LT3:VDM形式仕様記述とFRAMによるレジリエントなテストシナリオの分析 (および情報セキュリティ産学共同研究センタ)

日下部 茂：長崎県立大学 情報セキュリティ学科
（小田さん：SRA、張先生：南山大学、…）

2022年11月05日

- 本資料は添付の公開資料の内容や個別の調査結果・知見を発表者が個人レベルでまとめたものです．

募集中！

- 長崎県立大学・情報セキュリティ学科
  - 情報セキュリティ産学共同研究センター
    - ✓**共同研究募集中！**
  - 定員倍増(40->80)
    - ✓**インターンシップ先募集中(学部3年)**

厳密な仕様記述とテスト

- 数理的な事前条件, 事後条件＋実行可能な仕様
  - テストケースの形式的な生成
  - 証明よりテスト、クラウド(Hadoop)でブルートフォース
  - 仕様記述：開発者目線寄り？

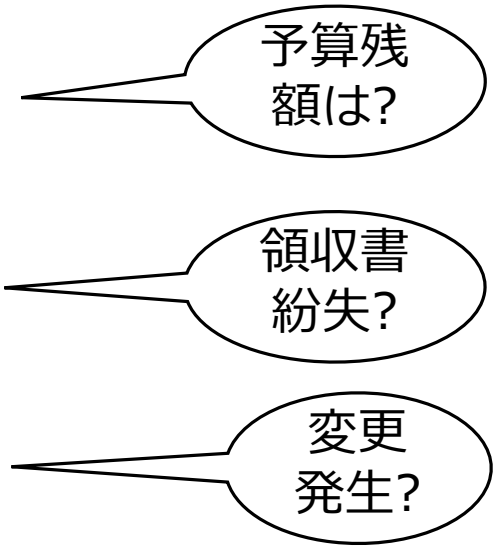
↓

- 硬いコア仕様と柔軟な運用シナリオを分析
  - 数理的に定義される硬さがにあだになる時も（杓子定規?）
  - Inspired by 硬さによる不幸
    - ✓例：医療安全、Safety-II、…
  - WAIとWADのすり合わせ、でもコアなところは硬く

シナリオ記述と仕様記述

例：出張経費処理

1. 出張したい人が出張申請して、
2. 上司や会計担当が承認して、
3. 出張して
4. 出張した人が精算申請をして、
5. 上司や会計担当が精算承認して、
6. 出張した人に旅費や手当を振り込む



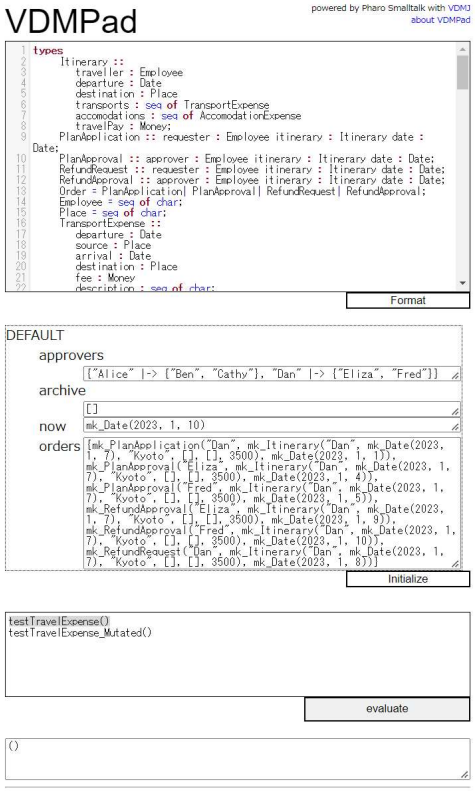
WAI: Work As Imagined　　WAD: Work As Done

VDMでの実行可能仕様記述とシナリオテスト

WAI:Work As Imagined

正規の例

問題なし

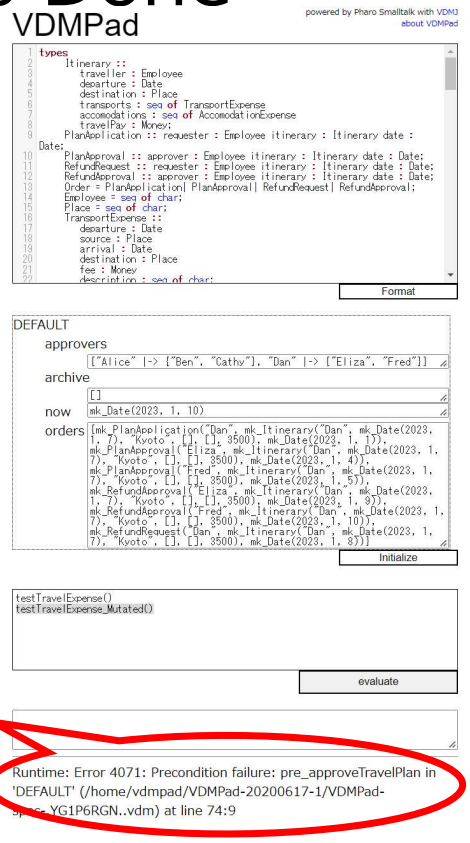


WAD:Work As Done

承認が出張日より後に

怒られる(^^;)

実務的にはOK?



杓子定規→レジリエント

機能共鳴分析手法 FRAM: Functional Resonance Analysis Method

- システムの機能間の依存性や結合性の様子をモデル化し分析する手法
- 2004年に南デンマーク大・E. Hollnagelが開発.
- FRAMでの機能とは，ある結果を提供するために必要な活動や活動のセットのこと. 人，組織，システムが行うことを指す
- レジリエンスエンジニアリング，新しいセーフティ(Safety-II)
  - 「物事が正しい方向へと向かうことを保証する」
- 四つの原理による
  - The Principle of Equivalence of Successes and Failures
  - The Principle of Approximate Adjustments
  - The Principle of Emergence
  - The Principle of Functional Resonance

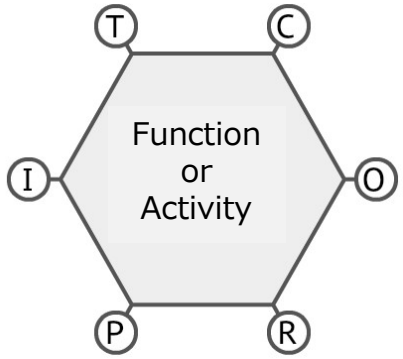
機能共鳴分析手法 FRAM

機能共鳴分析手法 FRAM: Functional Resonance Analysis Method

- 機能を６つの側面で(5つの入力側面と1つの出力側面)
- ツールあり：FMV

モデリング手順

1. 機能とその側面の把握と定義
2. モデル化とモデルの可視化
3. 可視化したモデルに対する分析



I	INPUT:機能が処理を行い変化するもの．あるいは開始するトリガ
P	PRECONDITION:機能が実行される前に存在すべき条件
R	RESOURCE:機能が実行されるときに必要とするもの(実行条件), あるいは機能が消費する資源
T	TIME:機能実行時の時間的制約(開始時刻, 終了時刻, 継続時間, 等)
C	CONTROL:機能の実行を制御する方法やパラメータ(手順,指示,等)
O	OUTPUT:機能の結果．何らかの実体か状態変化

人間中心設計HCDでWAIからユーザ志向に

山崎，他“人間中心設計入門”近代科学社，2016

HCDサイクルの４つの活動	主な手法・サブプロセス
① 利用状況の把握と明示	● 利用状況の把握 ● 利用状況の調査 ● アンケート ● フィールドワーク ● エスノグラフィ ● ダイアリー法 ● インタビュー
② ユーザーの要求事項 の明確化	●グランデッドセオリー法 ●ペルソナ ●シナリオ法 ●品質機能展開
③ ユーザーの要求事項を満足させる設計による解決策の作成	● 発想法 ● パターンランゲージ ● 共感的デザイン ● 参加型デザイン ● プロトタイピング
④ 要求事項に対する 設計の評価	● ユーザビリティテスト ● インスペクション法 ● 心理的尺度 ● 生理学的手法 ● 長期的な評価

必要な調整・変動のシナリオを想定した仕様・テスト

例：出張経費処理

1. 出張したい人が出張申請して、
2. 上司や会計担当が承認して、
3. 出張して
4. 出張した人が精算申請をして、
5. 上司や会計担当が精算承認して、
6. 出張した人に旅費や手当を振り込む