ソフトウェアテストシンポジウム2004
2004/01/27(火)

組み込み商品群における ソフトウェアの妥当性確認

組込みソフトウェア管理者・技術者育成研究会
SESSAME 酒井 由夫

組み込みシステムにおける解決すべき問題

- 組み込みシステムへ降りかかる多様な要求
- 求められる高安全性・高信頼性
- しかし開発期間の延長は許されない
- **これらの問題を解決するにはどうすればよいのか？**

結論

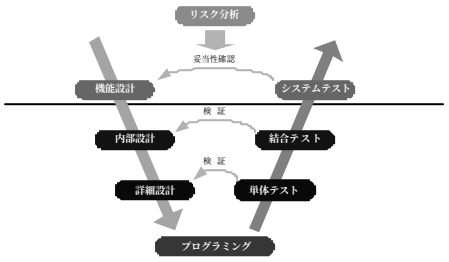
- 組み込み機器の安全性・信頼性をリスクマネージメントによって確保する
- 組み込み商品群におけるコア資産とバリエーションを実現する部分を明確に分離し異なるテストのアプローチをとる
- **これらにより短期間で効果的な組み込みソフトウェアの妥当性確認(Validation)を実施することができる**

組み込み機器におけるプロダクトライン戦略

- 組み込み機器は幅広い商品グレードを持ち、ソフトウェアのみならず、さまざまな資産を再利用することが多い
- 組み込み機器を商品群としてとらえ、プロダクトライン戦略によってコア資産を摘出・利用・管理することで差分開発を加速し商品開発を効率化できる
  - プロダクトラインはCMU/SEIにて定義されたソフトウェア開発のアプローチ

プロダクトラインの3つの活動

開発プロセスの上流工程にリスク分析を 下流工程プロダクトラインを適用



リスク分析の必要性

- 商品出荷後に不具合が発生
  - リコール→莫大な回収費用→企業の信頼が低下
- リスク分析の結果は技術者の暗黙知となっていて無意識のうちに再利用している
  - 暗黙知のままにしておくと漏れ、抜けがでる
- 品質の高い商品を提供している組織はリスクに関する情報を資産化している

リスク分析の意義

- 商品の安全性や信頼性を効果的に確保する近道はリスク分析とリスクマネージメントである
- リスク分析を行い対策を実施することで、組み込み機器におけるハードウェアの曖昧さを許容し、無限に想定されるヒューマンエラーを効率的に回避する
- 組み込み商品群に対するリスク分析の結果と対策の多くは商品の要求仕様の変化とは対照的に普遍的であり、コア資産として代々蓄えられながら継承されていくべきものである

リスク分析表を使ったマネージメント

- 電子ポットのリスク分析表の例

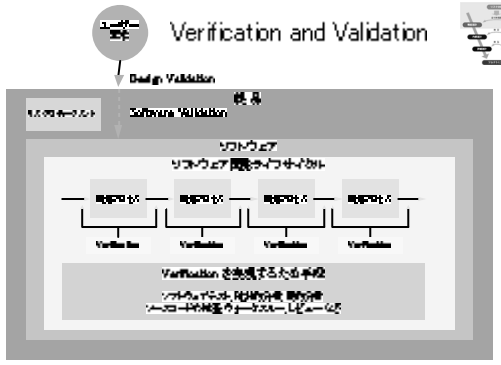
番号	障害	原因	重要度	発生の可能性／故障率	対策	実施確認の方法	チェック
No.	Hazard	Cause	Level of Concern	Likelihood/ Failure Rate	Method of Control	Trace	Check
A-1	ヒーターの異常加熱により火災が起こる	サーミスタの故障 ヒーターの故障	High	1/10000（故障率）	**ハードウェアによる対策** 温度ヒューズによるヒータへの回路切断 **ソフトウェアによる対策** ブザーによる注意喚起とエラー表示（10秒）を行う。	設計書番号 #001 テスト計画 #001	□ □
		水の量が少ないに加熱した	High	たまにあり（Moderate）	**ソフトウェアによる対策** 第1水位センサがオフ状態ならば、ヒーターの沸騰ボタンは動作しない。	設計書番号 #002 テスト計画 #002	□ □

出典：Guidance for FDA Reviewers- PremarkrtNotification Submissions for Automated Testing Instruments Used in Blood Establishments

Validation（妥当性確認）とVerification（検証）

- ソフトウェアライフサイクルプロセス（SLCP）の中の個々のプロセスをきちんと定義し、各プロセスの入力と出力を検証することがVerificationとなる
- Verificationの積み重ねがValidationされているという結論に結びつく
- **Validationはユーザー要求に製品が適合しているという「自信」が十分なレベルに達するまで行う必要がある**
- **リスク（障害）がユーザーに与える影響が大きければ大きいほどValidationは慎重かつ確実に行われる必要がある**

Verification and Validation



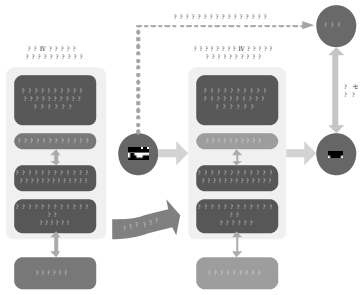
ハードウェア制御を多く含んだ組み込みシステムの

単体テスト・結合テストの方針

	単体テスト	結合テスト
ハードウェア制御を含むコア資産	自動テスト	テストケースを作成
	静的テストツールを利用する	シミュレーションテストを実施する
ハードウェア制御を含まない受動的なモジュール群	テストケースを作成	テストケースを作成
	xUnitなどのテストフレームワークを利用	シミュレーションテストを行う
コア資産でない、ハードウェア制御を含んだモジュール群	自動テスト	テストケースを作成
	静的テストツールを利用する	実機テストで十分に検証する

工数小（スクリーニング）
工数中（設計検証）　工数大（設計検証）

コア資産のシミュレーションテストの例



結論（再掲）

- 組み込み機器の安全性・信頼性をリスクマネージメントによって確保する
  - リスク分析表
- 組み込み商品群におけるコア資産とバリエーションを実現する部分を明確に分離し異なるテストのアプローチをとる
  - プロダクトライン
- **これらにより短期間で効果的な組み込みソフトウェアの妥当性確認(Validation)を実施することができる**

何かご質問はありますか？

E-mail でもお受けします

xx_sakai@d3.dion.ne.jp