

ソフトウェア認証の現状と 産総研の取り組みについて

水口大知

産業技術総合研究所

システム検証研究センター

システム検証研究センターの研究活動

システム検証技術の基礎研究

- 数理的検証技法
- モデル検査法や定理証明法など

システム検証の『フィールドワーク』

- 企業との共同による実用化研究
- 技術者向け研修コースの開発

• 活動拠点

- 大阪・千里中央
- 大阪・池田, 秋葉原, つくば

<http://unit.aist.go.jp/cvs/>

背景

- ソフトウェアの遍在化・社会基盤化
 - ソフトウェアの品質確保が、安心・安全な生活を営むための必須条件
- ソフトウェアの品質や性能に踏み込んだ国際規格が、相次いで策定されている
 - 規格に基づく認証活動が欧米では始まっている
- 一方で、国内体制整備の遅れ

CVS-AIST「ソフトウェア認証研究班」(2005～)

ソフトウェアの認証

- ソフトウェアが定められた要求事項を満たしているということの保証を、第三者が与えるための手続き

現状

- ソフトウェア認証への対応が急務な国内3業界
 - 安全制御機器業界
 - 自動車業界
 - 計量器業界
- ソフトウェアについての要求事項を含む規格がある・できつつある
 - IEC 61508 (E/E/PE安全関連系の機能安全)
 - ISO 26262 (自動車の機能安全)
 - 欧州計量器指令(MID), OIML D-SW
- 認証方式についてのコンセンサスがない

安全制御機器

IEC 61508 – Functional safety of electrical/electronic/programmable electronic safety-related systems (1998-2000)

- プラントや工場等における, コンピュータ技術を用いた安全系のための規格
 - 構成要素(センサー, PLC, ネットワーク機器, RTOS など)も対象
- Part 3: Software requirements
 - ソフトウェア安全ライフサイクル
- 安全度水準(SIL)に応じた技法・手法を推奨
 - SIL 4では形式手法が「強く推奨」されている

問題点

- IEC 61508の普及につれて、国内メーカーも認証取得を目指している
- ✓ どのように開発したらよい？
 - 要求事項が概念的、評価対象が不明確
 - 推奨される手法・技法のうちどれをどの程度まで用いればよい？
 - 形式手法といわれても...
- ✓ 認証機関は、
 - 欧州中心で費用高
 - 評価基準が不明確
 - 国内認証機関を！

自動車

ISO/WD 26262 – Road vehicles – Functional safety (2008?)

- IEC 61508の自動車分野規格
- 自動車における、コンピュータ技術を用いた安全系のための規格
 - ブレーキ、ステアリング、パワートレイン、HV、エアバックなど
 - X-by-wire技術、カーナビ協調制御で範囲は拡大
- Part 6: “Software development”
 - IEC 61508と同様の要求事項
- 発行後、欧州法規化の可能性あり

コメント

- ✓ 本当にベストプラクティス？
- ✓ これで本当に安全につくれるのか？
- ✓ 認証のための負担だけが増加？
- ✓ なぜ形式手法？
- ✓ 非関税障壁になり得る？

計量器

MID: Measuring Instruments Directive (2004)

- 2006年10月30日施行
- 特定計量器についての欧州指令
 - ガスメータ, 電気メータ, はかり, タクシーメータなど
- セキュリティについての要求事項を含む
 - データやソフトウェアの改竄防止
- 国際規格も策定中
 - OIML D-SW “General Requirements for Software Controlled Measuring Instruments”

課題

- ✓ 産総研は国内において特定計量器の型式承認を実施するNotified Body
- ✓ 認証手順を示し、技術ガイドラインを示す必要がある
 - メーカーにおいて実施可能、合意可能でなければならない
- ✓ 認証手順に従って、型式承認を実施しなければならない

ソフトウェア認証の問題点

- 要求事項が曖昧
- 要求事項の合理性が不明
- 認証基準が曖昧
- 技術ガイドラインが不十分
- 規格策定が欧州主導
- 国内に認証機関がない
- 認証費用が高い
- ...

CVS-AIST「ソフトウェア認証のcase studyを!」

「模擬認証プロジェクト」

- (模擬的な)システムの開発プロジェクトを立ち上げ、開発と認証のシミュレーションを平行して実施する
 - 可能な限りフォーマルに
 - 『フィールドワーク』のひとつ

期待される成果

- 認証ノウハウの蓄積
 - 客観的な認証基準の策定
 - 技術文書の作成
 - 規格に示されている手順や手法の妥当性の検討
 - 既存の規格へのフィードバック
 - 新たな規格作りへの展開
 - 規格に沿った開発ノウハウの蓄積
- ✓ 国内ソフトウェア認証機関設立へ向けての第一歩

サポートインダストリ

- 戦略的基盤技術高度化支援事業
 - 経産省, 中小企業基盤整備機構
- 「機能安全対応自動車制御用プラットフォームの開発」
 - IEC 61508 SIL 3対応の車載用RTOS, 通信ミドルウェアを開発する
- 2006年12月より3ヵ年
- 名古屋大学, (株)ヴィッツ, 東海ソフト(株), (株)サニー技研, 名古屋市工研, 道立工試, 産総研CVS
- CVSは, 第三者評価 = 模擬認証を担当

おわりに

- 3業界の動向と模擬認証プロジェクトについて紹介
- ソフトウェア認証は、緊急かつ現実的な課題である
- 今後、ソフトウェア認証に対する需要は、身近な領域に広がり、重要性はますます大きくなる
- よい認証制度は、関連する業界および利用者である市民からの信用が不可欠
- 模擬認証プロジェクトは、フォーマルな技術に立脚して、こうした信用の確立に貢献する