ソフトウェアシステムの信頼性と安全性

Reliability and Safety of Software-intensive Systems

中島　震
Shin NAKAJIMA

どんな研究？

「ソフトウェアを支配するのは，自然法則ではない．複雑さである」と云われています．信頼性と安全性に関して，システムに期待されるレベルを達成するには，複雑さの理由を解明し，その複雑さを低減する方法を確立しなければなりません．ところが，万能の解決策がないことは良く知られています．本研究室では，ソフトウェアの開発過程で遭遇する，重要な3つの課題に着目して，研究ならびに教育に携わっています．

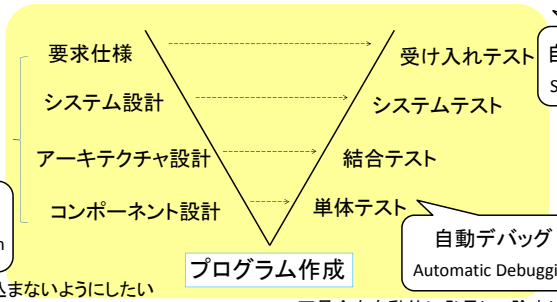
何がわかる？

「つながる世界」のイノベーションは，私たちの社会と生活を豊かにします．同時に，基盤をなすソフトウェアは複雑化する一方です．リスクを低減する技術は，着実に進んできているにも関わらず，常に一歩，出遅れます．科学的な方法で，リスクに立ち向かうことが期待されます．でも，「科学的」とは，何なのでしょうか．そもそも，ソフトウェアの科学やソフトウェア開発の科学は，どのような現象を解明しようとしているのでしょうか．

状況設定

信頼性
期待される機能を果たす
想定される「故障」への対策を考える
ハードウェア→偶発的故障
ソフトウェア →系統的故障

安全性
機能を果たさなくなった後にリスクを回避・低減する
安全性を担保する機能を最初から考えておく（機能安全）



構築からの正しさ
Correct by Construction
系統的故障が入り込まないようにしたい

自動デバッグ
Automatic Debugging
不具合を自動的に発見して除去したい

自己適応システム
Self-Adaptive System
周囲（要求仕様，動作環境）の変化に対応したい

リスク
発生確率と影響の深刻さを定量的に見積もりたい

ディペンダブル・システム
リスクが許容範囲内である

研究内容

構築からの正しさ

課題：開発上流工程で用いる設計書が曖昧なことから，開発が進むと共に入り込む誤りを，完全には除去できない

方法：曖昧さの入り込まない記述と，これを利用した開発の方法（形式手法）を用いる

現状：欧州を中心に膨大な知見が蓄積されているが，国内では，その技術体系が正しく理解されていない

内容：大学院修士課程レベルの基礎教育（総研大，東工大で実施）

(1) モデル規範形式手法（VDM, Z, B, Event-B）の共通基礎
状態ベース仕様，リファインメント，証明条件
(2) 自動検証の基礎（プログラム自動検査を含む）
ロジック・モデル検査，有界モデル検査，テスト自動生成
(3) オブジェクト指向デザインへの応用
UML/OCL, 状態遷移ダイアグラム/Statechart

自己適応システム

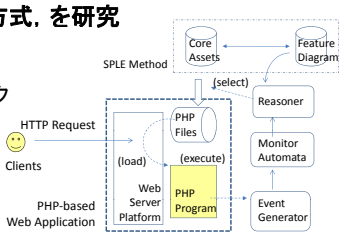
課題：システム開発の前提条件を明らかにすることが難しいので，サービスイン後に，システム変更が頻繁に起こる

方法：システム自身の実行状態ならびに実行環境の状況を監視し，不具合を検知した場合，システムの機能振る舞いを変更する

内容：深刻な被害に至らない「柔らかな不具合」という考え方を導入し，自己適応Webアプリケーションの方式，「柔らかな不具合」の発生確率を定量的に予測する方式，を研究

最近の論文
(1) 自己適応Webアプリケーションシステム：概念アーキテクチャと実現フレームワーク
コンピュータソフトウェア，2012年8月
(2) 実行時干渉の発生確率予測
コンピュータソフトウェア，2013年8月

挑戦的萌芽研究（2011～2014年）



自動デバッグ

Automatic Error Localization Method

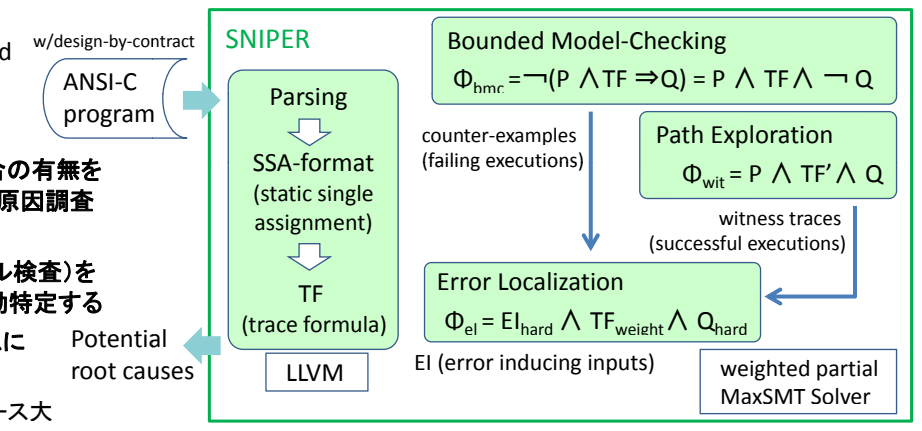
不具合検知 → **不具合箇所特定** → 修正

課題：プログラムを対象とした検査技術が進展し，不具合の有無を自動的に調べることが可能になったが，不具合の原因調査に膨大な時間と労力がかかる

方法：プログラム自動検証の方法（SATベース有界モデル検査）を応用して，不具合の原因箇所（root causes）を自動特定する

現状：既存研究では原因箇所特定ができないCプログラムに適用して成功

共同研究：総研大（Si-Mohamed LAMRAOUI），法政大，ニース大



連絡先：中島震／ 国立情報学研究所　アーキテクチャ科学研究系　教授
TEL：03-4212-2507　　FAX：03-3556-1916　　Email：nkjm@nii.ac.jp