大学共同利用機関法人 情報・システム研究機構
国立情報学研究所
National Institute of Informatics

トップエスイー ソフトウェア開発実践演習

システムやドメインの実践的形式仕様記述演習

株式会社デンソー　須崎拓真　takuma.suzaki.j8e@jp.denso.com
三菱電機マイコン機器ソフトウエア株式会社　徳田伸矢　tokuda.shinya@mms.co.jp
リコーITソリューションズ株式会社　滝沢幹雄　mikio.takizawa@jp.ricoh.com

課題、取り組み

- 【課題】実世界の法・規定に対して形式仕様記述することで、要求や仕様のモデリングや形式化・検証に関するプラクティスおよびその検討力を身につける。
- 【取り組み】東京ディズニーランドのファストパスについて形式仕様記述を行う。

解決のアプローチ

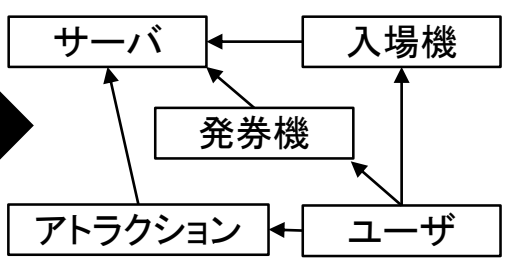
1. ファストパスの実際の仕様を調査する。
2. モデル化して形式化対象を決定する。
   重要な機能に集中して形式化を行う。
3. VDM++で分担ごと形式仕様を記述する。
   二人で同じ仕様を記述して差異を比較する。
4. VDMUNITで形式仕様の妥当性を検証する。
   網羅的な動的テストを自動的に実行する。

形式化プロセスの実践

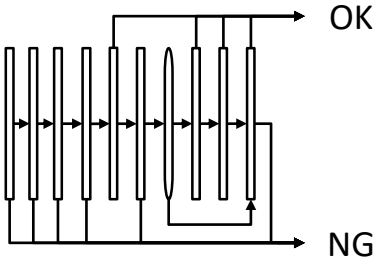
1. 仕様調査 → 2. モデル化 → 3. 仕様記述 → 4. 仕様検証

実際の仕様を調査

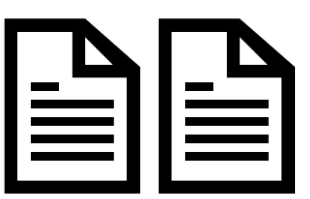
コンポーネント分割



機能のチャート化

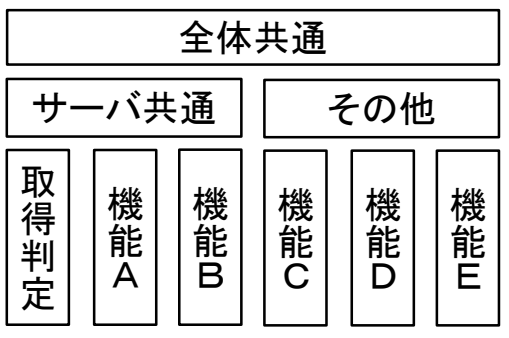


同値仕様の記述比較



着眼点で表現に違い

機能分割



- オブジェクト指向
- 契約による設計
- 重要度の検討
- 作業分担の決定

VDM++による仕様記述

検証結果をフィードバック

VDMUNITによる妥当性確認

自動化で効率的

評価

- **ファストパスの仕様が明確になった。**
  仕様が検証可能な状態になったことにより、その曖昧さや妥当性を確認できるようになった。
- **形式化と検証のプラクティスが身についた。**
  組織的な形式化と検証のプラクティスを通して、仕様を成熟させることができるようになった。
- **形式仕様記述のメリット・デメリットを体験できた。**
  仕様について統一的な理解を得ることはできたが、教育コストは高く、記述には時間がかかった。

業務への展開

形式仕様を開発に導入した場合、人による仕様解釈は不要となり、設計やテストの自動生成が可能になる。