

ディペンダブルソフトウェア開発に向けた形式手法の研究

Formal Methods for Dependable Software Development

中島 震
Shin NAKAJIMA

何がわかる？

ディペンダビリティへの関心が高まっています。ひとつのシステムには、発注あるいは購入者、開発者、運用者、利用者など多くのステークホルダが関わります。立場によって、システムに対する期待が違ふでしょう。信頼性を論じる際の拠り所になる「正しさの基準」が異なるといえます。「正しさとは？」を理解することが重要です。

どんな研究？

どのような正しさの基準があり、どのように担保するかを、形式手法と呼ぶ技術アプローチから考えます。特に、ロジック・モデル検査に代表されるアルゴリズムベースの形式検証法を採用します。「正しさ」の確認法を自動化する技術を確認し、ソフトウェア工学の道具として提供したいと考えています。

内容

産業界の取組みとの連携

ディペンダブルソフトウェア・フォーラム (DSF, Dependable Software Forum)

参加企業：NTTデータ、富士通、日本電気、日立製作所、東芝

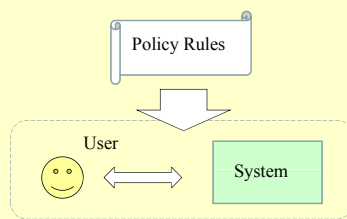
ソフトウェアの信頼性と安全性向上を目指す — 形式手法適用評価WG

産学戦略的研究フォーラム(SSR)：Cyber-Physical Systems 時代のソフトウェア工学

ディペンダビリティの新しい課題と研究活動

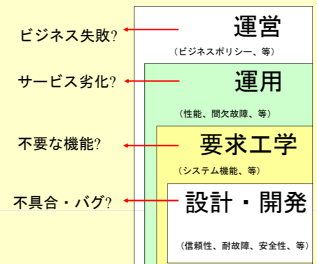
Any useful computing system interacts with the world outside the computer.
(M. Jackson, 1999)

システムの周辺



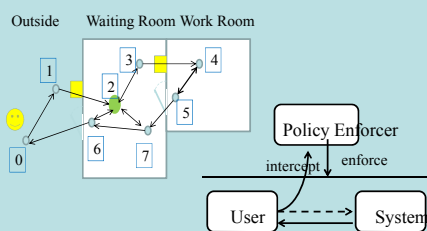
ディペンダビリティスタック

開発時の予測



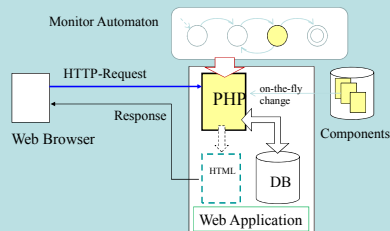
ポリシー規則の分離

- 2階層フレームワーク
- ガイドシステムの利用者振る舞い



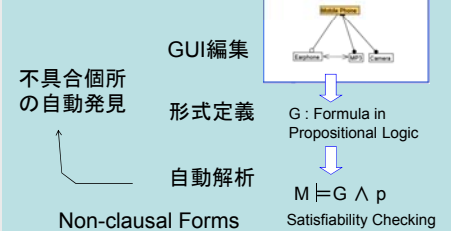
実行時の自己適応

- モニタオートマトン
- 不具合検知→プログラム置換



SPLE: プロダクトライン

- FODAフィーチャダイアグラム
- FD-Checker



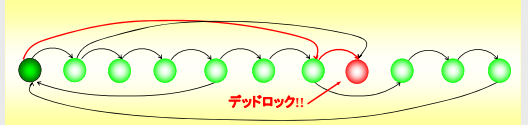
基礎技術

アルゴリズムベース形式検証 algorithmic verification

- 基本技術とプログラム品質保証への応用

プログラム検査

- Specification-based Testing (SBT)：法政大学
事前・事後条件からのテスト自動生成
- Modular Verification：総研大博士課程
DbCとモデル検査の組み合わせ



「モデル検査法」
(教科書)

2008年→

←2010年

