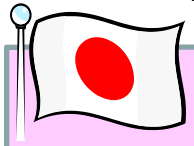
機能安全規格 ISO 26262 対応
ソフトウェア開発の効率化への取り組み

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。

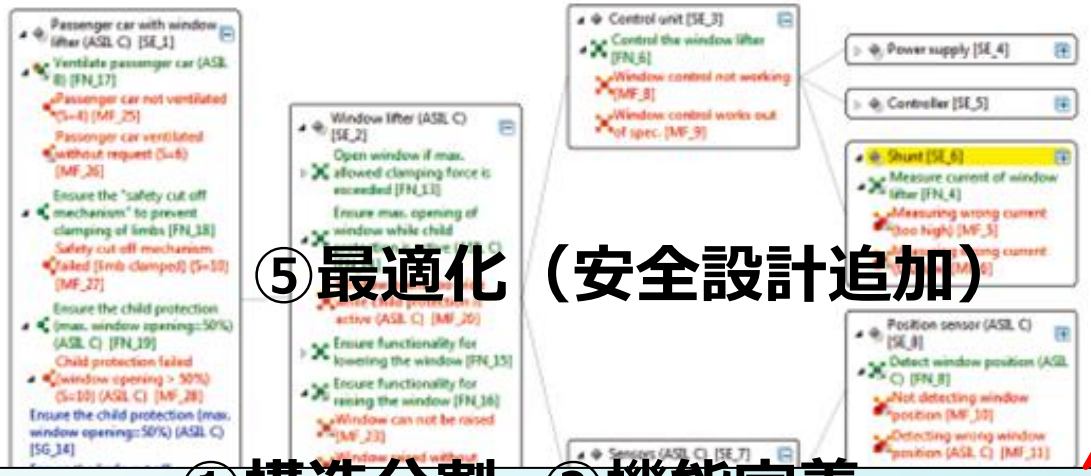
準形式記述における課題

- 機能安全開発の現状
  - 各図を個別に作成。
    - 規格要求を満たすために愚直に作業。
  - 各図間の情報連携（整合）が不十分。

- 課題
  - 情報間の不整合が発生。不整合の検出が困難。
    - 理由：各図間の情報連携意識が乏しいため
  - 開発（作図）効率が悪いのではないか？（推測）
    - もっと流れるように作図を進めれないか？

VDAのFMEA手法の推奨

- VDA：ドイツ自動車工業会
- 5ステップメソッドのFMEA手法
  - ① Product breakdown to system levels
  - ② Functional description of system
  - ③ Failure Analysis
  - ④ Risks Evaluation
  - ⑤ Risk Optimization
    - 参考：http://www.opsalacarte.com/reliability-blog/dfmea-acc-to-vda-5-steps-approach/



⑤最適化（安全設計追加）

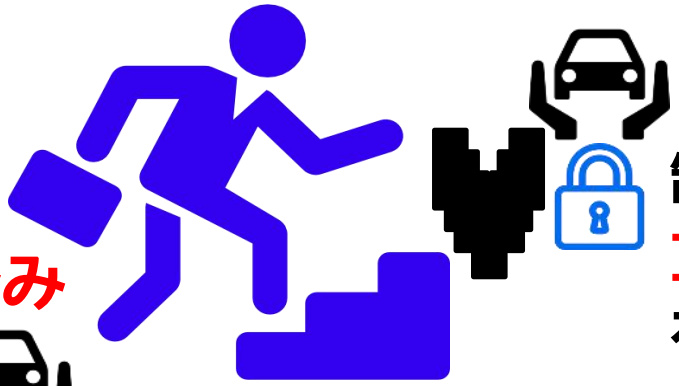
構造分割・設計と安全分析を並行実行可能

①構造分割　②機能定義

③影響分析（安全分析）　④リスク評価

【当社事例】 Safety＆Security要求事項のギャップを詳細整理

自動車機能安全規格
ISO 26262 対応済み
を前提



制御セキュリティ規格
IEC 62443対応
を想定

ISO 26262対応では不足事項、
達成度評価、対応策を整理
（当社経験に基づく）

IEC 62443要求事項

章番号	和訳	ISO26262適合根拠	ISO26262適合判定
5	Phase1 セキュリティ管理プロセス		
5.1	目的		
	セキュリティ管理プロセスの目的は、セキュリティ関連アクティビティを計画し、スケジュールを決定し、割り当てを行い、能力のある作業者がそれを満たすことを保証することである。	**[part2-5.4.3 能力管理]** 安全ライフサイクルの実行に関わる人々が責務に対応できる十分なレベルの能力を持っていることを保証しなければならない、とある。 **[part2-6.4.3 安全活動の計画及び調整]** 安全管理者は必要とされる技能、能力及び資格を所有している人物に、タスクを委任することができる、とある。 **[part2-6.4.3.6]** 安全活動の計画は、次の記載を含まなければならない。 c)活動の実行に責任を持つリソース d)活動の実行に必要なリソース e)開始時点及び期間 以上よりISO26262の安全活動計画によって、ほぼ同等のことはなされている。 セキュリティを安全に読み替えることで対応可能と判断し△とする。	△
5.2	論理的根拠		
	セキュリティ関連アクティビティを計画、管理に注意が払われていない場合、そのアクティビティは、十分な時間とリソースを割り当てられず、行き当たりばったりの方法で完了する可能性がある。したがって、これらのアクティビティを十分に計画することを保証することで、作業成果物の結果の品質を保証する助けとなる。	同上	△
5.3	SDSA-SMP-1-セキュリティ管理計画		
	要件 セキュリティ管理が既に標準ソフトウェア開発ライフサイクルの一部として含まれている場合を除き、セキュリティが開発ライフサイクルを通して取り組まれたことを保証するための計画を文書化するものとして、セキュリティ管理計画を独立したもしくは他の計画書の一部として文書化しなければならない。	**[part2-6.5 作業成果物]** 6.4.3から6.4.5の結果として安全計画を作成するよう要求している。 今回の場合、セキュリティ管理がライフサイクルの一部として含まれているわけではないので、セキュリティ管理計画を作成するor組み込む必要がある。 セキュリティを安全に読み替えることで対応可能と判断し△とする。	△

画像引用：http://www.flaticon.com/

【当社事例】VDAのFMEA手法のセキュリティへの応用（1/2）