2016　STAMP Workshop in Japan

ソフトウェアIV&VとSTAMP

2016年12月5日

有人宇宙システム株式会社

安全開発保証部

星野　伸行

自己紹介

- 2000年より、有人宇宙システム株式会社（JAMSS）安全開発保証部ソフトウェアグループにて、宇宙航空研究開発機構（JAXA）殿が開発する宇宙機搭載ソフトウェアに対して、**品質保証（安全性、信頼性）**及び、**独立検証と有効性確認（IV&V）**業務に従事
- IV&Vの手法として、当初よりMITのNancy Leveson教授の提唱する**Intent Specification**（意図された根拠のある仕様）の考え方を踏まえ、上位要求特にシステム安全要求と、ソフトウェア仕様／設計との紐づけを重要視。**ソフトウェア仕様／設計をモデル解析**（SpecTRM状態遷移マトリクス）し、その振る舞いがシステム安全要求に適合していることを確認
- システム全体の安全要求から、個々のシステム及びソフトウェアが満たすべき具体的な安全要求／安全制約を抽出する方法として、**STAMP/STPA**を採用。大規模システムに対応したIV&V手法を確立

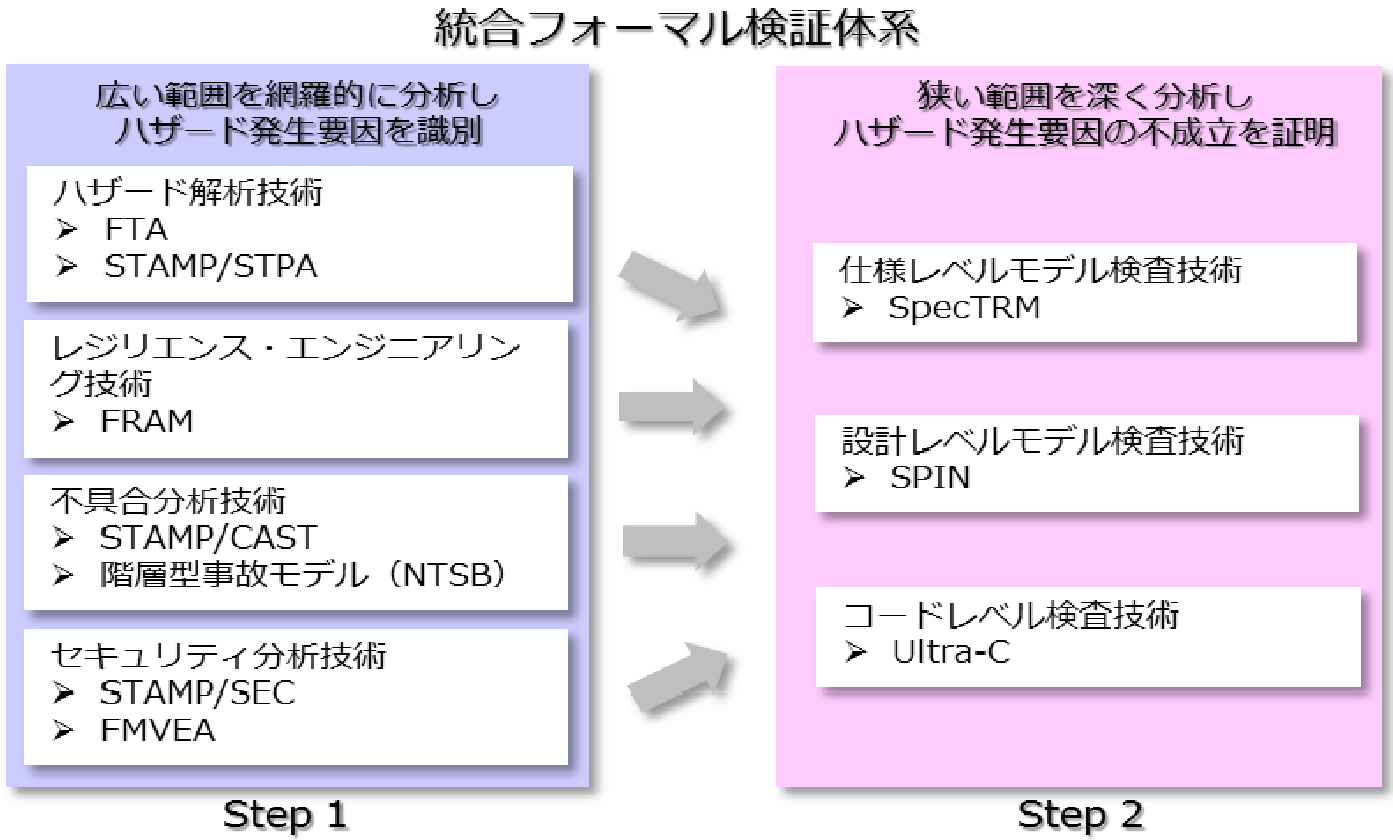
ソフトウエアIV&Vとは？

- JAMSSは、1996年、JAXA（航空宇宙研究開発機構）と共同で、我が国初のソフトウエアIV&Vを、宇宙ステーション計画に対して実施
- ソフトウエアIV&Vの目的は、当時増大しつつあった**ソフトウエアの要求・設計誤りに起因する事故**の撲滅
- ソフトウエアの**実装ミスではなく、要求・設計誤り**を見つけるために、様々な手法を開発

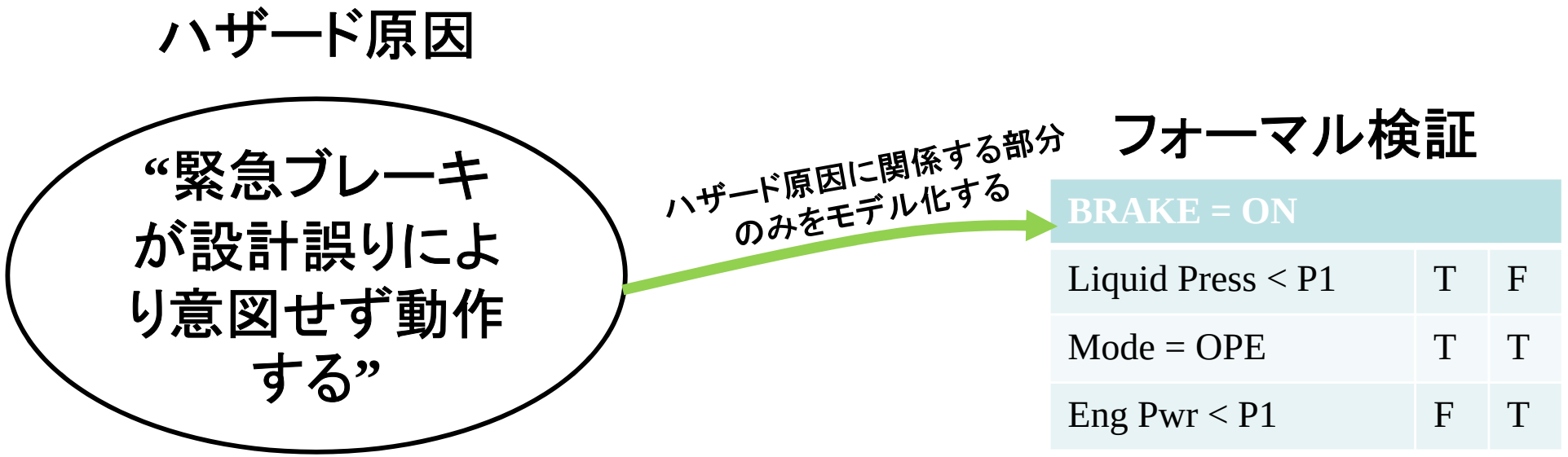
ARIANE 5 Flight 501 Failure Report by the Inquiry Board

統合フォーマル検証

- **検証対象を絞る技術**、フォーマルメソッドなどを基にした**フォーマル検証技術**を組み合わせ、大規模システムに適用



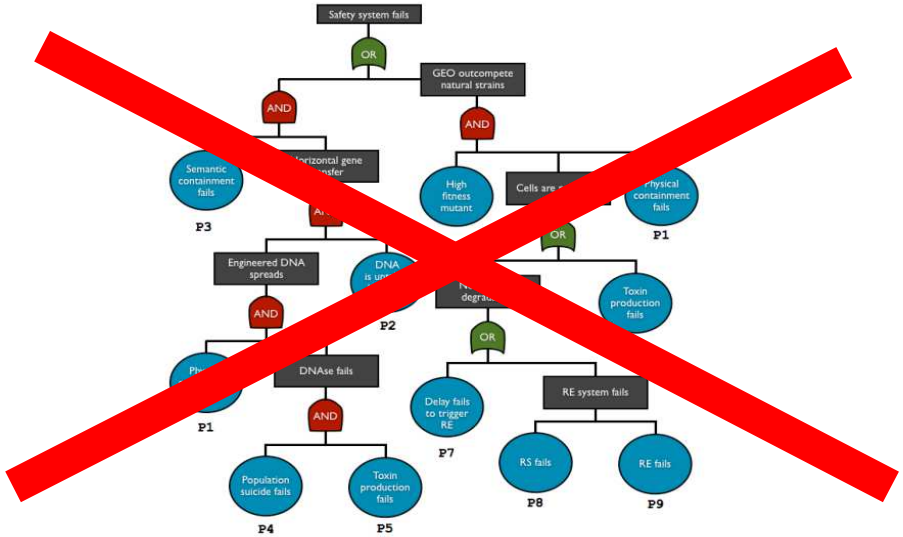
- **ハザード原因のみにフォーマル検証を適用**
  - ソフトウエアハザード解析を行い、そこで識別されたハザード原因に対してのみ、フォーマル検証を実施



BRAKE = ON		
Liquid Press < P1	T	F
Mode = OPE	T	T
Eng Pwr < P1	F	T

ソフトウエアハザード解析とは？

- ソフトウエアハザード解析は、通常のハザード解析と異なる
  - ソフトウエアは故障しない
  - ソフトウエアは劣化せず、いつも書かれた通りに動く
  - FTAのように、故障を分析する手法は合わない.



ソフトウエアハザード解析手法の研究

- 1999年以降、HTV（コウノトリ）の安全解析を開始。Nancy Leveson教授の考案したSpecTRM-RLモデリング言語を用いた分析を誘導制御ロジックに適用。フォーマルメソッドを大規模システムに適用した国内初の事例

- 2010年以降、STAMP/STPAの初期理論の改善を行いつつ、HTV, GPM等、JAXAの人工衛星のソフトウエア独立評価に適用。HTVは5号機まで全て成功中の世界で唯一の補給機として、宇宙ステーションへの最も安全なドッキング方式の基準となり、米国の補給機設計がこれに追従

従来の安全解析手法

FTA（Fault Tree Analysis）、FMEA（Failure Mode and Efect Analysis）

- システムの構成要素に着目
- 解析できる主なハザード（非安全）要因
  - 機器の故障
  - 人間の操作ミス

STAMP（Systems-Theoretic Accident Model and Process）／STPA（STAMP based Process Analysis）：システム理論に基づくアクシデントプロセスモデルによる安全解析

- システム構成要素間の相互作用に着目
- 解析できる主なハザード（非安全）要因
  - 制御（コントロール）の誤り
  - コミュニケーションの誤り

水槽の水位を一定に保つシステム

- 構成要素と役割
  1. 水槽本体（水位計、給水ポンプ、排水バルブを含む）
  2. 水位制御器（コンピュータ）
     - 水位計が上限値になったら、排水バルブを開ける
     - 水位計が下限値になったら、排水バルブを閉める
     - オペレータの指示により、給水ポンプを作動／停止させる
  3. オペレータ（人間）
     - 通常時、給水ポンプを作動させる
     - 水位計が上限値を大きく超えたら、給水ポンプを停止させる

従来の安全解析によるハザード要因

アクシデントの定義

水漏れ

ハザード（アクシデントが潜在している具体的な状態）の定義

水槽から水が溢れる

ハザード要因

- 給水ポンプの故障（開き放し）
- 排水バルブの故障（閉り放し）
- 水位計の故障（過小値出力）
- 制御器の故障
- 制御ソフトウェアのエラー
- オペレーションミス
- 停電、など

STAMP/STPAの手順

Step 0：（準備1）アクシデント、ハザード、安全制約の識別

Step 0：（準備2）コントロールストラクチャーの構築

Step 1：非安全なコントロールアクション（UCA）の抽出

Step 2：ハザード要因（HCF）の特定

Step 0:（準備1）アクシデント、ハザード、安全制約の識別

対象システムにおいて分析対象となる、アクシデント、ハザード（アクシデントが潜在している具体的な状態）を定義し、ハザードを制御するためのシステム上の安全制約を識別

- アクシデントの定義

  水漏れ

- ハザード（アクシデントが潜在している具体的な状態）の定義

  水槽から水が溢れる

- 安全制約の定義

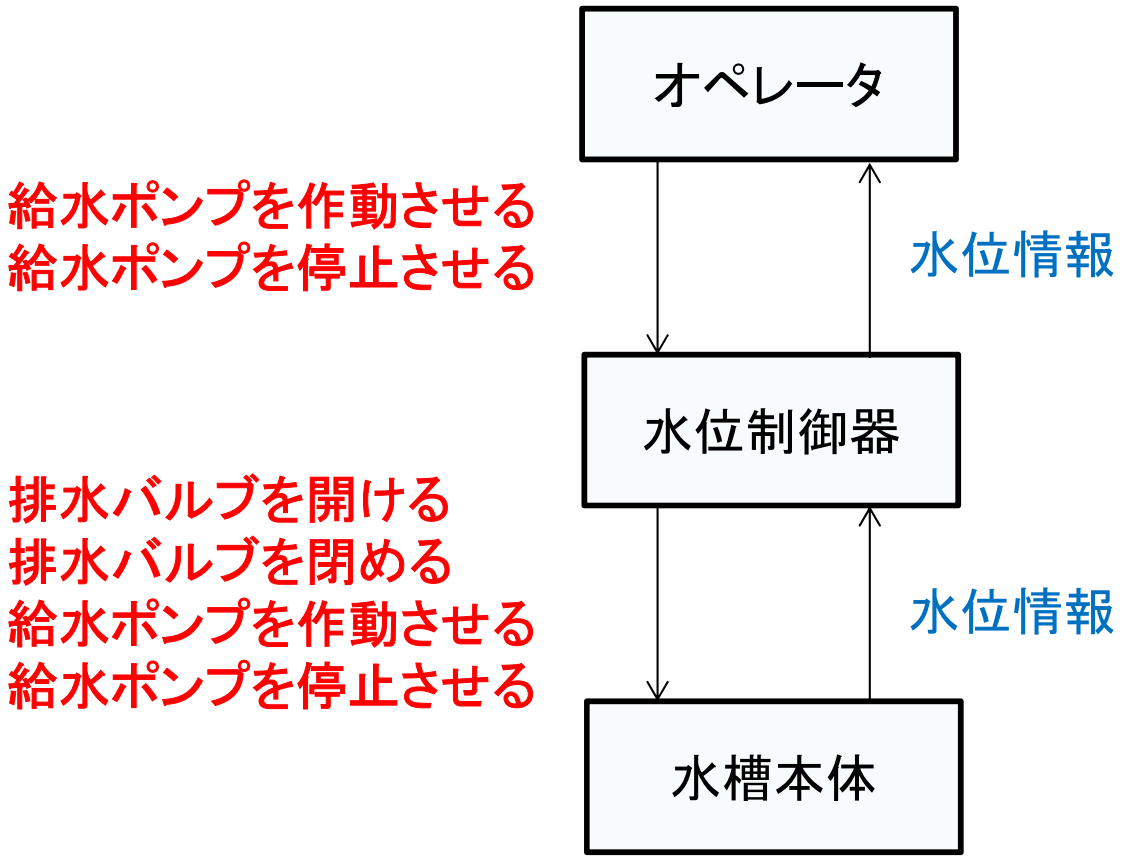
  水槽から水が溢れない

Step 0：（準備2）コントロールストラクチャーの構築

システムにおいて、安全制約の実現に関係するコンポーネント（サブシステム、機器、組織等）、及び、コンポーネント間の相互作用（コントロールアクション、フィードバックデータ）を分析し、制御構造図（コントロールストラクチャー）を構築

Step 0：（準備2）コントロールストラクチャーの構築

安全制約：水槽から水が溢れない



（凡例） 赤太字： コントロールアクション（安全制約の実行に必要な指示）
青細字： フィードバックデータ（必要な情報）

Step 1：非安全なコントロールアクション（UCA）の抽出

コントロールストラクチャーから、安全制約の実行に必要なコントローラーによる指示すなわち**コントロールアクション**を識別し、**4種類のガイドワード**を適用して、ハザードにつながる**非安全なコントロールアクション**（Unsafe Control Action：UCAという）を抽出

1. 与えられないとハザード
2. 与えられるとハザード
3. 早すぎ、遅すぎ、誤順序でハザード
4. 早すぎる停止、長すぎる適用でハザード

Step 1：非安全なコントロールアクション（UCA）の抽出

No.	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
1	給水ポンプを停止させる	水位計が上限値を大きく超えたときに、給水ポンプを停止しない →ハザード？	通常時に、給水ポンプを停止する →ハザード？	給水ポンプの停止が遅れる →ハザード？	給水ポンプの停止の指示は、長時間継続しないので、適用外
2	排水バルブを開ける	水位計が上限値を超えたときに、排水バルブを開けない →ハザード？	通常時に、排水バルブを開ける →ハザード？	排水バルブの開が遅れる →ハザード？	排水バルブの開が途中で停止する →ハザード？

Step 1：非安全なコントロールアクション（UCA）の抽出

No.	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
1	給水ポンプを停止させる	水位計が上限値を大きく超えたときに、給水ポンプを停止しないと、ハザードに至る。（UCA 1）	通常時に、給水ポンプを停止させても、水位は低下するが、ハザードには至らない。	給水ポンプの停止が遅れると、ハザードに至る。（UCA 2）	給水ポンプの停止の指示は、長時間継続しないので、適用外
2	排水バルブを開ける	水位計が上限値を超えたときに、排水バルブを開けないと、ハザードに至る。（UCA 3）	通常時に、排水バルブを開けても、水位は低下するが、ハザードには至らない。	排水バルブの開が遅れると、ハザードに至る。（UCA 4）	排水バルブの開が途中で停止すると（バルブが中途半端に開いた状態）、ハザードに至る。（UCA 5）

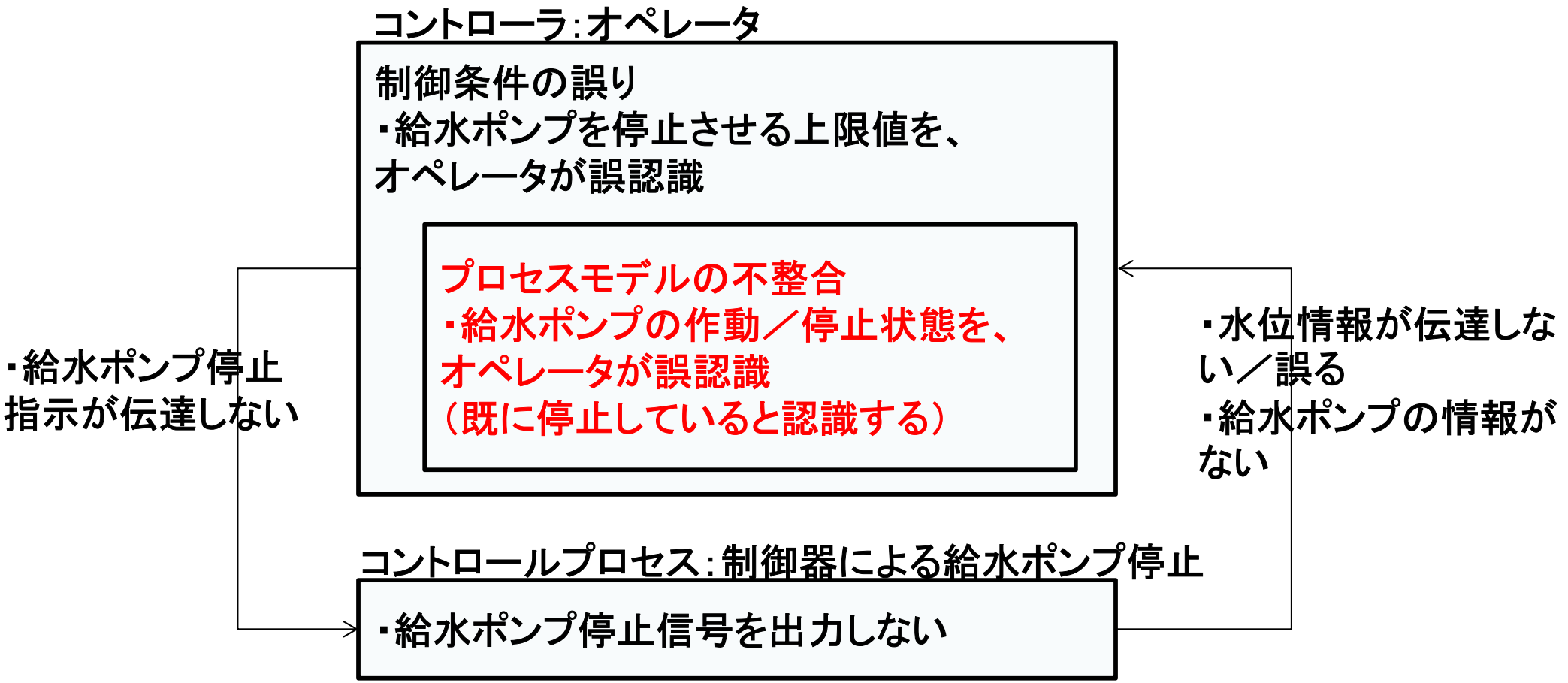
Step 2：ハザード要因（HCF）の特定

Step1で抽出した非安全なコントロールアクション毎に、関係するコントローラーと被コントロールプロセスを識別して、**コントロールループ図**を作成し、ガイドワードを適用して**ハザード要因**（Hazard Causal factor：HCFという）を特定

特に、ソフトウェアや人間に起因する要因として、コントローラーの想定する**プロセスモデルが、実際のプロセスの状態と矛盾することで起きる要因**を特定

Step 2：ハザード要因（HCF）の特定

解析例：
（UCA 1）　水位計が上限値を大きく超えたときに、給水ポンプを停止しないと、ハザードに至る。



Step 2：ハザード要因（HCF）の特定

STAMP/STPAによるハザード要因の特定例

- 給水ポンプを停止させる上限値を、オペレータが**誤認識**(UCA 1の要因)
- 給水ポンプの作動／停止状態を、オペレータが**誤認識**(UCA 1の要因)
- 水位情報のレスポンス遅れを、オペレータが**認識していない**（UCA 2、UCA 4の要因）
- 排水バルブの開／閉状態を、制御器が**誤認識**(UCA 3の要因)
- 排水バルブの半開状態があり得ることを、制御器が**認識していない**(UCA 5の要因)

比較：従来の安全解析によるハザード要因の特定例

- 給水ポンプ、排水バルブ、水位計、制御器の**故障**
- ソフトウェア**エラー**
- オペレーション**ミス**
- **停電**

Step 2：ハザード要因（HCF）の特定

STAMP/STPAで導かれるハザード要因の特徴

- 制御対象の**状態の誤認識**
- 制御**条件の誤認識**
  - 大規模複雑システムで多発する不具合要因
  - コンピュータだけでなく、人間、組織の要因分析にも適用可能

ハザード要因を制御／除去するために、システム／ソフトウェア設計で考慮すべき、**具体的な安全制約**を提供する（複数要素が関係するような制約。安全は創発されるもの - Leveson）

- **STAMP/STPA結果による安全制約の分析例**
  - 給水ポンプを停止させる上限値を、オペレータに**警報で通知**すること
  - 給水ポンプの作動／停止状態を、オペレータが**モニタ確認**できること
- 比較：**従来の安全解析結果による安全制約の分析例**
  - 給水ポンプは1故障を考えて**2重冗長**にすること
  - ソフトウェアの給水ポンプ停止機能が**正しく動作**すること

STAMP/STPAの恩恵

従来の安全解析手法の利点

- 機器や組織の単一故障によるハザード要因を、分岐条件を論理的に組むことで**網羅的に分析**できる
- システムの想定される異常を整理できる

STAMP/STPAの利点

- 機器や組織の相互作用によるハザード要因を、**システム全体の振る舞いを確認**しながら分析できる
- システムの目的が理解できる

各手法を**うまく組み合わせる**ことで、システム安全性解析の効果を上げることができる