本スライドは、当日のセミナー資料から一部を抜粋したものです。

機能安全と安全システム技術

2011年11月18日

高田 広章

名古屋大学 大学院情報科学研究科 教授
附属組込みシステム研究センター長

NPO法人 TOPPERSプロジェクト 会長

Email: hiro@ertl.jp　URL: http://www.ertl.jp/~hiro/

今なぜディペンダビリティか?

組込みシステムのネットワーク接続と社会インフラ化

- 組込みシステムがネットワーク接続され，社会インフラ化が進むことで，その障害が社会に大きな影響を与える

説明/証明責任に対する社会意識の変化

- 先端技術の潜在リスクに対する不安
- メーカの説明/証明責任に対する要求の高まり

コンピュータ制御の拡大

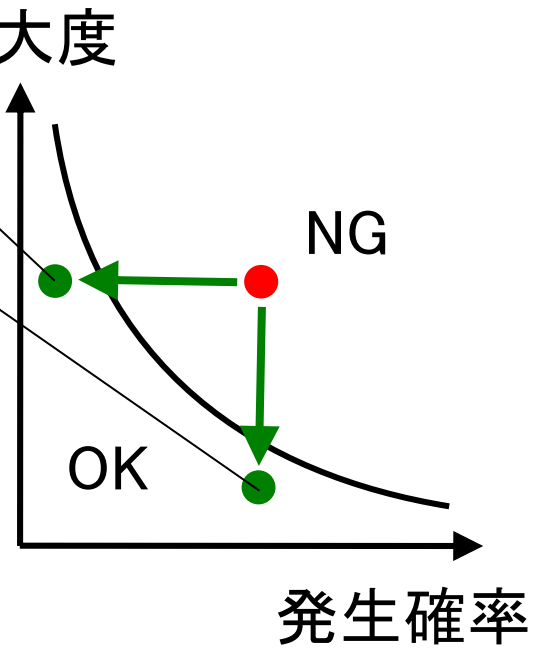
- システムの高機能化・省エネルギー化・低コスト化のために，従来は機械的/電気的に実現されていた機能が，コンピュータやネットワークにより実現される例が増加

組込みシステム/ソフトウェアの複雑化

- システム/ソフトウェアの複雑化の進行により，ディペンダビリティの確保が困難に

安全システム技術

- 許容度を超えるリスクを，軽減するための技術
  - 事故の発生確率を下げる
  - 事故の重大度を下げる



高信頼システム技術

- フォールトアボイダンス
- フォールトトレランス

フェールセーフ（fail safe）

- システムの構成要素が故障しても，システム全体が安全側（重大度が低い側）に動作するように設計する
  例）ABSの制御システムが故障したら，動作を止める
- 故障を検知する方法とそれによる検知率が問題
- 安全側の動作がないシステムには，適用できない

安全設計の事例

! 車載制御システムの安全設計の事例として，NASAの報告書に記載されているトヨタの電子スロットル制御システムの安全設計を紹介

NHTSA&NASAの調査報告の概要

- NHTSA（米運輸省高速道路交通安全局）が，2011年2月に，トヨタ車の急加速†問題に関する調査報告を行った
  - † 原文では “unintended acceleration (UA)”（意図しない加速）
- NHTSAとNASAは，トヨタがすでにリコールしている件以外に，急加速が起こる原因は見つからなかったと結論
- 電子スロットル制御システムの調査については，NASAが協力
  - 調査内容に関しては，報告書にまとめられている
  - 報告書の全文は，NHTSAのウェブサイトにある

車載システムのための機能安全規格

ISO/DIS 26262 （DISは“Draft International Standard”の意味）

- “Road vehicles – Functional safety –”
- IEC 61508の自動車分野向けのサブ規格
- 基本的な考え方はIEC 61508を踏襲しているが，自動車分野の状況に合致するように様々な修正/追加規定
  - 自動車向け安全度水準ASIL AーDを規定
  - 自動車に特化したハザード分類の方法を定義
  - 大量生産品であることを考慮
  - 複数の組織で開発することを考慮

ISO/DIS 26262における機能安全の定義

- 電気・電子システムの誤動作を原因とするハザードによる許容できないリスクがないこと（ISO/DIS 26262-1 独自訳）

機能安全規格への対処指針

規格対応の目的を明確にすること

- 認証を取ることが目的(ユーザから要求されている場合など)なら，最低限のコストでクリアするべき
- 製品の安全性を向上させたいなら，規格の中で自社に役に立つところだけ採用すればよい(必ずしも全部やる必要はない)．それには自社の強みと弱みを知ることが必要
- その両方なら，メリハリを付けるべし

留意すべきこと

- 規格に書いてあるプロセスをそのままの形で実施しないこと．各規定の趣旨を理解し，自社のプロセスと比較し(gap analysis)，できていない規定のみ新たに対応すればよい
- 安全機能を入れ過ぎると，信頼性が下がることもある