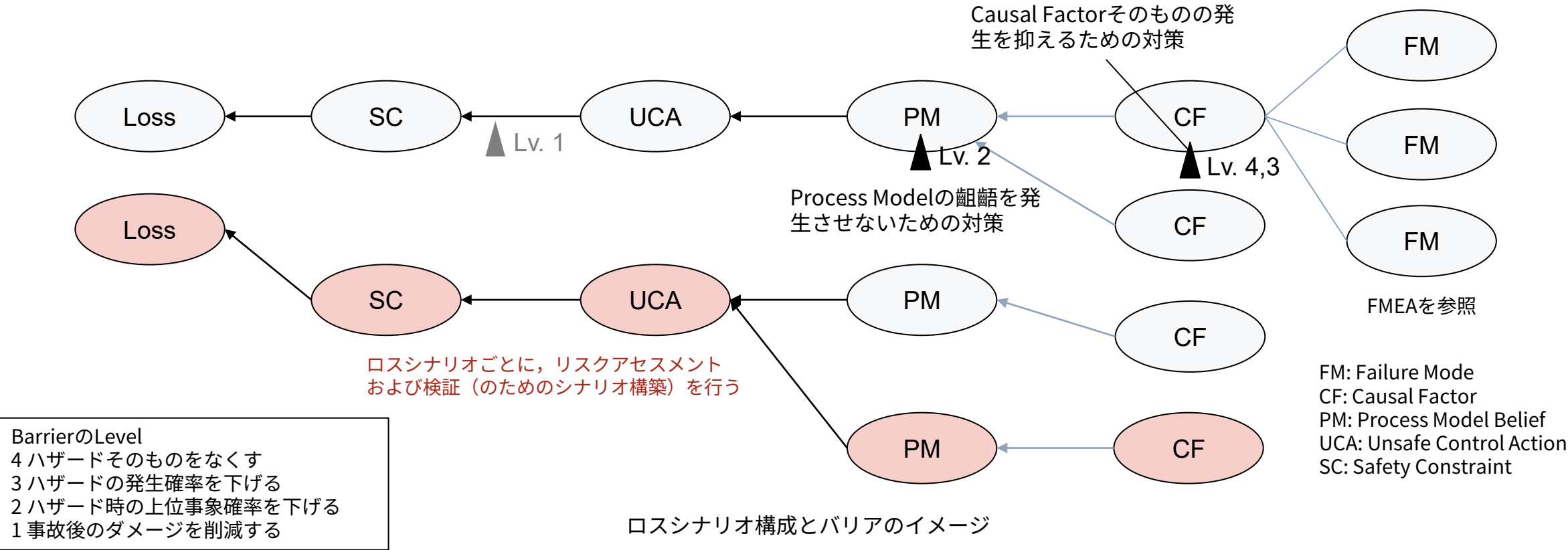
Process Modelの齟齬の理由は

具体的なインプット(i)や処理における仮定（a）等

を踏まえて機能ブロックレベルまで具体化

HCF, バリア種類別整理, リスク評価, テストシナリオ作成

- ロスシナリオをベースに, UCA間の関係性やバリアの位置づけを明確化, 安全要件に追加
 - Causal Factorの発生を抑える対策, 発生してもProcess Modelの齟齬を生まないための対策, 等
- ロスシナリオごとに, Severity/Frequencyを評価
 - 対策の十分性を評価するとともに, 検証のためのシナリオの優先順位付けに活用



目次

1. 背景

- 海運における課題
- MEGURI2040プロジェクトにおける自動運航船開発と実証
- 自動運航船に対するコンセプト開発と安全性

2. モデルを活用したコンセプト設計とSTAMP/STPAの導入

3. STAMP/STPAの実践

- 自動運航船システムへのSTPA適用事例（先行研究）
- STPA実施のポイント
- 分析の流れ

4. STAMP/STPA結果の検証・妥当性評価シナリオとしての活用

- 記述モデルと数値モデルを組み合わせたシナリオベース検証フレームワークの提案

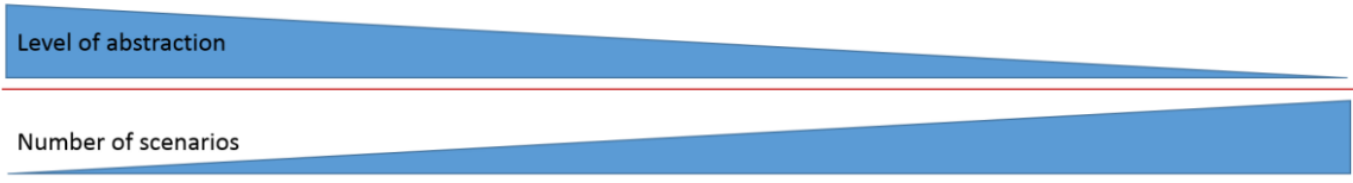
5. まとめ

記述モデルと数値モデルを組み合わせたシナリオベース検証フレームワークの提案

- 自動車業界で採用されている3段階の抽象度のシナリオ記述を採用 (Menzel et al., 2018)
 - ① STPA を通じた **Functional Scenario** の抽出
 - ② 運用設計領域 (Operational Design Domain: ODD) を踏まえた **Logical Scenario** の定義
 - ③ ガウス過程回帰とサンプリングを通じた **Concrete Scenario** の試行

段階的なシナリオ記述

Functional scenarios	Logical scenarios	Concrete scenarios
<u>Base road network:</u> three-lane motorway in a curve, 100 km/h speed limit indicated by traffic signs	<u>Base road network:</u> Lane width [2.3..3.5] m Curve radius [0.6..0.9] km Position traffic sign [0..200] m	<u>Base road network:</u> Lane width [3.2] m Curve radius [0.7] km Position traffic sign [150] m
<u>Stationary objects:</u> -	<u>Stationary objects:</u> -	<u>Stationary objects:</u> -
<u>Moveable objects:</u> Ego vehicle, traffic jam; Interaction: Ego in maneuver „approaching“ on the middle lane, traffic jam moves slowly	<u>Moveable objects:</u> End of traffic jam [10..200] m Traffic jam speed [0..30] km/h Ego distance [50..300] m Ego speed [80..130] km/h	<u>Moveable objects:</u> End of traffic jam 40 m Traffic jam speed 30 km/h Ego distance 200 m Ego speed 100 km/h
<u>Environment:</u> Summer, rain	<u>Environment:</u> Temperature [10..40] °C Droplet size [20..100] μm	<u>Environment:</u> Temperature 20 °C Droplet size 30 μm

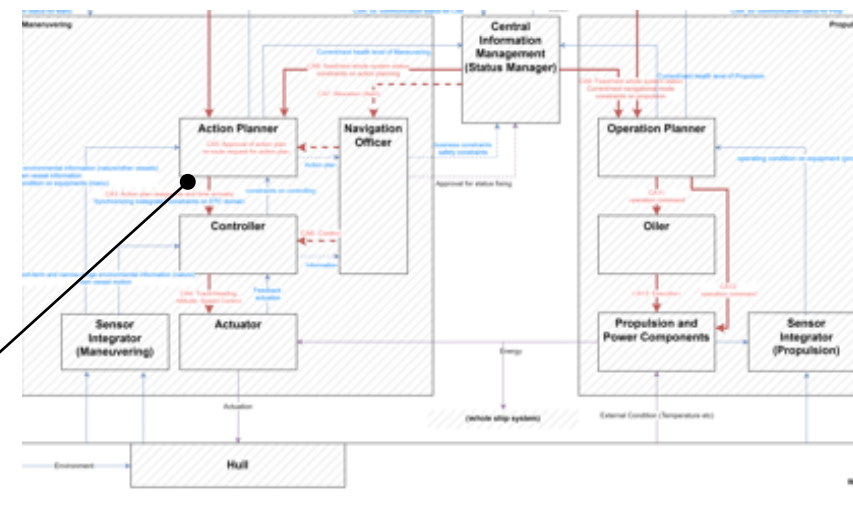


①STPAを通じたFunctional Scenario抽出【前述】

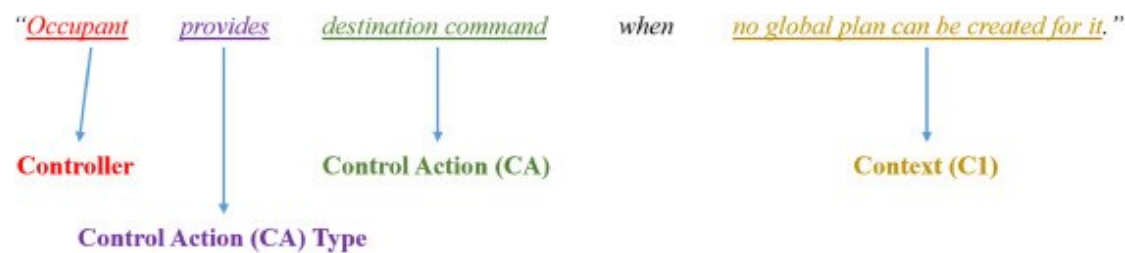
- STPAにおいて危険なコントロールアクション (UCA) を抽出する際に生じるコンテキストを詳細に記述
- プロセスモデル（コントローラが把握するシステムの状態）の現実との乖離を踏まえて要因を記載することで，Functional Scenarioを抽出

危険なコントロールアクション (UCA3-NT-1)

大洋航海を自律ステータスFAで航行中，周囲に他船がいるときに，**Action Planner**からの**行動計画**が**提供されない・遅れて提供される**
[SC1. 他船や周辺JSX障害物との離隔距離保持]



- Action Plannerのプロセスモデル：他船が周辺にいないと想定している
- 理由：他船の認知ができていない（入力への信頼）
- 原因：Sensor/Integratorの故障，経験劣化，性能限界



Khastgir et al, 2021

ロスシナリオ (as Functional Scenario) (LS-UCA3-NT-1-B1C2)

大洋航海を自律ステータスFAで航行中，周囲に他船がいるときに，**他船認知Sensor/Integratorの故障・不具合**で**Action Planner**は他船が周辺にいないと想定する状況が**続き**，**Action Planner**からの**行動計画**が**提供されず・遅れて提供され**，他船との距離近接，さらに衝突・座礁に至る

②ODD を踏まえたLogical Scenario定義

- Functional Scenarioを参考にしつつ，テスト環境（避航操船シミュレータ）に合わせたシナリオを抽出
 - 自動運航船のODD構成要素を定義し，その中からLogical Scenario記述のための入力指標を抽出

Functional Scenarioの例 (LS-UCA3-NT-1-B1C2)

大洋航海を自律ステータスFAで航行中，周囲に他船がいるときに，他船認知Sensor/Integratorの故障・不具合でAction Plannerは他船が周辺にいないと想定する状況が続き，Action Plannerからの行動計画が提供されず・遅れて提供され，他船との距離近接，さらに衝突・座礁に至る

自船周囲で衝突可能性のある船を突然認識する状況を想定，十分な離隔距離を確保して避航できることを検証

Logical Scenario記述の例

シナリオ入力変数

Dynamic Elements of (each) ship: Other ship(s)

- v_{target} 他船速力: [0..12] knot
- θ_{target} 他船検出位置: [60..300] degree (衝突点からの角度)

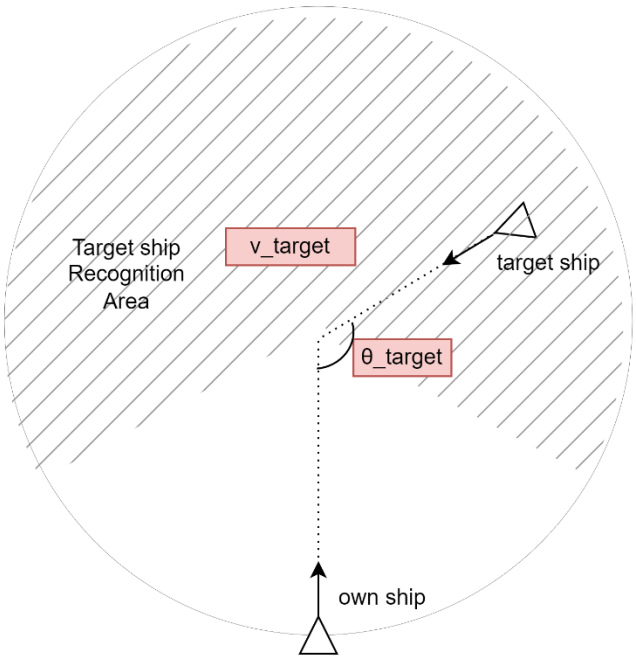
評価関数

Robustness 避航動作における最小離隔距離

前提条件

- 登場する他船は1隻を想定，NGAは想定しない（大洋航海中を想定）
- 1NM先の衝突点に近づくことを想定（1NM以内の検知率は十分に高いと想定）
- 他船は避航しないことを想定

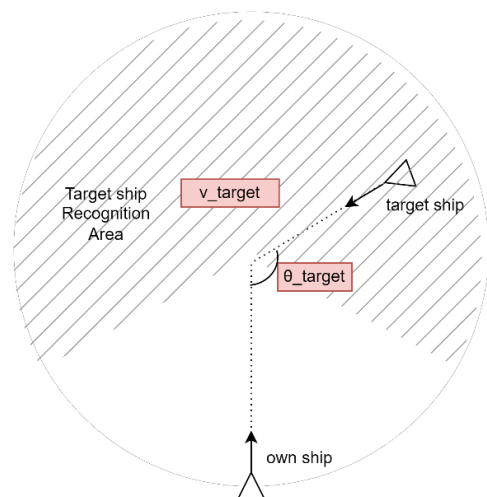
シナリオの概要



③ ガウス過程回帰とサンプリングを通じたConcrete Scenarioの試行

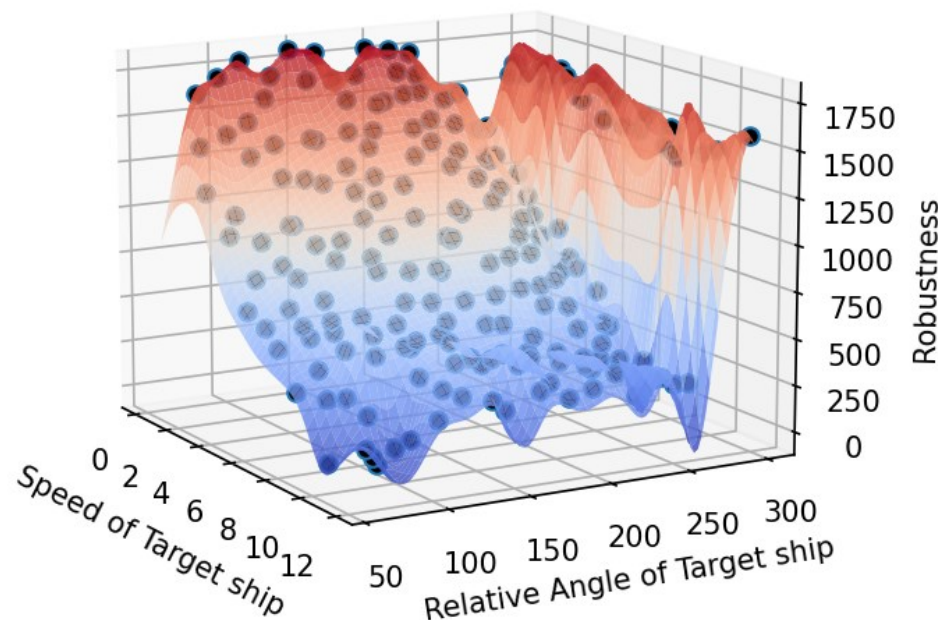
- Logical Scenarioで定義した連続空間から，Sobol' 列を用いてサンプルを抽出（準モンテカルロ法）
 - ガウス過程回帰 (GPR) で得られた関数の 99% ($\pm 2.58 \sigma$) 信頼区間で安全性を確認
 - 留意すべき状況に対してはODD外とし，適切なフォールバック（人間による監視・オーバーライド等）

Logical Scenario空間

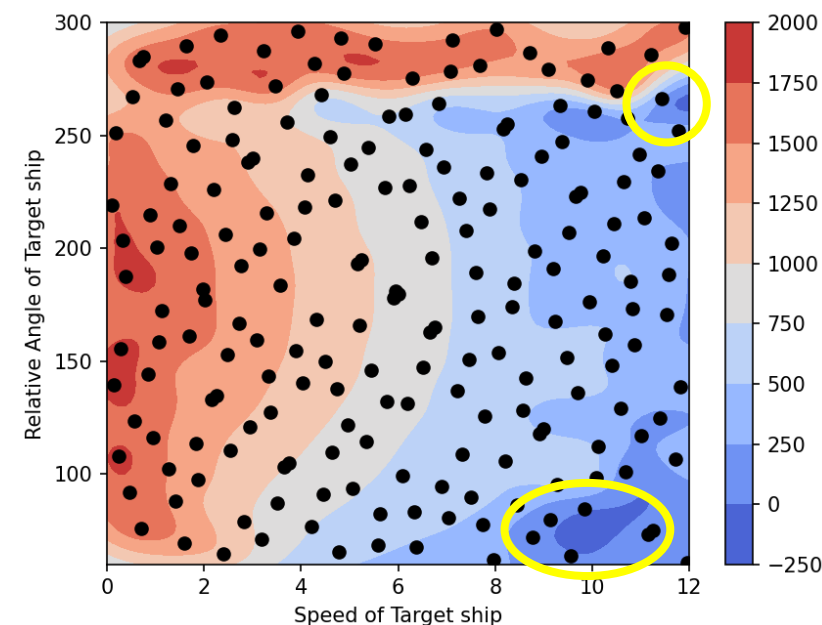


v_{target} 他船速力: [0..12] knot
 θ_{target} 他船検出位置: [60..300] degree

シミュレーション結果
(黒：シミュレーション結果，色・面：回帰関数の平均)



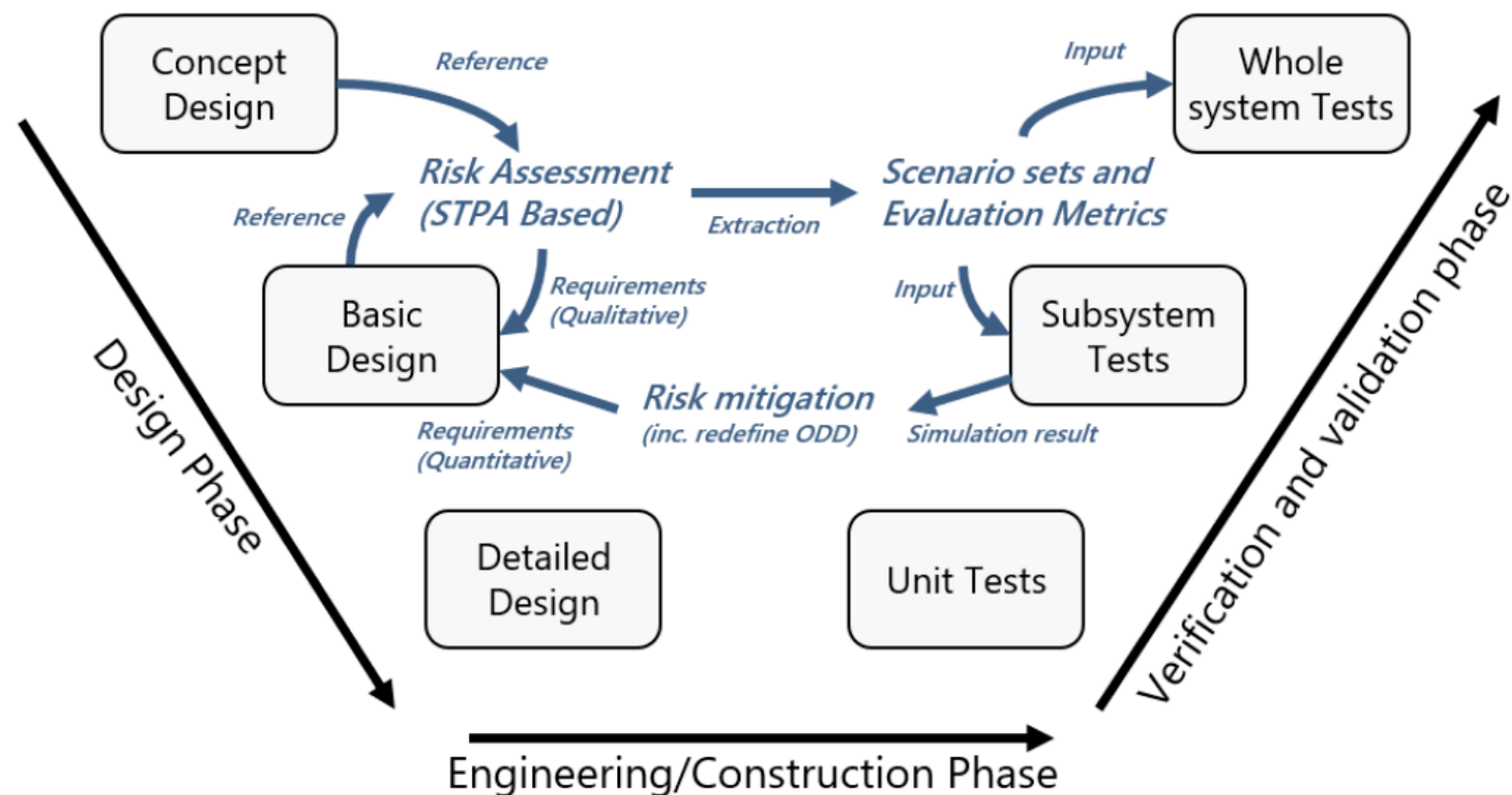
シミュレーション結果
(Robustness Scoreの0.5 パーセンタイル下側信頼区間の値)



Robustness 最小離隔距離 [m]

記述モデルと数値モデルを組み合わせたシナリオベース検証フレームワークの提案

- 概念モデルを用いたリスク解析（STPA）では、リスクの定量化が困難 (Zhang, 2022)
 - 数値モデルによるシミュレーションを実施する場合、シナリオの絞り込みが困難 (Karla and Paddock, 2016)
- リスクアセスメントからのシナリオ抽出+数値シミュレーションベース検証フレームワークを提案



Vモデルにおける本フレームワークの位置づけ

目次

1. 背景

- 海運における課題
- MEGURI2040プロジェクトにおける自動運航船開発と実証
- 自動運航船に対するコンセプト開発と安全性

2. モデルを活用したコンセプト設計とSTAMP/STPAの導入

3. STAMP/STPAの実践

- 自動運航船システムへのSTPA適用事例（先行研究）
- STPA実施のポイント
- 分析の流れ

4. STAMP/STPA結果の検証・妥当性評価シナリオとしての活用

- 記述モデルと数値モデルを組み合わせたシナリオベース検証フレームワークの提案

5. まとめ

まとめ

- 自動運航システムの社会実装に向け，その安全性の担保は大きな課題
- 人と機械を含む構成要素の相互作用に由来するハザード抽出およびリスクの定量評価等を通じ，既存の船と同等以上の安全性の論証が必要
- 自動運航システムのコンセプト設計段階にSTPAを適用し，汎用性を持たせたシステムモデル群と，プロセスモデルの齟齬も含めた発生要因に関するガイドワードを用いて，ロスシナリオを効果的に抽出する手法を紹介
- 抽出されたシナリオを基に，段階的にテストシナリオを具体化する手法を示し，STPAを設計のみならず検証・妥当性確認にまで活用する一連の流れを提示
- [【参考】 DFFASドキュメンタリー映像](#)

