トップエスイー修了制作

組込みソフト教育コンテンツの制作
検証モデル「データ送信システム」を教材に

関口賢三　　gutti.twins@gmail.com

開発における問題点

時間的制約の要求を満たすための設計スキルの中で「並行タスクの実行時間」を扱うスキルは重要なものの1つである．これは，原理と仕組みの理解に加え，どのような手法・設計・実装が有効か否かを考察する経験知が重要である．　ところが、設計担当分野の細分化により，設計者が本スキルを身につける機会が減少した．そこで本スキルを積ませる教育コンテンツが望まれていた．

手法・ツールの適用による解決

施策として「並行タスクの実行時間」の設計スキル向上を目的に教育コンテンツを試作し効果を分析した．モデル検査器SPIN(注)はモデルの実行の振舞いを網羅的に検証可能である．この特徴を生かしSPINで教材（検証モデルと検証クレーム）を制作した。 さらにこれをベースとした教育用コンテンツで講習会を実施した．　(注)SPINは時間を扱えないため離散的時間カウンタをモデルに実装した．

施策

教材制作
- ・検証モデル「データ送信システム」
- ・検証クレーム・・・実行時間の要求
- ・検証モデルをベースとした講習会資料

部内講習会

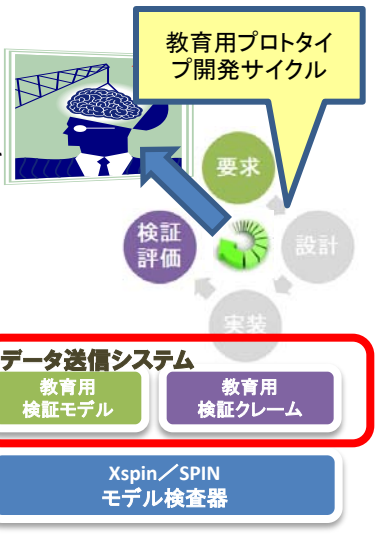
受講者
- ・形式手法ツール未経験者
- ・組込み設計経験者／未経験者混在

講習時間

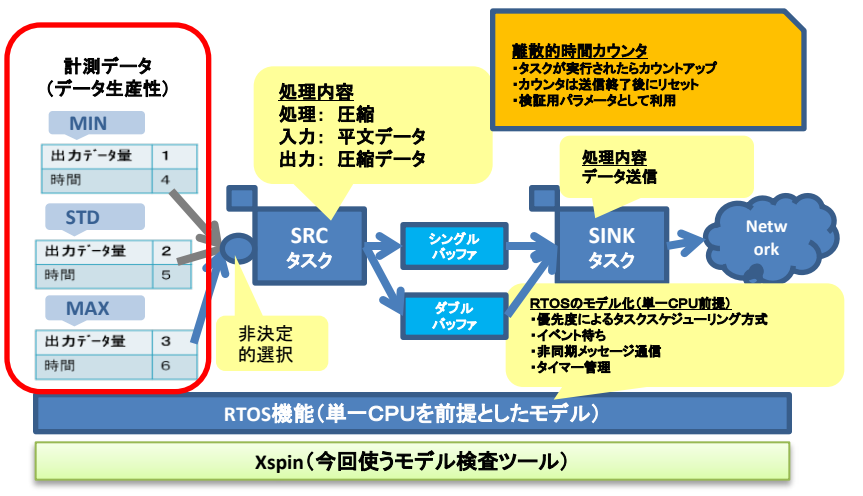
週1回2時間x5回＝10時間

意見交換

効果確認／今後の検討



制作した教育用検証モデル



効果確認分析／今後の対応

本制作はトライアルということで効果確認はアンケートではなく意見交換で代替した．

目的とねらい	受講者の意見	分析	今後の対応
「並行タスクの実行時間」スキルの重要性を認識させる	『ソフト処理時間が時間的要求のポイントであることが明確になった。』	有効：　狙いどおり 有識者：明確に理解 新人：検証クレームは理解したが振舞いの理解までは至らず	部内外へアプローチ
SPINの有効性を認識させる（1） 要求の明確厳密化	『検証クレームの意味は明確に分かった』	有効：　狙いどおり 検証クレームの有効性有り	設計モデル検証につなぐ検討： （例）LTLによる検証
SPINの有効性を認識させる（2） 実行の確からしさを自ら確認できる	『検証クレームに対して反例が出るパラメータとの関係は分かった』 『コードを見て追ってデバッグしてみないと分からない』	要求の理解と検証だけでは不十分：　想定内 設計モデル／モデル記述言語／モデル検査器の理解と設計モデルのコーディングデバッグ経験が必要	次スライド参照のこと

受講者の意見	分析	今後の対応
『詳しいシーケンス図が欲しい』	モデル設計図面が不充分 ・実行の観点の記述が不足	モデル設計図面の改善 仕様書に実行の意味を明記 （例） ・状態遷移図とシーケンス図の合体 ・イベント待ちや同期方法の明記
『プログラミング言語と異なるようだ。　難しい！』 『トレースの解釈が難しい』 『深く理解したいのでデバッグしてみたい』	簡単な説明では不十分：　想定内 ・受講者はC++などの一般プログラミング言語の知識をベースに考えがち ・モデル記述言語（promela）が命題であることが理解され難い ・モデル記述言語によるコーディング・デバッグ・検証　経験必要 ・モデル検査器のしくみと理論に関する教育（例えばTop SEの基礎理論講座）が必要	教材の改善・追加 一般プログラミング言語との差を出す教材とサンプル （例） ・モデル記述言語（promela）の制約 －ステートメントが真なら進む －コールスタックなし －インライン関数で戻り値不可
『状態遷移図からモデル記述言語への変換の方法？』	詳細設計化に必須の課題 （教材で未記載）	教材の追加 ・プロセスの公平性／同期／デッドロックの関係性 ・実行の可能性とデッドロック

本制作はトップエスイーの設計モデル検査の導入用教材としての副次目的があった。これについても効果が確認できた。

田辺，宇佐美，吉岡，　設計モデル検証（基礎編）講座，トップエスイープロジェクト講義資料，NII，2011

Zhiming Liu, Lecture Notes on Programming Concurrent Computer Systems, UNU/IIST, May 2005