SPI Japan 2012

高信頼ソフトウェア開発への取組み

～製品安全、機能安全、システム安全～

2012年10月11日

パナソニック株式会社

中川 雅通

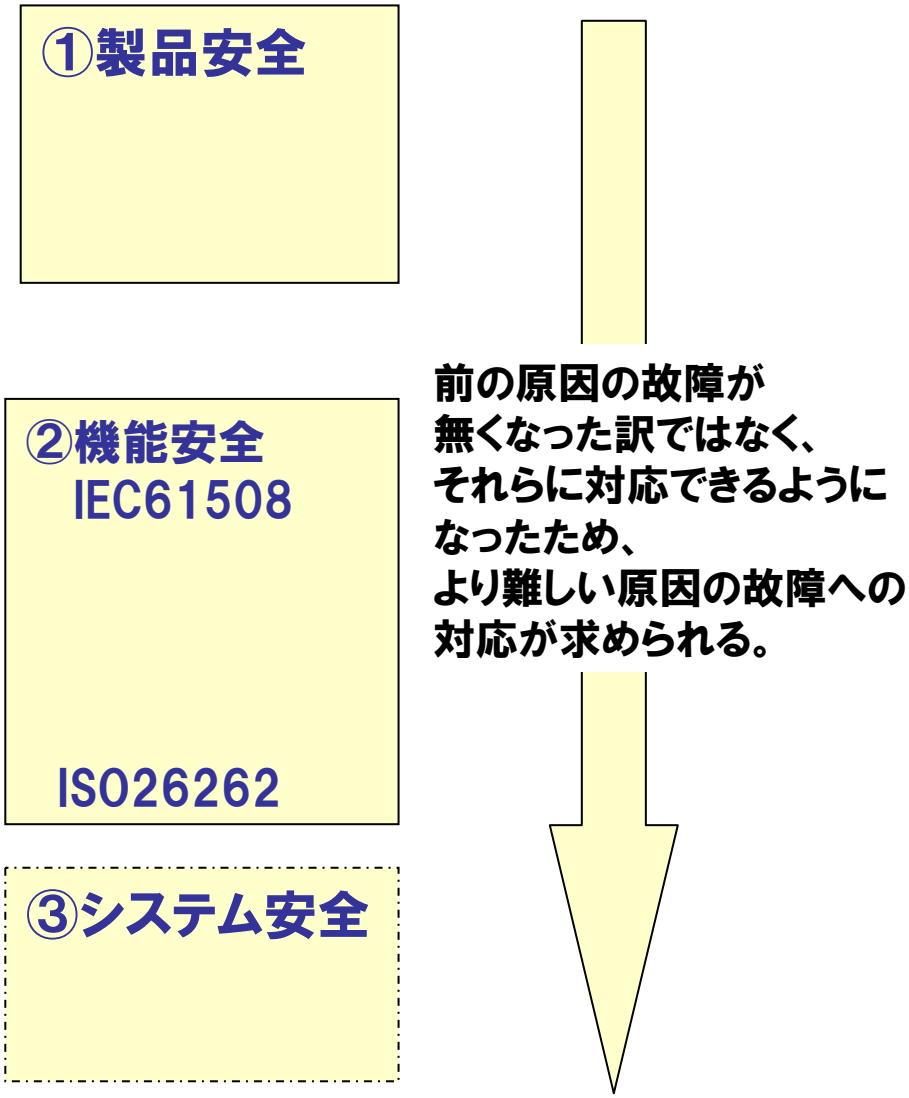
はじめに

- 製品の信頼性、安全性へのソフトウェアの果たす役割が強まっている。
- また機能安全、大規模化するシステムへの対応も必要となっている。

- 従来の製品安全から、機能安全、システム安全への流れと、それらでの取組みについて説明する。

故障の原因モデル

- 確定論
  - 構造、材質などが故障の原因
  - 経年劣化
- 確率論
  - 部品のばらつき
  - 信頼性モデル
- 開発プロセス
  - 設計、開発の過程に潜む不具合（システマティック故障）
- システム間、環境
  - システム間の整合性のずれ
  - 利用環境の変化



①製品安全：家電の寿命

皆さんのお宅の家電は何年製造モデルですか？

50年代以前	60～70年代	80～90年代	2000年以降
 白黒テレビ	 カラー	 薄型ﾌﾞﾗｳﾝ管	まだ現役！
	  全自動 2ドア	  ファジイ制御 野菜室	 HD、3D デジタル放送 薄型ﾃﾞｨｽﾌﾟﾚｲ
博物館？	大半は廃棄済み		  斜めドラム乾燥機 省電力 現在の商品

家電製品の製品寿命は10-20年と非常に長い

①製品安全：経年劣化

経年劣化による重大製品事故続発し、社会問題

- ●事故情報の公表遅れが被害拡大
- ●**長期使用製品の経年劣化**による事故

消費生活用製品安全法の改正

■ **重大製品事故報告の義務化と公表**（07年5月14日施行）

事故情報の積極的な開示と処置

■ **長期使用製品の点検制度**（09年4月1日施行）

経年劣化に対する安全対策、点検体制整備

経年劣化への対応の例

長期使用製品安全点検制度 では、特定の商品（特定保守製品）に対し

・お客様から所有者票を特定製造事業者などに返送し、同事業者がこれを適切に保管、その後、点検時期をお客様にお知らせし、要請に応じて点検（有償）を実施

・製品本体やリモコンなどのラベルに特定保守製品である旨を表示

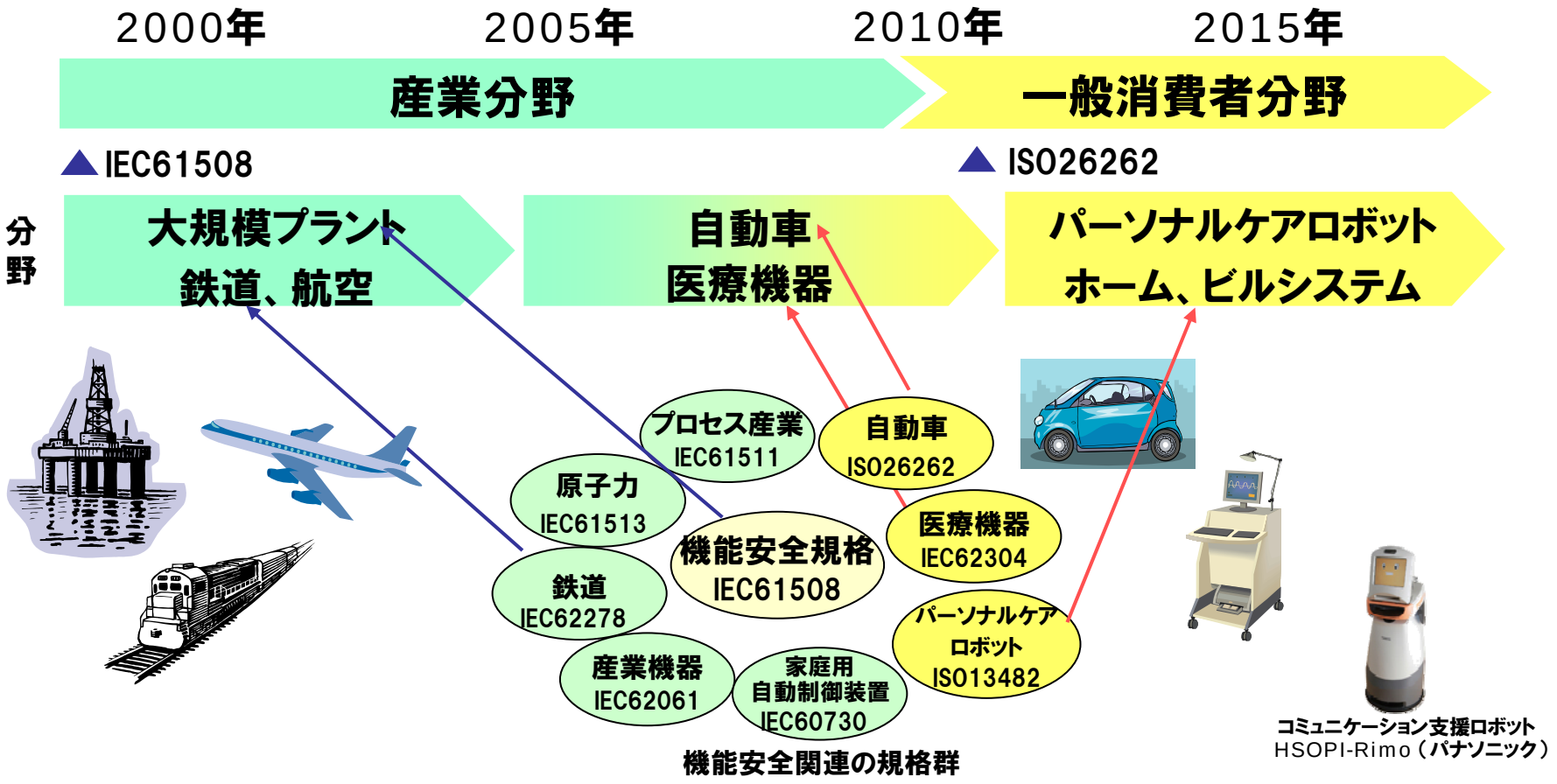
を実施しなければならない。

弊社 浴室用電気乾燥機の取組み例

・**点検時期の到来をリモコンに表示**（点検＝チェックを意味する「C」を点滅）する機能を搭載して、お客様の点検もれがないようお知らせ

②機能安全

機能安全： マイコンなどの電気・電子的な装置の働き（機能）により実現されている安全性
機能には、故障の検出、安全な停止制御、ユーザへの警告などがある



産業分野から消費者分野への波及しつつある。その先頭が自動車の機能安全

②機能安全規格の特徴

- **安全度水準(SIL,ASIL)**
  - 絶対安全ではなく、リスクを減らすという考え方
- **システマティック故障** ⇔ ランダムハードウェア故障
  - 部品故障だけでなく、設計ミス、ソフトウェアバグなどへの対応
- **プロセス、人、組織も対象**
  - Systematic故障に対応するには、製品だけでなく、
    それを作った組織、人、開発プロセスを対象にしなければならない
  - 開発、製造、保守、廃棄までの安全ライフサイクルを視野に
- **説明責任**
  - とくに自動車機能安全規格ISO26262では、安全ケースという考え方
    を取り入れて説明責任の考え方がより明確に

故障の分類

- **ランダムハードウェア故障**
  - 構成部品・機器などの多様な劣化のメカニズムのもとで時間的に無秩序に発生する故障
    - 例：ハード部品の劣化

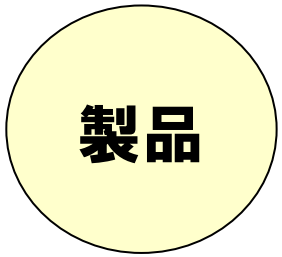
対策
- 故障率などによる統計的な分析、対策
- SILに応じた故障率まで下げる。高信頼の部品の使用、2重化など

- **システマティック故障**
  - 設計過程、製造過程、運転手順、文章化などに直接関わり、これらの中で故障原因が入り込むことで、必然的に発生する故障
    - 例：要件の誤解、IFのミスマッチソフトウェアのバグ、回路の設計ミス

対策
- 定量的な対策が不可能。プロセス、手順の管理、改善
- 安全ライフサイクルに基づいた改善
  ＋SILに応じた開発手法、検証を行う

製品＋マネジメントの規格

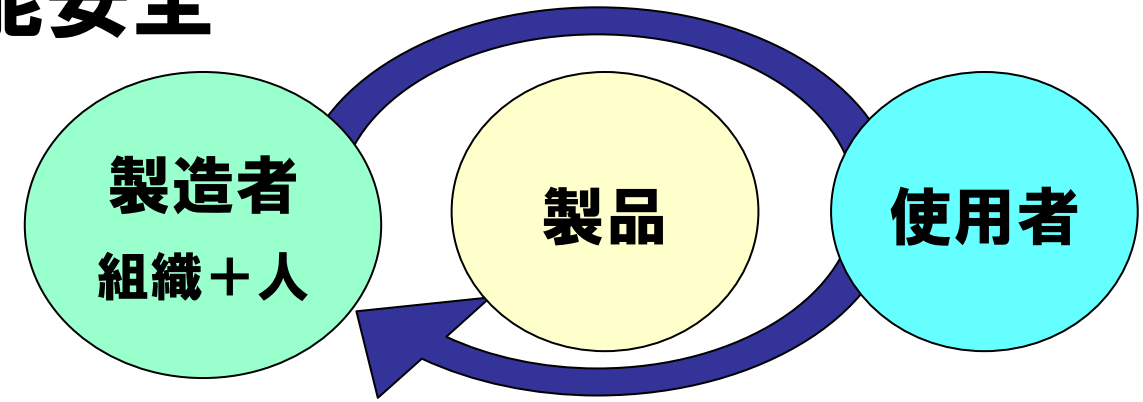
従来の製品安全



製品仕様の要求 → 製品安全認証

製品だけを見る（故障率など）

機能安全



安全ライフサイクルの要求 → プロセス、マネジメント

ソフト開発では当たり前だが、安全では機能安全から取り入れ

説明責任

- 機能安全規格は、その時点での最善を尽くすための最低限の守るべき水準
- 万が一の市場問題の発生した時への備え
- 複数社での開発での責任分担
- 規格自体にも、**根拠を明確化した設計、テスト、トレーサビリティ**など
  他者への説明責任の考え方が背景にある。

説明を行う体系として「**安全ケース**」が
ISO26262では導入された。

英国の鉄道、航空などでの安全性を
説明する文書体系として使われていた。

ただISO26262には、右の図のように
安全ゴールや安全要求と、開発成果物
をArgument(論述)してつなぐという
説明しかない。

→ どう具体化すればよいのか？

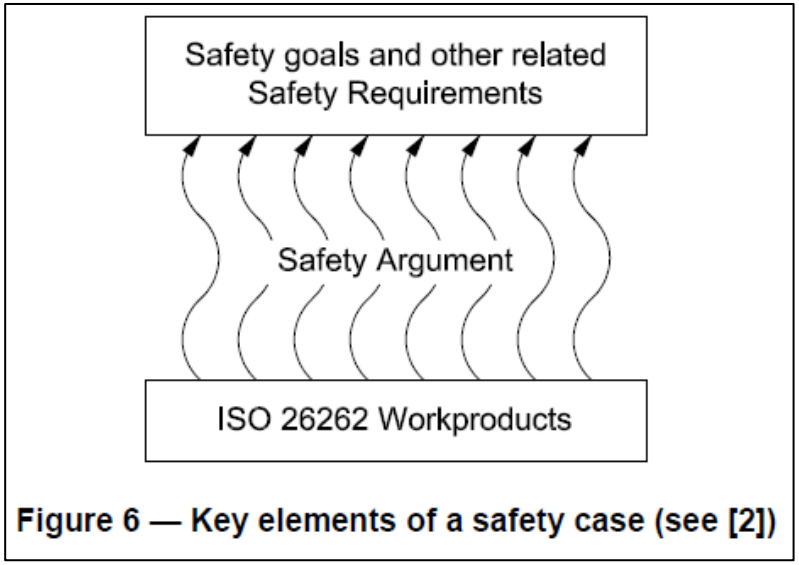
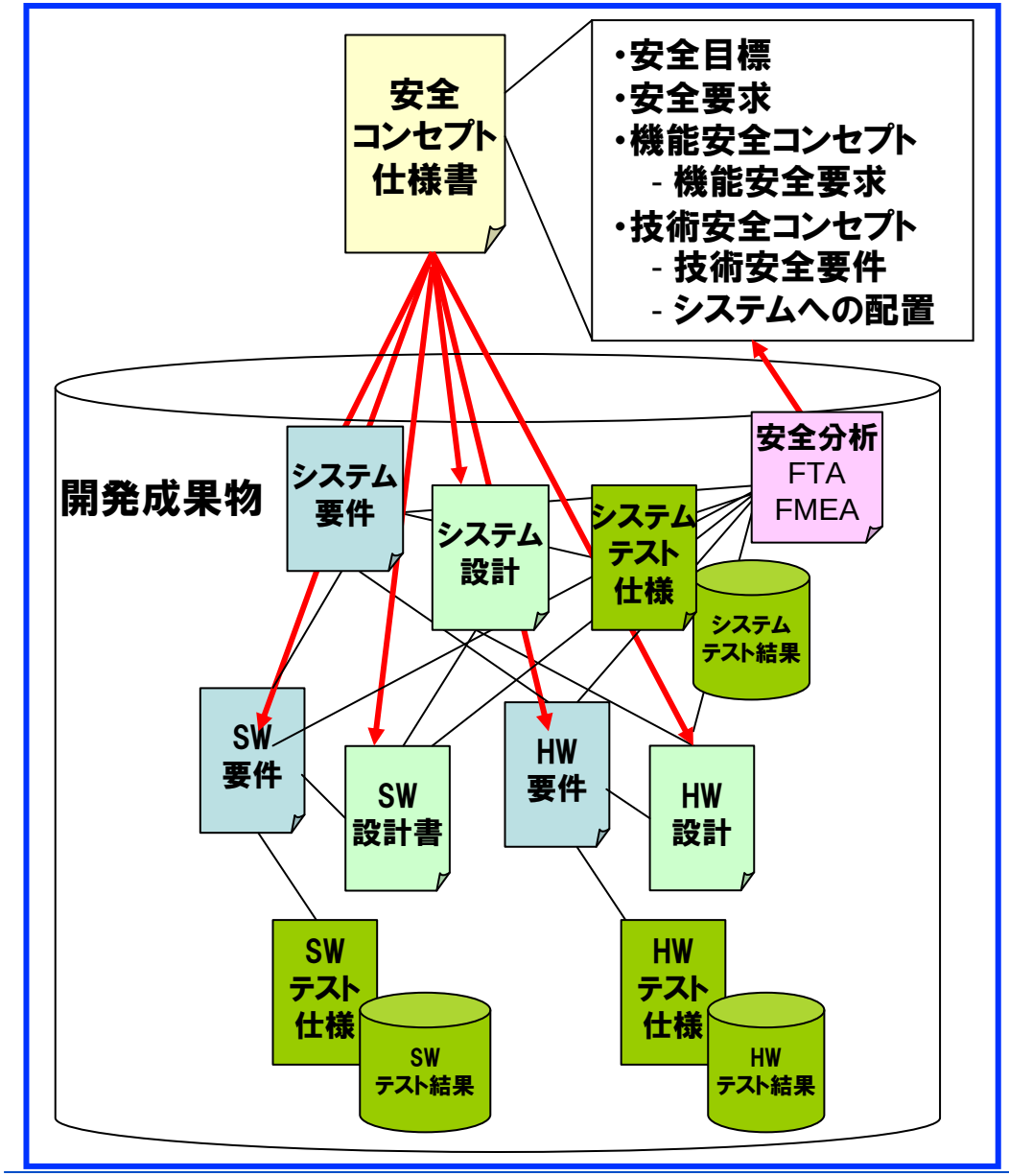


Figure 6 — Key elements of a safety case (see [2])

ISO 26262-1-:2012
5.3 Understanding of safety cases より

安全ケースの具体構成の例



この文書体系全体が安全ケース

- 開発成果物の中で安全関連の項目（要件、設計の構成要素など）を、結びつける要として、「安全コンセプト仕様書」を作成
- 安全コンセプト仕様書には、
  - 安全項目のIndexの役目、
  - 安全項目間の関係を説明する記述

  を含む
- 安全項目間の十分性は安全分析により担保する

②機能安全への取組み

◆ ISO26262への取組み

– 数年前より社内で勉強会を実施

– 2011年

• 機能安全対応のプロセス体系を構築、パイロット開発で試行

• 第三者認証機関からISO26262プロセス認証取得

– パナソニック株式会社 (TUV SUDより 2012年2月)

– パナソニック アドバンスト テクノロジー株式会社(SGSより 2012年8月)


CERTIFICATE

No. Q4B 12 02 68246 002

Holder of Certificate: Panasonic Corporation

Factory(ies):

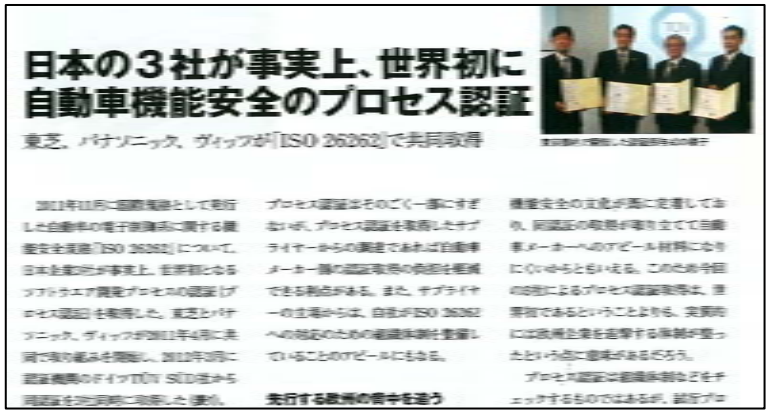
Certification Mark:

Scope of Certificate: Software Development Process

Applied Standard(s):


CERTIFICATE NO FS/71/220/12/0014

CERTIFICATE


日本の3社が事実上、世界初に
自動車機能安全のプロセス認証

東芝、パナソニック、ヴィッツが「ISO 26262」で共同取得

日経エレクトロニクス 2012.4.16号

– 具体的な取り組み内容は、この後の発表でご紹介

• 開発プロセス、機能安全監査・審査、レビュー手法 など

ISO26262とシステム安全

IEC61508と比べて、システム安全の考え方が取り入れられている

- 一般消費者が利用
- 構成要素の積上げではなく、機能を果たすシステムに着目
- 複数の組織の共同作業

} システム安全

	IEC61508	ISO26262
対象	(暗黙に)工場、プラント	自動車
操作する人	熟練した技術者	一般消費者 但し運転免許保有
安全機能	主に安全系の保護システム	通常の制御システム
安全度水準	SIL	ASIL
安全度水準の対象	構成要素、部品個別	機能
実装する組織	(暗黙的に) 1つ	複数 (メーカ、サプライヤ)

③システム安全

個別システムを組み合わせた統合システムの安全性

【課題】

- 個々の要素システムが正しく安全に動いても、要素間インターフェースの不整合などにより、安全性が脅かされる
- 個々の要素が追加、変更、削除されるなどダイナミックな変更により設計時の想定外になる(オープンネットワークシステムなど)
- 利用者自体も要素システムの一つで、複雑で予測が難しい
- 安全の責任範囲が不明瞭になりやすい
  - 組合せによる不具合は、誰の責任か
  - そもそも不具合の原因究明が困難

先進的な取組みが行われているが、確立したアプローチはまだない

③システム安全への先行取組みの例

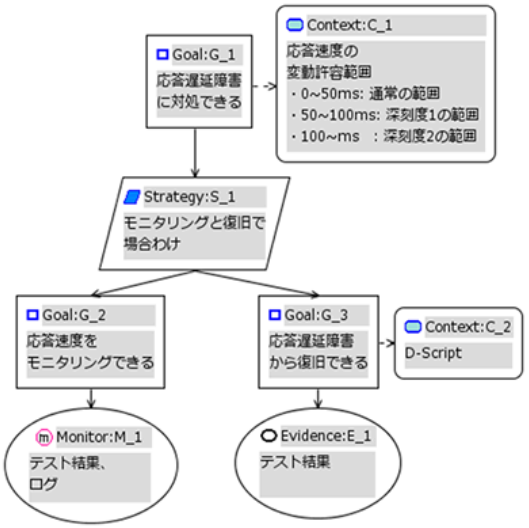
- JST-CREST DEOSプロジェクト http://www.dependable-os.net/osddeos/index.html

  Dependability Engineering for Open System

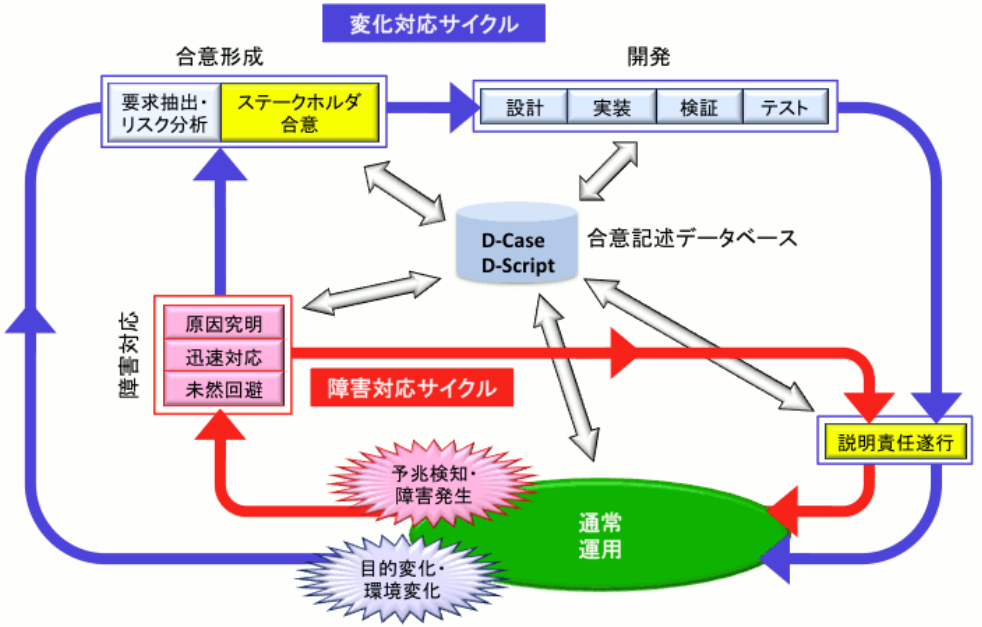
【特徴】

・ディペンダビリティの合意および証拠の**動的な記述**が可能なD-Case 言語

・リアルタイムの障害に対応する障害対応サイクル(赤)と、
要求・環境変化対応サイクル(青)の2重サイクルによる、未知の変化への対応



D-Caseの例



まとめ

- 安全への取り組みの対象が、材質、機構から、部品の経年劣化、ソフトウェア、システムと拡大
- 機能安全が、産業分野から消費者分野へ展開
- 機能安全の特徴：
  - リスクベース → ハザード分析、安全度水準(SIL、ASIL)
  - システマティック故障への対応 → プロセス、組織マネジメント
  - 説明責任 → 安全ケース
- 今後、システム安全への取組みが必要

ご清聴ありがとうございました

Panasonic

ideas for life