Pre-Formalメソッドとしての STAMPモデリング

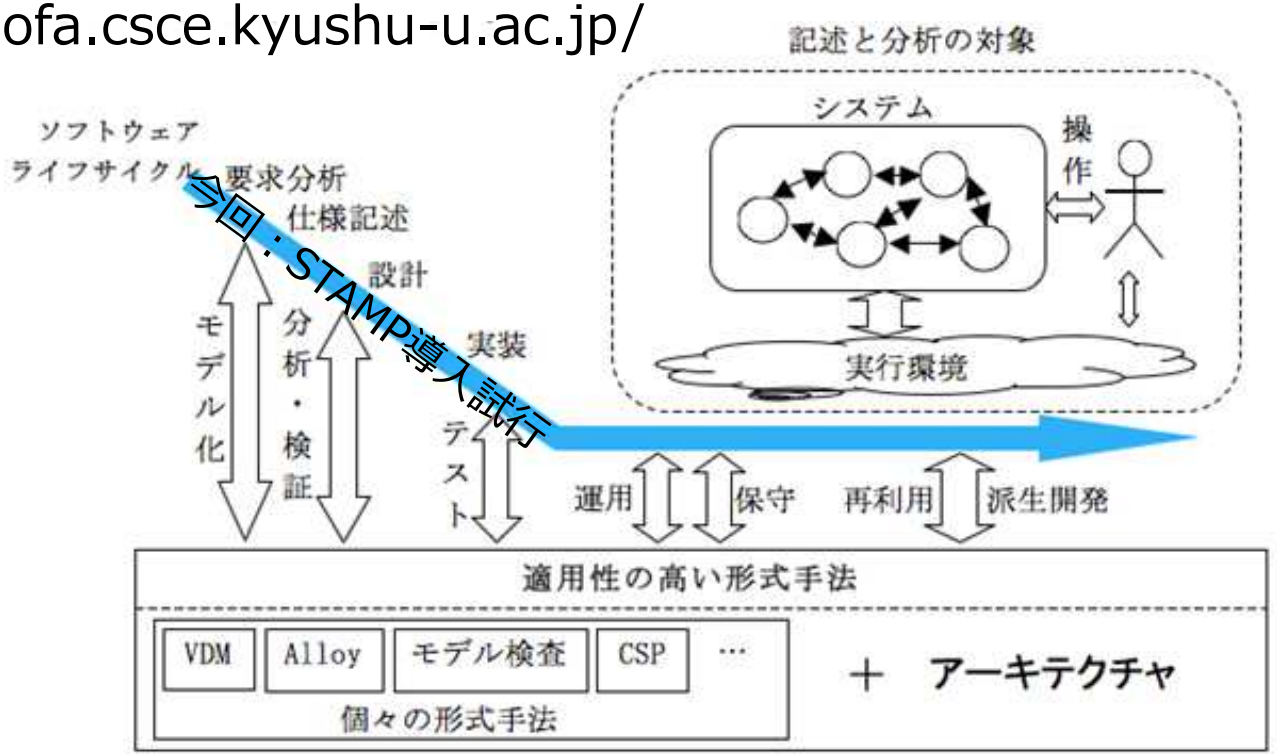
九州大学・システム情報科学研究院
日下部茂
荒木啓二郎

想定，対象など

- 新しい手法の導入による，クリティカルソフトウェアのプロセスのテーラリングに関心があるエンジニアや管理者など
- 基本的にトップダウンのアプローチだけれどもテーラリングの対象は特定のフェーズに限定したものではない
- 個別の要素技術の優劣の議論ではなく，要素技術の特徴を活かす併用法についての発表
- 例えばSTAMP(Systems-Theoretic Accident Model & Processes, Nancy G. Leveson教授(MIT))のみが関心事の場合
  - 提唱者のWebページに多数の資料が公開されている[1]
  - 日本でも(WOCS^{2}の)事例発表[2,3]や日本語の報告書もある[4]

研究グループの紹介

- システムのライフサイクルの各段階に応じた形式手法活用
  - アーキテクチャ指向形式手法に基づく高品質ソフトウェア開発法の提案と実用化, 科研基盤研究(S), 荒木啓二郎代表, 2012～2016年度
  - http://aofa.csce.kyushu-u.ac.jp/



形式手法の有用性と普及

- 形式手法：クリティカルなソフトウェアの開発に有効なアプローチのひとつ
- 例えば，産業界での事例の報告[5]で，形式手法の利用は成功か，との問いに対し9割以上が成功と回答
  - 強く同意が61%
  - 同意が 34%
  - どちらともいえない5%
- 一方，実際の現場での利活用は限定的

→相乗効果が期待できる有用な手法との併用

形式手法導入障壁の例

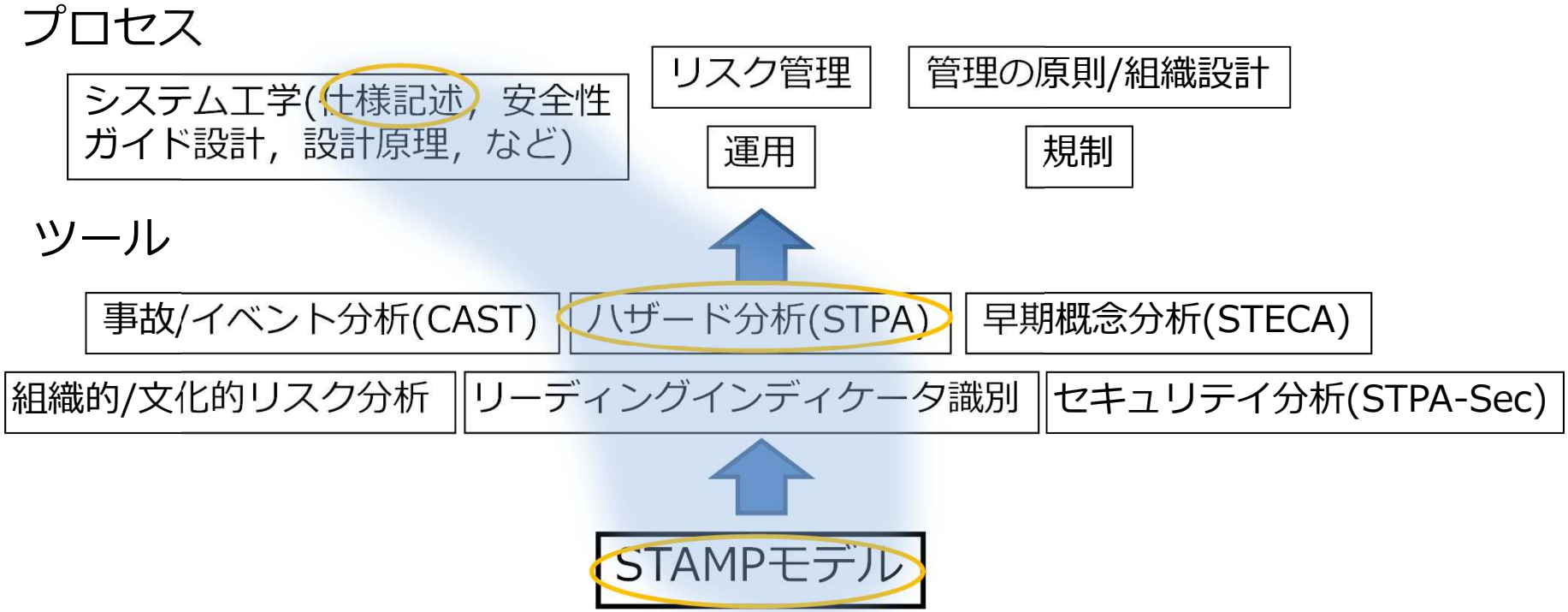
- ステークホルダが見通しを持ちにくい
- 記述中や記述後，複数のステークホルダやフェーズの間でモデルを活用することが容易でない
  - 記法になじみがない
  - 捨象の基準や事前・事後条件の意図や背景が不明だと，実装やテストで有効に活用できない

→形式的なモデルを構築する前の活動や成果物も重要

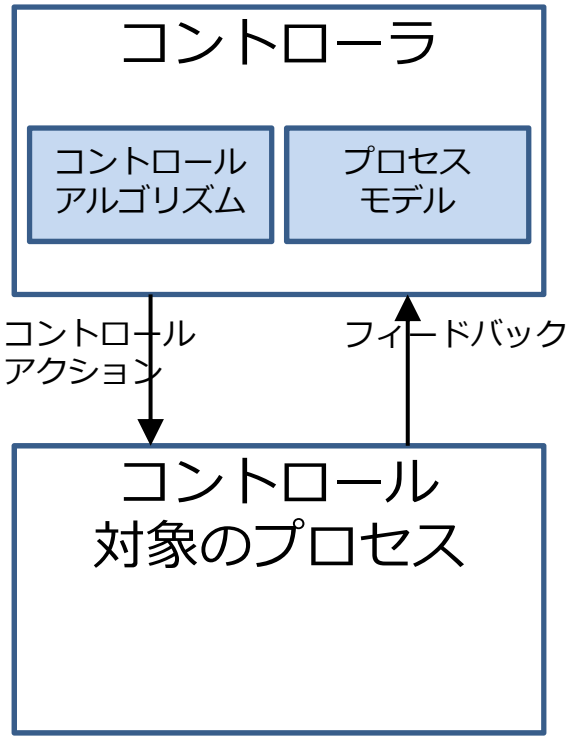
  - 例えば，自然言語などの非形式的な記述による作業成果物から形式的なモデルを開発する作業を支援する，用語辞書ツールや，UMLツールなど
  - 今回はSTAMPに基づくツールとプロセス

STAMPに基づくツールとプロセス

STAMP(Systems-Theoretic Accident Model & Processes, Nancy G. Leveson教授(MIT))：ソフトウェアやハードウェア，社会システムも含んだ包括的な分析が可能な事故モデル



STAMPの基本コントロール構造



- トップダウンのモデリング
- 相互作用と制約に焦点
  - コントロール対象プロセスの抽象的モデル
  - コントロールループの不変条件
  - コントロールアクションの事前条件・事後条件

→形式的モデルの主要要素に

形式モデル構成の手引の例

1. 要求を読む
2. 可能性のあるデータ型(しばしば名詞から)と関数(しばしば動詞から)を抽出する
3. 型に関する表現の概略を描く
4. 関数に関する概略を描く
5. 関数から不変な性質を決定することによって型定義を完成させ，それらを定式化する
6. 関数定義を完成させ，必要があれば型定義を変更する
7. 要求を再検討して，モデルの中で各項目が考慮されていることを確認する

STAMP/STPAの活用：プロセスモデルやコントロールアクション，安全制約

STAMP/STPAの手順例

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：受容できない損失が発生するイベント
- ハザード：システムを取り巻く環境の最悪の条件によって，アクシデントにつながり得るシステムの条件の集合，状態

準備2：コントロールストラクチャの構築

- システムの安全制約に関連するコンポーネントと相互作用を識別

Step 1:非安全なコントロールアクション(UCA:Unsafe Control Action)の識別

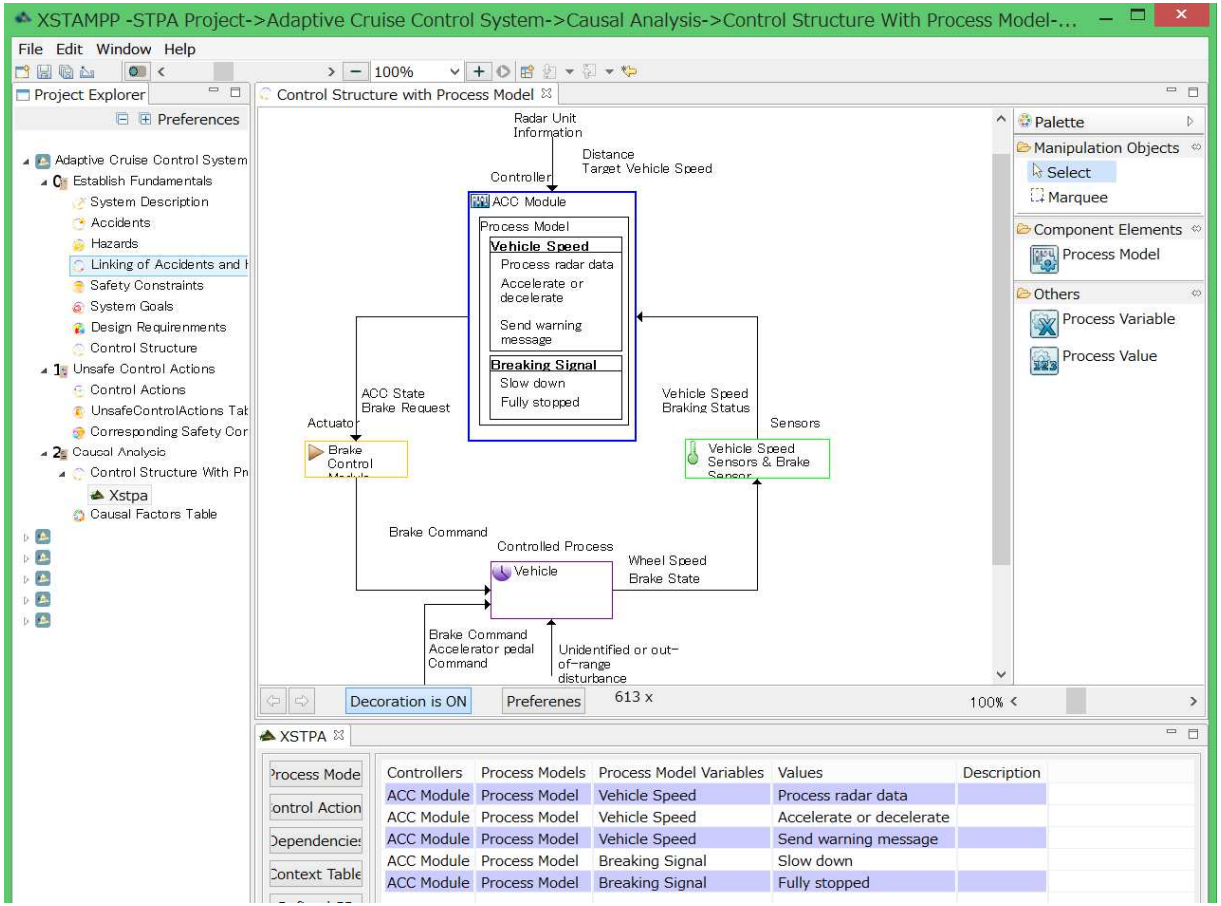
1. “Not Provided” 必要なコントロールアクションが供給されない
2. “Incorrectly Provided” 誤った非安全なコントロールアクションの供給
3. “Provided Too Early, Too Late, or Out of Sequence” 不適切なタイミングでの供給
4. “Stopped Too Soon,…” 不適切な停止 (途中で停止, 必要以上に供給)

Step 2:Causal factor(誘発要因)の特定

- UCA毎にコントロールループを作成し，詳細なハザード要因を分析する

支援ツールの例

XSTAMPP(eXtensible STAMP Platform), Asim Abdulkhaleq



試行

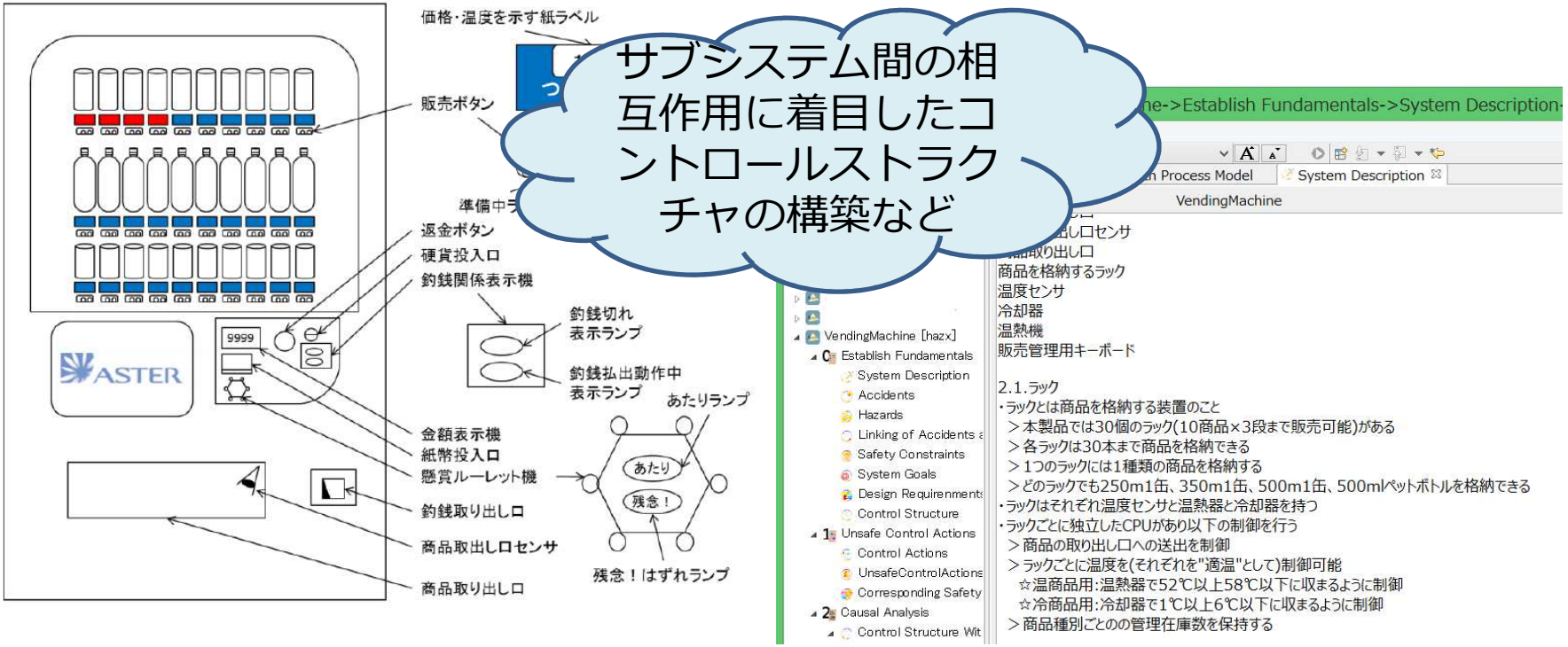
Pre-formalメソッドとしてのSTAMPモデリングプロセス
(今回は，STPAとVDMの組み合わせ)

- 後続する形式的なモデリングをより効果的に支援?
- 多様なステークホルダ間での形式的モデルの理解を促進?

試行対象：主に既存の例題を利用

- NPO法人ASTERのテスト設計コンテスト2015の例題
- Co-modeling/Co-simulation ツール(Crescendo)報告書の例題[8]
- (共同研究での事例)

テスト設計コンテスト2015の例題



Crescendo Co-modeling, Co-simulation

- DESTECS (Design Support and Tooling for Embedded Control Software)　http://www.destecs.org/
- 組込みシステムの大規模複雑化
  - 実機を作成しテストするようなアプローチは困難
- モデルベース開発
  - 現実世界のシステムの連続時間の動きを，離散時間で動作するコンピュータの中で完全に表現することは難しい
- Co-simulation
  - プラント（連続時間）とそのコントローラ（離散時間）をそれぞれ適した表現方法でモデリング（CT-model・DE-model）
  - これらのモデルをツール(Crescendo)を用い，一つのモデル（Co-model）としてシュミレーション
- 例題を利用：コントローラとその対象という観点

評価

観点

- 引き続く形式的モデリングのプロセスをよりよくガイド?
- STAMPモデルにより形式的モデルの理解を促進?

主観的評価

- アクシデント，ハザード，安全制約の識別は形式的モデリング時の抽象化や捨象に有用
  - コントロールストラクチャはモデルの構造に対する指針
  - 形式的なモデリング以前に実施可能な分析を促進
- 利用可能なガイドラインの選択肢が広がるが，能力度や成熟度によって効果は異なる模様
  - 例：VDMエキスパートだとVDMだけで事足りることも多い
- STAMP/STPAに形式的仕様記述言語を用い分析をより効果的に
- STAMPモデリング準備段階の支援(STPA Step0相当)の必要性

関連研究

- John Thomas, Extending and Automating a Systems-Theoretic Hazard Analysis for Requirements Generation and Analysis, Ph.D. Dissertation, MIT Engineering Systems Division, 2013.

- Asim Abdulkhaleq, A Comprehensive Safety Engineering Approach for Software Intensive Systems based on STPA, 3rd European STAMP Workshop, 2015.

まとめ

クリティカルなソフトウェアの開発での形式手法の導入をより効果的に → 形式的なモデリングの前のアクティビティとしてSTAMP/STPA活用の提案，予備評価

- 引き続く形式的モデリングのプロセスをよりよくガイド
- STAMPモデルにより形式的モデルの理解を促進
- アクシデントの定義により安全工学の知見活用も可能[9]
- 形式的モデル化でSTAMP/STPAを効果的にする相乗効果

今後の課題

- より多くの事例，可能な限り客観性の高いデータ獲得
- ガイドライン化
- 他の組み合わせや効果的なツール連携の検討

参考文献

1. MIT Partnership for a Systems Approach to Safety (PSAS), http://psas.scripts.mit.edu/
2. 中尾春香他, Modeling & Hazard Analysis using STPA, 8th WOCS, 2011
3. 寺田庸弘他, 宇宙機における不具合分析手法CASTの適用, 11th WOCS, 2014
4. STAMP手法に関する調査報告書, IPA/SEC, 2015
5. Jim Woodstock, et.al, Formal methods: Practice and experience, ACM Computing. Survey. 41, 4, Article 19.
6. ジョン・フィッツジェラルド他，ソフトウェア開発のモデル化技法，岩波書店，2003
7. An STPA Primer, psas.scripts.mit.edu/home/home/stpa-primer/
8. Claire Ingram, et.al., Crescendo Examples Compendium, Crescendo Technical Report TR-002, 2014
9. Nancy Leveson, MIT OpenCourseWare, 16.863J System Safety, Spring 2011. http://ocw.mit.edu