安全性確認のための
根拠記述モデルの提案

太田 清隆
Kiyotaka Ota

北九州市立大学 大学院 国際環境工学研究科
情報工学専攻 山崎進 研究室
The University of Kitakyushu

背景

- 組込みシステムに高い安全性が要求されている
  - 高い安全性が必要な製品(自動車，医療機器など)
  - 生活家電
- 安全性の確認のために説明が求められる
  - 従来の説明方法
    - ・国際標準規格に則った開発プロセスの使用
    - ・十分なテスト

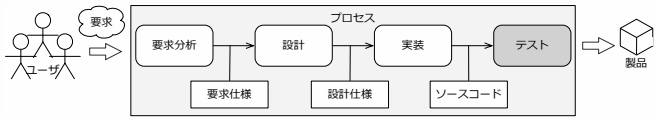

図1:大まかなソフトウェア開発の流れ

問題

- 開発プロセスにおける問題
  - 設計仕様が要求仕様を実現する仕様として妥当か分からない
  - 製品の開発プロセスとして適切か分からない
  - 各工程の成果物(アウトプット)が妥当か分からない
- テストにおける問題
  - どのような危険性に対するテストなのか分かりづらい
  - どのテストがどの要求を保証するのか分かりづらい

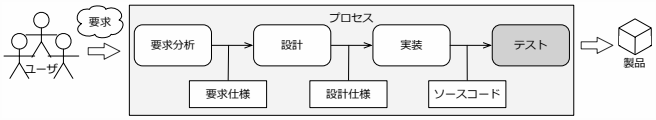

図1:大まかなソフトウェア開発の流れ

キーアイディア

- 「妥当か･適切か」の説明が不足している

そこで...

根拠に着目する
- 工程や成果物の妥当性を説明･確認できるようにするために

根拠とは

- アウトプットや決定などに至った理由
  - 「なぜそのようなアウトプットになったのか」
  - 「何のためにこのようなアウトプットにしたのか」
- WhatとHowをつなぐWhyやFor whatにあたる
- 根拠を示すことでアウトプットの妥当性を説明･確認することができる

根拠を記述することで分かること(1/2)

- 開発プロセスにおける問題
  - 要求仕様と設計仕様の対応関係が分かる
  - 製品の性質などを考慮した開発プロセスだと分かる
  - 成果物に至った理由や成果物の目的が分かる

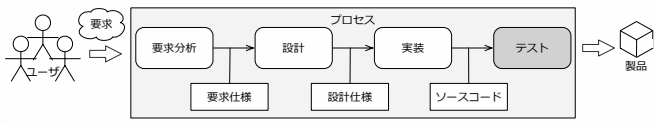

図1:大まかなソフトウェア開発の流れ

根拠を記述することで分かること(2/2)

- テストにおける問題
  - どの危険性を考慮したテストなのか分かる
  - どの要求を保証するテストなのか分かる

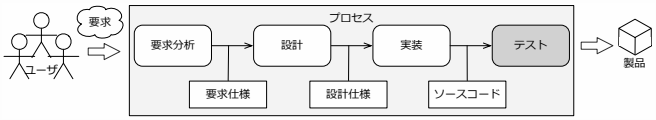

図1:大まかなソフトウェア開発の流れ

根拠記述の現状

- 自然言語で記述されている
  - 書類などに文章として記述される
- 記述方法のガイドラインは確立されていない
  - 根拠を表現するモデルがない
  - どの範囲まで記述すれば良いのかわからない

提案

- 根拠記述のためのモデルを作成する
  - 根拠の記述方法を提案
- ETロボコンを題材にする
  - ETロボコンにおける危険要素を除外する機能の根拠を記述
  - ETロボコンにおけるテストの根拠を記述

ETロボコン

- 組込みシステム開発における若手エンジニアに教育の機会を提供することを目的とした大会
- 組込みシステム開発の分析･設計のモデリングに関する教育に力をいれている
- ライントレースカーの走行タイムと設計モデルを競う

図2:ETロボコン2010走行体

提案モデル

- グラフィカルな記述モデル
- 機能やテストなどの提案に必要な知識の記述
  - 危険要素(Hazard)を除外する機能を考えるのに必要な知識を記述する
  - テストの決定に必要な知識を記述する

詳しくはポスターにて

提案モデルの目的

- 自然言語の削減
  - 自然言語による記述を少なくすることで客観性を持たせる
- 背景知識の記述
  - 機能やテストの提案の背景となる知識の記述することで理由を説明する