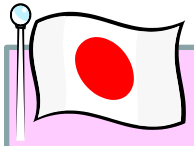
本スライドは、当日のセミナー資料の一部を抜粋したものです。

機能安全ISO 26262対応 ソフトウェア開発の効率化への取り組み

株式会社ヴィッツ
執行役員 機能安全開発部 部長
株式会社アトリエ 取締役
森川 聡久

従来開発と機能安全開発の大きな違い



従来開発

①壊れないモノ作り

・自己努力によって壊れにくいもの、バグゼロが目標

・匠の技術で作られた高信頼性部品を使用

②日本流開発スタイル

・担当者間の“すり合わせ開発”で、効率的に開発を進行

・開発文書の出来栄えは不十分（必要最小限）

安全性強化

不慣れな開発スタイルへ

機能安全開発

①壊れても安全なモノ作り

・高品質の証拠を積み重ねた開発によってバグゼロが目標

・万が一構成部品が故障しても危険にならない「仕組み」が必要

②安全説明力のある開発

・PL訴訟時に安全を客観的に説明できる開発文書の作成やエビデンスが必要

組込みシステムの複雑化による事故多発への対応として「実の安全性向上」と「PL訴訟対策」のため、機能安全は生まれた。
機能安全規格への適合で、過剰な安全対策を排除可能。

日本企業は「安全説明力」が課題!!

②安全説明力

KMC_Profile_20120706.pdf

Functional Safety (ISO 26262)

Effort for safety projects increase compared to non safety-related projects

ISO/DIS 26262	Effort Increase
ASIL A	5 - 20 %
ASIL B	10 - 35 %
ASIL C	20 - 60 %
ASIL D	40 - 100 %

Note:
- Estimation, not measured data
- Many factors heavily influence actual effort
- Clarify assumptions and requirements before making estimations

過剰対応

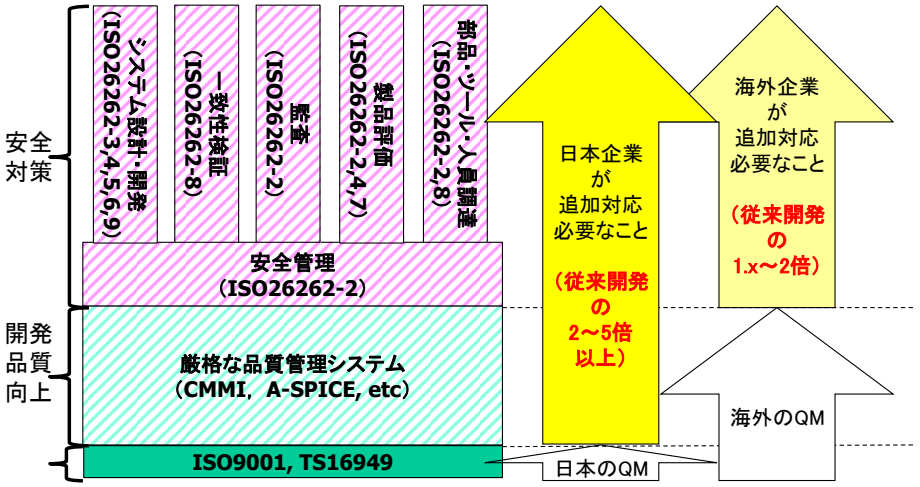
合格

★欧米

従来開発コストの1．X倍

慣れるまでは数倍

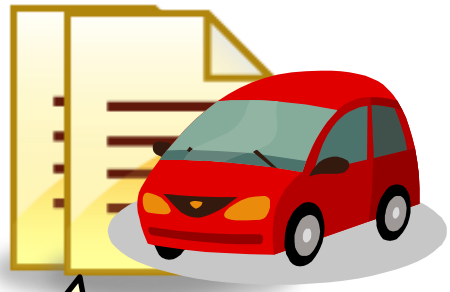
★日本



①安全性向上

安全規格適合
(IEC61508, ISO26262,
ISO13849, etc)

トレーサビリティ管理の必要性
～なぜ必要か？何に使うのか？～



品質向上

規格対応

①機能安全規格等への対応

②要求の設計・実装・検証漏れを防ぐ

③変更・派生開発の要求・設計・検証漏れを防ぐ

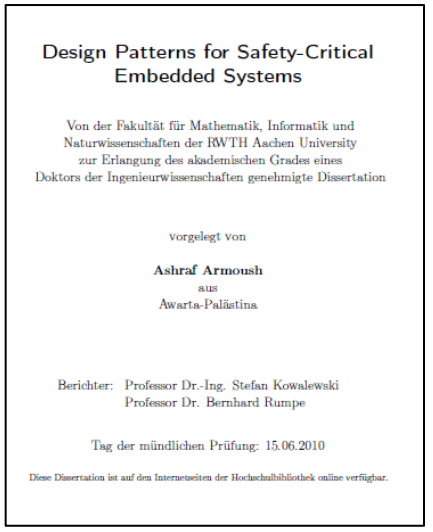
説明責任

④第三者に設計、検証漏れがないことを分かりやすく示す

設計変更、あるいは派生開発時の影響分析

文献調査＆活用方法の概要

- 調査した2文献
  - Bruce Powell Douglass, “Real-Time Design Patterns”, Addison-Wesley, 2002.
  - Ashraf Armoush ,”Design patterns for Safety-Critical Embedded Systems”, 2010.


Design Patterns for Safety-Critical Embedded Systems

Von der Fakultät für Mathematik, Informatik und Naturwissenschaften der RWTH Aachen University zur Erlangung des akademischen Grades eines Doktors der Ingenieurwissenschaften genehmigte Dissertation

vorgelegt von

Ashraf Armoush
aus
Awarta-Palästina

Berichter: Professor Dr.-Ing. Stefan Kowalewski
Professor Dr. Bernhard Rumpe

Tag der mündlichen Prüfung: 15.06.2010

Diese Dissertation ist auf den Internetseiten der Hochschulbibliothek online verfügbar.

- 活用方法
  - 安全設計のノウハウをデザインパターンとして分類、整理し、UML、ブロック図、決定木などを利用して構成やパターンの選択基準を表現したことで、**安全設計のノウハウを理解しやすい形で表現**している。
  - 安全設計のデザインパターンでは、（他のデザインパターンと違い）、**非機能要求がパターンの選択基準や効果の中で重要な意味を持っていることを主張**している。
  - **教育・開発に適用することで、効率化**できる手ごたえあり。

Bメソッド適用開発ライフサイクル

開発文書のレビュー、トレーサビリティ管理、コーディング、テスト実施などの活動を省略可能