モデルベースアプローチに基づく障害原因診断手法
～活動の概要と障害原因診断手法の体系化～

2014年11月21日

会津大学　コンピュータ理工学部　教授
兼本　茂

背景・問題意識、前提とする状況

- 大規模・複雑化し、ネットワークを通じて個々のシステムが連携することにより新たなサービスを提供することが拡大している
  - → トラブルが発生した際の影響範囲が大きく、かつ深刻になる危険がある
    障害発生の主たる原因を早急に見つけ出し緊急対策により影響を最小化することが求められる
- 新たなシステムの基幹を担う要素がソフトウェアに替わってきている
  - → 障害が発生したときのシステムの診断や原因分析、対策をソフトウェアを中心としたシステム視点に変えなければならない
- 世の中のシステム障害がシステム視点から分析されていない実態がある
  - システム相互間の複合原因や長期間の保守によるシステムの劣化が原因と考えられる障害が増えてきている
- 新たにソフトウェアを中心とするシステム視点の方法論、および、それを使いこなせる人材の育成が求められている

→モデルベースアプローチに基づいた迅速な障害原因診断技術

1

目的と対象者

- **原因の追究**
  重要インフラ(製品・制御システム)にシステム障害事象が発生したときに、ソフトウェア面の原因を、迅速かつ的確に、指摘できるようにする。
  - モデルベースアプローチの積極活用により・・・
  - システムおよびソフトウェアの原因箇所を絞り込む
  - 対象とする原因: 要求仕様の欠陥、システム間インターフェイス不具合、ソフトウェア実装エラー、外部環境変化によるソフトロジックの不完全仕様の顕在化、保守・更新管理の不徹底によるバグの作り込み、システムの改ざん
- **人材育成**
  - 障害事象から原因究明(と対策など)を実施できる人材を育成
  - 同様の障害発生を防ぐ教育コンテンツの作成
  - 原因究明ツールの習熟・普及に関わる教育コンテンツの作成
- **対象者**
  システム運用の事業者、システム開発者、監督機関、事故調査委員会関係者

2

活動目標(IPA・JASA共同プロジェクト)

- 障害原因診断に関して、客観性を持った第三者検証活動としての役割を確立する
  - 類似の活動
    - 事故調査委員会・・ソフトウェアという特殊な製品を対象にした調査手法は未成熟
    - IV&V機関・・開発企業の知的所有権に配慮した独立検証の困難さ
    - 安全関連ソフトウェア開発コンサルタント・・各種規格やツールの習熟のコスト

  →「事後V&V」手順としての体系化
- 客観性を持った第三者検証に要求されること
  - 障害発生後の初動調査と情報収集
  - システム要求仕様の理解・モデル化
  - ソフトウェアを含んだシステムのハザード分析手法の調査・検討
  - システムとソフトウェアのどこに原因があるかを見極める診断手法
  - ソフトウェアロジックの不具合を見極める形式検証手法、テスト手法
  - 障害原因診断結果の体系的な整理と教育コンテンツとしてのデータベース化

  →モデルベースアプローチによる透明性・客観性の確保、迅速化

3

目標達成への手順(１)

■ ソフトウェア欠陥に関する過去の障害事例の調査

- 過去の障害事例を抽象化し、脚色まで含めて、ケーススタディの対象にできるようなシナリオを作成

■ 事後V&Vとしてのフレームワークの確立

- 障害発生後の初動調査・情報収集方法の標準手順の検討
- システム要求仕様の理解のための方法論、形式検証手法の検討
- ソフトウェアを含んだシステムのハザード分析手法の調査・検討
- システムとソフトウェアのどこに原因があるかを切り分ける診断手法の検討
- ソフトウェアロジックの不具合原因究明のための形式検証手法、テスト手法の検討
- 障害原因診断結果の体系的な整理と教育コンテンツとしてのデータベース化の検討

4

目標達成への手順(２)

■ ケーススタディ

- 要求仕様の形式検証に関する各種手法の比較評価
- 形式手法等のツールを使ったソフトウェア障害診断手法の有効性検討
- 各種ハザード分析手法の事後V&V活動としての有効性評価

■ 対象とするシステム

- モデルベース開発方式に基づいて、障害原因診断のためのテストベッドにしうるシミュレータ(化学プラントシミュレータ)を開発する。
- 過去の抽象化された障害事例を模擬でき、その障害原因究明のための情報が提供できる。また、対策後の健全性が確認できる。

5

IPA・JASA共同プロジェクト

■ ミッション
- 目標実現のため、行動計画の策定、事例検討と全体計画の立案・実行を行う

■ WGメンバー表

	名 前	勤 務 先	部 署
主査	兼本 茂	会津大学	教授
副主査	金田 光範	東京都立産業技術研究センター	産学公連携コーディネータ(JASA)
委員	漆原 憲博	(株)ジェーエフピー	代表取締役社長(JASA)
委員	大原 衛	東京都立産業技術研究センター	情報技術グループ主任研究員
委員	岡野 浩三	大阪大学	准教授
委員	岡本 圭史	仙台高専	准教授
委員	北道 淳司	会津大学	教授
委員	高村 博紀	(株)アトリエ(DEOS協会)	研究員(JASA)
委員	田渕 一成	Biz3	情報技術グループ(JASA)
委員	中村 洋	(株)レンタコーチ	代表取締役(JASA)
SEC委員	三原、十山	IPA/SEC	

6

取り組みの経緯

■ ソフトウェア欠陥に関する過去の障害事例の調査

■ 事後検証用テストベッドの開発
- MATLAB/SIMULINKを用いた化学プラントシミュレータ
- システム・ソフトウェア障害模擬

■ 事後V&Vフレームワークの検討

■ 要素技術検討
- ソフトウェア制御ロジックの形式検証法
- 形式手法による要求仕様の検証法
- 新しい安全解析法　STAMP／STPA・CAST調査
- 障害原因の同定手法／制御システムセキュリティセンター(CSSC)との連携

7

原因と教訓(湘南モノレール事故)

- 異常割り込みにより、加減速シーケンスのループ内のカウンター処理が禁止されるソフトウェアのバグ。長期間にわたるハードの劣化により発生したノイズによってソフトウェアバグが顕在化
- 開発時のテスト漏れか、運用後の変更管理の不徹底かは不明
- 教訓
  - テストケースの網羅性の事前評価の大切さ
  - 変更管理・保守でのバグの作り込み防止
  - システム全体での安全設計の不十分さ(最も大切なブレーキ操作が働かなくなる可能性を全てレビューしていたか、運転員操作の優先度を考慮していたか、など)

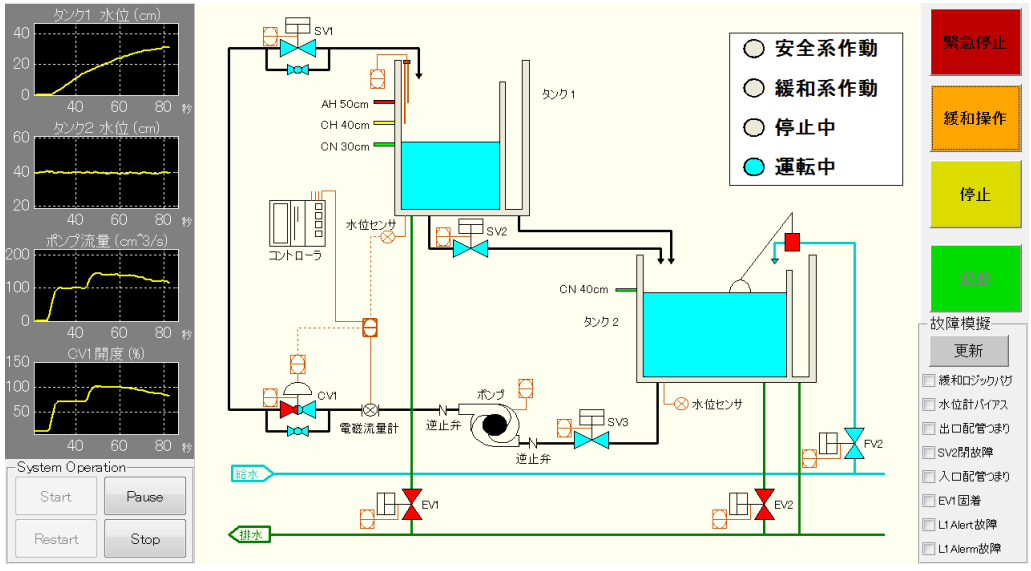
8

原因と教訓(駒場ダム異常放流)

- 機械の不具合、ソフトウェアのバグ、人間の操作ミスが重なって障害が致命的なものになる(スイスチーズモデル)
- フールプルーフ設計、人間工学を考慮した設計の不十分さ
- 教訓
  - 環境に大きな影響を与えるシステムでは、致命的な事故を考慮した安全設計(最後の砦をどうするか)が大切

9

検証用テストベッド（化学プラントシミュレータ）



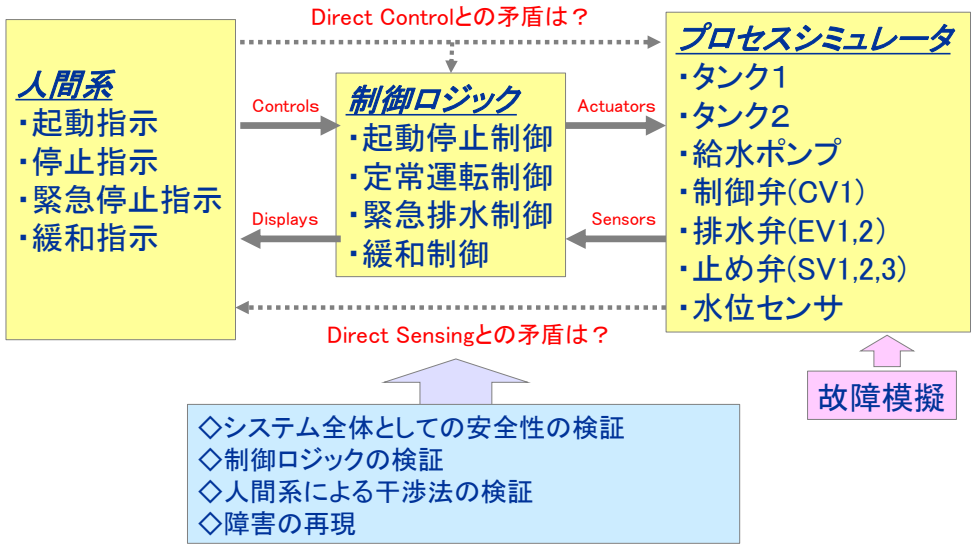
10

制御ロジックの仕様抜粋

- **起動機能・定格運転制御機能**
  - 起動指示ボタンにより、タンク2を一定レベルまで注水する。排水弁の制御はしない。
  - 一定時間後に、止め弁を開いて、ポンプを起動して、タンク1に注水する。各機器の操作はシーケンス制御とする。
  - 定格に達したあとは、PID制御による運転に移行
- **停止機能**
  - ポンプを停止、止め弁は開→閉、排水弁は閉のまま、注水弁は開→閉。水は張ったままでの停止操作
- **緊急排水機能**
  - タンク1のアラームレベル越え、または、運転員指示で、タンク1の水を、排水弁経由で直接排水路に排水する。合わせて、ポンプ停止、止め弁を閉める。
  - タンク1は、安全系（アラームレベル、アラートレベル）と、常用系（水位制御用）の二つの水位センサを備える
  - タンク2の溢水防止のアラームは設けない
- **緩和機能**
  - タンク1アラートレベル越え、または、運転員指示で、3秒間排水弁を開け、その後12秒だけ受付禁止とする。ポンプと制御系は動作のまま。

11

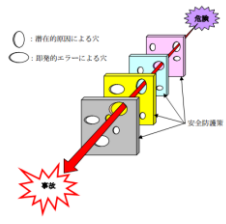
テストベッドとしての化学プラントシミュレータ



12

故障模擬機能(案)

- 常用系水位センサのバイアス
- 安全系水位センサ(アラーム、アラート)の故障
- 排出配管つまり
- タンク1排出止め弁(SV2)の閉故障
- 入口配管閉故障または注入配管つまり
- 配管リークまたは蒸発
- 制御弁(CV1)故障
- PID制御器故障
- 安全系ロジック故障
- 緩和系ロジック故障
- および、上記の多重故障
  (スイスチーズモデル)



過去の障害事例を参考に、抽象化した障害事例を模擬するテストベッド

■モノレールの衝突を、タンクからの溢水に対比させ、コントローラの制御ロジックのバグを再現
→形式検証によるバグの検知

■発電所制御の緩和ロジックを、タンクの溢水防止に適用し、運転員操作と自動ロジックの干渉を再現
→形式検証によるバグの検知

■コントローラ不具合による信号挙動の変調を再現
→障害原因切り分けのシステム診断手法の検証

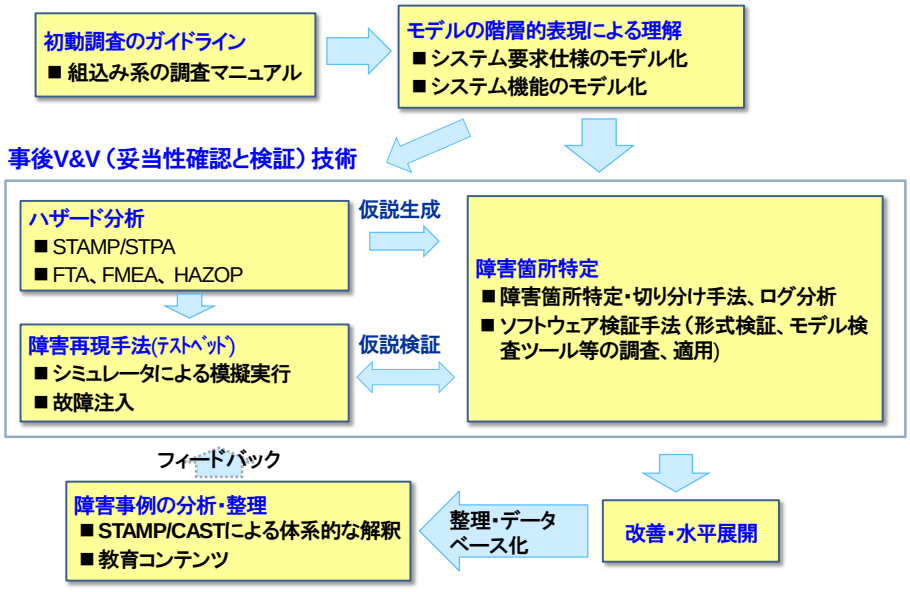
13

事後V&Vのフレームワーク

- JAMSS(有人宇宙システム株式会社)や欧州で実施されている、第三者機関によるIndependent Validation &Verification (IV&V)を参考にする。
- 下記の要求項目を反映した体系図とケーススタディによる適用方法の具体化を図る
  - 障害発生後の初動調査・情報収集方法の標準手順の検討
  - システム要求仕様の理解のための方法論、形式検証手法の検討
  - ソフトウェアを含んだシステムのハザード分析手法の調査・検討
  - システムとソフトウェアのどこに原因があるかを切り分ける診断手法の検討
  - ソフトウェアロジックの不具合原因究明のための形式検証手法、テスト手法の検討
  - 障害原因診断結果の体系的な整理と教育コンテンツとしてのデータベース化の検討

14

事後V&Vのフレームワーク

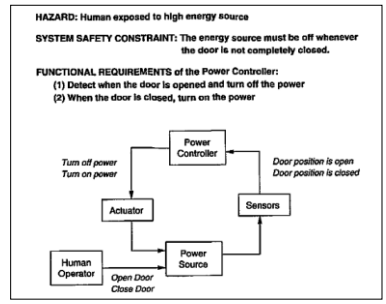


15

STAMP／Engineering a Safer World by N.Leveson

- STAMP （システム理論に基づく事故モデル）
  - System-Theoretic Accident Model and Processes
  - Three basic constructs: (1) Safety constraints, (2) hierarchical safety control structure, (3) process models
- STPA （STAMPによる安全解析法）
  - System-Theoretic Process Analysis
- CAST （STAMPによる事故分析法）
  - Causal Analysis based on STAMP

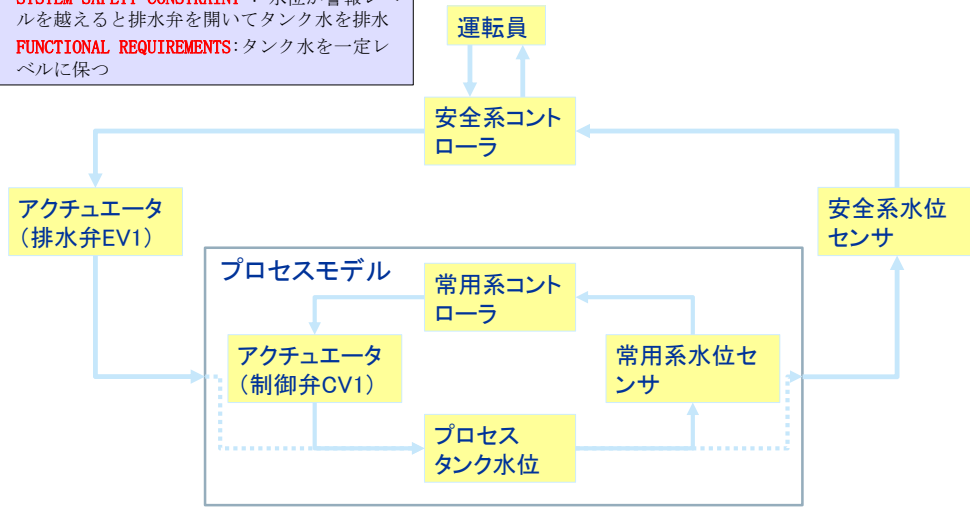
現在の複雑な人工物システムでは、システムを構成するサブシステムやコンポーネントに不具合がなくとも，サブシステムやコンポーネントの相互作用によってハザードが発生する。従って、従来型のリスク分析手法では限界がある。



16

化学プラントシミュレータの制御構造図

- HAZARD(H1) ： タンクからの溢水
- SYSTEM SAFETY CONSTRAINT ： 水位が警報レベルを越えると排水弁を開いてタンク水を排水
- FUNCTIONAL REQUIREMENTS:タンク水を一定レベルに保つ



17

まとめ・ReactiveからProactiveな体制へ

- 障害原因診断に関して、客観性を持った第三者検証活動としての役割を確立する　→事後V&V手順としての体系化

- 客観性を持った第三者検証に要求されること
  - 障害発生後の初動調査と情報収集
  - システム要求仕様の理解・モデル化
  - ソフトウェアを含んだシステムのハザード分析手法の調査・検討
  - システムとソフトウェアのどこに原因があるかを見極める診断手法
  - ソフトウェアロジックの不具合を見極めるFTA、テスト手法
  - 障害原因診断結果の体系的な整理と教育コンテンツとしてのデータベース化

→ケーススタディを通して、個々の要素技術の確立を目指す

18

ご清聴ありがとうございました

詳細はブースデモンストレーションをご覧下さい

19